SINTEZA

obiecțiilor și propunerilor/recomandărilor

la proiectul HCE al BNM pentru aprobarea Regulamentului cu privire la autentificarea strictă a clienților și standardul deschis, comun și sigur de comunicare între prestatorii de servicii de plată

Conținutul punctelor din proiectul prezentat spre avizare și coordonare	Participantul la avizare (expertizare)/consultare publică	Nr. obiecției/ propunerii/ recomandării	Conținutul obiecției/propunerii/ recomandării	Argumentarea autorului proiectului
I. Obiecții și propuneri de ordin general				
-	B.C. „MAIB" S.A.	1	Lipsa obiecțiilor/ propunerilor pe marginea proiectului de regulament	
-	B.C. „Energbank" S.A.	2	Lipsa obiecțiilor/ propunerilor pe marginea proiectului de regulament	
-	Banca Comercială Română Chișinău S.A.	3	Lipsa obiecțiilor/ propunerilor pe marginea proiectului de regulament	
-	Ministerul Dezvoltării Economice și Digitalizării	4	Lipsa obiecțiilor/ propunerilor pe marginea proiectului de regulament	
-	OTP Bank S.A.	5	Daca clientul efectuează o plata din aplicația băncii, dar de pe conturile deschise în altă banca, de la cine va putea solicita extras /document confirmativ? Conform art.9 al Legii nr. 308/2017, "banca este obligata sa păstreze documentele termen de 5 ani pe suport de hârtie + 5 ani în format electronic după terminarea relației de afacere". Care banca este responsabilă de furnizarea informației aferente operațiunii?	**Comentariu:** Informațiile se furnizează de la banca ce administrează contul de plăți cu privire la extrasul de cont. Referitor la confirmarea executării plății, aceasta trebuie să o facă prestatorul de servicii de inițiere a plății, în acest caz OTP (această informare are la bază confirmarea primită de la prestatorul de servicii de plată care oferă servicii de administrare cont).
-		6	În cazul când clientul deține conturi în diferite instituții bancare / financiare, care ulterior vor fi integrate într-o singură aplicație, cine se face responsabil de respectarea securității contra fraudelor ?	**Comentariu:** Prestatorul de servicii de inițiere a plății este o instituție licențiată și reglementată prin Legea nr. 114/2012, prin urmare are aceleași obligații de păstrare a securității datelor ca o bancă și de aplicare corespunzătoare a cerințelor de autentificare strictă a clienților (SCA) pentru accesul la cont și orice acțiune la distanta care poate implica un risc de fraudare a plății sau alte

				abuzuri (ex. înrolarea aplicației de AIS pe telefonul clientului).
-		7	Conform LEGII 114/2012 art. 56 alin (1) " Utilizatorul serviciilor de plată poate obține corectarea unei operațiuni de plată din partea prestatorului numai dacă informează pe prestatorul său de servicii de plată, în cel mai scurt timp, dar nu mai târziu de 13 luni de la data debitării contului său, despre faptul că a constatat o operațiune de plată neautorizată sau executată necorespunzător, care generează reclamație, inclusiv în conformitate cu art.70". Cine se face responsabil de tratarea reclamațiilor si corectarea plăților executate?	**Comentariu:** În toate situațiile de refuz la plată/corectare operațiune este responsabil ASPSP, întrucât acesta ține contul de plăți al USP și asigură transferul fondurilor. PISP nu intră în posesia fondurilor USP.
-	VISA	8	European experience has demonstrated that SCA implementation is challenging. Implementation of SCA does not only depend on issuers and acquirers, but also on the active cooperation of merchants. We note that in the EU, it took more than 5 years for SCA to be fully enacted, and even today, there are several use cases that cannot be achieved in practice, among other issues. For these reasons, we encourage the National Bank to carefully consider the results of the PSD2 review (*Study on the application and impact of Directive (EU) 2015/2366 on Payment Services (PSD2) by EU Commission*), which highlights the major challenges of the SCA implementation. One of the points raised in the Study is that "*the SCA requirement has made the customer journey in a transaction more difficult and cumbersome which can mean consumers do not complete e-commerce transactions. Moreover, there remain loopholes in SCA, which allow fraudsters to circumvent security provisions*".	**Comentariu:** Conform *Studiului de impact al PSD2,* pe lângă provocările întâlnite în implementarea SCA, a fost subliniat inclusiv faptul că ratele de fraudă au scăzut în urma implementării SCA, precum și că SCA a fost un catalizator pentru industrie (emitenți, achizitori, comercianți) pentru a-și consolida apărarea împotriva fraudei printr-o mai mare utilizare a sistemelor în timp real și a unor reguli mai stricte împotriva fraudei.
-		9	Visa would need at minimum twelve months to review its internal rules and procedures, and inform the ecosystem accordingly.	**Comentariu:** Prezentul proiect de regulament a fost publicat pentru consultări publice pe data de 06.03.2023, iar intrarea în vigoarea a acestuia este prevăzută pentru data de 5 august 2024. Astfel, considerăm că este suficient timp pentru toți actorii pieței să depună eforturi în sensul pregătirii pentru conformare cu prevederile regulamentului (fiind o perioada similară cu cea alocata pentru piața UE). Mai mult ca atât, cât timp VISA este prezentă inclusiv pe piața UE, aceasta are experiența și pregătirea tehnică pentru a implementa SCA inclusiv pe piața din RM.

-		10	Ecosystem participants, in addition to issuers and acquirers, must be ready for the rollout. - Merchants handling card present transactions must learn how to work with the new response code and handle additional authentication requests from issuers on their point-of-sale terminals. If this is not properly done, transactions may be declined. - E-Commerce merchants must be capable of handling new response code, and learn the support of exemptions, correct coding and presentment of transactions, utilization of new use cases in EMV 3-D Secure. Inefficient rollout of regulation would hinder the growth of Moldova's online commerce, having a significant negative effect on the economy as a whole. - 100% accuracy from day 1 is highly unlikely - real-time test cases, following the technical implementation will reveal errors that could not have been predicted. Even the most tech savvy merchants/marketplaces/gateways cannot handle Strong Customer Authentication use cases without faults.	**Comentariu:** Experiența VISA, inclusiv de implementare a cerințelor SCA pe piața din UE, va facilita implementarea acestor cerințe inclusiv pe piața din RM.
-		11	Historically, the CIS (Commonwealth of Independent States) & Southeast Europe markets, especially Moldova, have had low levels of fraud rates in card present transactions. Visa is confident, that postponing the SCA implementation deadline would not have a negative impact on the fraud rates. In addition to that, usage of biometric verification on customer devices for payments with Third Party Wallets (e.g. Apple Pay) already provide compliance measure with SCA requirements.	**Comentariu:** Îngrijorarea nu este în „card present transactions" ci ``card not present`` – aici fiind necesare măsuri de securitate, care sunt prevăzute în prezentul proiect de regulament.
-		12	Expanding the concept of behavioral biometrics as inherence factor for remote payments: It has been proven that behavioral analytics solutions, such as 3DS profiling, are vastly superior in terms of fraud prevention compared to static knowledge factors.	**Comentariu:** Prestatorii de servicii de plată vor alege mecanisme SCA în funcție de clienți.
-		13	Flexibility on the use of SCA factors: Payment service providers should be free to develop solutions that satisfy the independence obligation without having to apply two factors from different prescribed categories, which are arbitrary and limit the development of effective two-factor solutions. The focus should be on the independence of those factors and the fact that the breach of one does not compromise the reliability of the others. Focusing on the liability shift, rather than non-compliance: If SCA requirements are not applied by a merchant/acquirer, the consequence shall be that the merchant/acquirer are liable for fraudulent transactions.3 Clarifying this liability shift in the Draft	**Comentariu:** Luând în considerare statutul Republicii Moldova – de stat candidat la UE, cadrul de reglementare național trebuie aliniat la prevederile UE. Prestarea serviciilor de plată, inclusiv în contextul aderării Republicii Moldova la Zona Unica de Plăți în euro, trebuie sa se desfășoare la „același nivel echitabil de joc". În ceea ce privește termenul propus de intrare în vigoare, a se vedea comentariul de mai sus.

			Regulation will help ensure consumer protection and is a sensible alternative to strict implementation of a pure SCA mandate. As a leading global payments company, Visa has experience with the technical aspects of the SCA implementation in different countries. Given that Visa will take all necessary measures from both technical and system operations perspectives to ensure implementation of the regulation, we would like to stress the importance of a reasonably established implementation timeframe so that payment service providers can harmonize their operations to the newly required technical and operational preparations and enhancements. Therefore, to avoid disruption and allow market participants to smoothly adapt to the changes proposed by the Draft Decision, we kindly ask you to postpone the process of the SCA implementation and split it into two stages with the nearest technically feasible timeline as follows: 1. October 15th, 2024 – Face-to-Face transactions (CP) 2. April 15th, 2025 – e-commerce transactions (CNP)	
	Ministerul Finanțelor	14	Textul proiectului urmează a fi redactat în contextul respectării regulilor stipulate la art.54 alin (1) din Legea 100/2017 cu privire la actele normative.	**Se acceptă**
II. Obiecții și propuneri la punctele din proiect				
Pentru aprobarea Regulamentului cu privire la autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare între prestatorii de servicii de plată În temeiul art. 5 alin. (1) lit. m), art. 11 alin. (1) și art. 27 alin. (1) lit. c) și art.49[1] alin.(2) din Legea nr. 548/1995 cu privire la Banca Națională a Moldovei (republicată în Monitorul Oficial al Republicii Moldova, 2015, nr. 297-300, art. 544) și art. 52[4] alin.(7) din Legea nr.114/2012 cu privire la serviciile de plată și moneda electronică (Monitorul Oficial al Republicii Moldova, 2012, nr. 193-197, art. 661), cu modificările ulterioare, Comitetul executiv al Băncii Naționale a Moldovei **HOTĂRĂȘTE:** **1.** Se aprobă Regulamentul cu privire la autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicate a prestatorilor de servicii de plată (se anexează).	Ministerul Justiției	15	Cu referire la temeiul juridic al actului normativ, expunem necesitatea indicării doar a temeiului juridic concret pentru emiterea actului normativ, referințe la alte acte normative și prevederi care nu constituie temei juridic de adoptare a actului normativ elaborat nu se vor indica în clauza de adoptare. În speță, temeiul legal al proiectului hotărârii „art. 5 alin. (1) lit. m), art. 11 alin. (1) și art. 27 alin. (1) lit. c) și art. 49 1a lin. (2) din Legea nr. 548/1995 cu privire la Banca Națională a Moldovei" , urmează a fi exclus, ținând cont de faptul că dispoziții care se referă la competența generală a autorității publice de a adopta acte normative în domeniul său de competență, nu constituie temei juridic de emitere.	**Se acceptă**

2. Prezenta hotărâre intră în vigoare la data de 5 august 2024.				
Prezentul regulament transpune 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 și Ghidul EBA/GL/2018/07 referitor la condițiile necesare pentru a beneficia de o exceptare de la mecanismul de urgență prevăzut la articolul 33 alineatul (6) din Regulamentul (UE) 2018/389.	Ministerul Justiției	16	Cu referire la clauza de armonizare, atenționăm că potrivit art. 44 alin. (3) din Legea nr. 100/2017 cu privire la actele normative, „(3) Clauza de armonizare indică tipul, numărul și denumirea oficială a actelor Uniunii Europene care se transpun în actul normativ, seria, numărul și data Jurnalului Oficial al Uniunii Europene în care au fost publicate actele respective, precum și măsura în care acestea sunt transpuse.”. Astfel, în contextul în care proiectul nu transpune integral actul UE, este necesară completarea clauzei de armonizare a proiectului în ceia ce privește gradul de transpunere a Regulamentul delegat (UE) 2018/389 al Comisiei precum și seria, numărul și data Jurnalului Oficial al Uniunii Europene în care a fost publicat actul UE.	**Comentariu:** Clauza de armonizare conține toate elementele enumerate.
2. Termenii, noțiunile și expresiile utilizate în prezentul regulament au semnificația celor prevăzute în lege și în alte acte normative emise de Banca Națională a Moldovei.	Ministerul Justiției	17	La pct. 2, propunem excluderea cuvântului „Termenii” având în vedere că este sinonim cu cuvântul „noțiunile”.	**Se acceptă**
3. Suplimentar, în sensul prezentului regulament sunt utilizate următoarele noțiuni: (...) Standard național de comunicare – set de specificații funcționale și tehnice, pentru interfețele specifice ale prestatorilor de servicii de plată care oferă servicii de administrare cont, care permit prestatorilor de servicii de inițiere a plății, prestatorilor de servicii de informare cu privire la conturi și prestatorilor de servicii de plată care emit instrumente de plată bazate pe card, accesul la conturile de plăți ale utilizatorilor de servicii de plată.	OTP Bank S.A.	18	La pct. 3, noțiunea ”Standard național de comunicare”, de specificat că acestea sunt aplicabile pentru prestatorii de servicii naționali și internaționali.	**Comentariu:** Acesta este standardul legat de open banking, legat de accesul la cont pentru prestatorii de servicii de inițiere a plății și prestatorii de servicii de informare cu privire la cont și vizează exclusiv comunicarea dintre prestatorii de servicii de plată din Republica Moldova.
		19	La pct. 3, propunem de definit noțiunea ”date sensibile”, ”consumator” și ”semnal temporal oficial”.	**Nu se acceptă** Noțiunea „date sensibile privind plățile” este definită în Legea nr.114/2012. Termenul „consumator” este unul consacrat și definit în Codul Civil al RM. Textul „semnal temporal oficial” este un termen specific Legii privind identificarea electronică şi serviciile de încredere nr. 124 din 19.05.2022.
4. 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 de prevenire și de limitare a operațiunilor de plată neautorizate sau frauduloase menționate la pct. 1 subpct. 1) și 2).	Ministerul Justiției	20	La pct. 4, 14, 19, 77 ș.a. abrevierea „subpct.” se va substitui cu abrevierea „sbp.”.	**Se acceptă??**

Mecanismele respective se bazează pe analiza operațiunilor de plată, având în vedere elemente specifice ale utilizatorului serviciilor de plată în condiții de utilizare normală a elementelor de securitate personalizate.				
5. Prestatorii de servicii de plată se asigură că mecanismele de monitorizare a operațiunilor sunt bazate de riscuri și iau în considerare, ca o condiție minimă, cel puțin următorii factori: 1) listele de elemente de autentificare compromise sau furate; 2) valoarea fiecărei operațiuni de plată; 3) scenariile de fraudă cunoscute în ceea ce privește furnizarea de servicii de plată; 4) indicatori privind compromiterea confidențialității, integrității sau autenticității sesiunii ca urmare a procedurii de autentificare; 5) registrul de utilizare normală și anormală a dispozitivului de acces sau a programului informatic furnizat utilizatorului serviciilor de plată de către prestatorul de servicii de plată; 6) poziția geografică anormală/neobișnuită a plătitorului; 7) poziția geografică cu risc ridicat a beneficiarului plății;	OTP Bank S.A.	21	La pct. 5, întru asigurarea conformității cu prevederile Regulamentului 2018/389, propunem micșorarea eșantionului de factori enumerați.	**Comentariu:** Factorii enumerați sunt preluați din reglementarea UE, fără a fi incluși alți factori suplimentari.
	ATIC	22	Referitor la subpct.6 - care sunt criteriile de evaluare a gradului de normalitate a poziției geografice? Va rezulta oare din acest punct situația în care utilizatorul de servicii de plată utilizează serviciul de informare cu privire la conturi fiind fizic într-un stat al UE și în momentul în care are un consimțământ valabil el va fi anulat i i se va cere repetat autentificarea strictă fiindcă administratorul de cont a considerat aceasta poziție geografică anormală/neobișnuită?	**Comentariu:** Cerința are în vedere comportamentul utilizatorului serviciilor de plată atunci când face plăți, nu în legătură cu locația în care s-a acordat consimțământ pentru prestatorul de servicii de inițiere a plății.
		23	Propuneri de modificare: *„5.Prestatorii de servicii de plată se asigură că mecanismele de monitorizare a operațiunilor sunt bazate pe ~~de~~ riscuri și iau în considerare, ca o condiție minimă, cel puțin următorii factori:”*	**Se acceptă** Cuvântul „de” va fi substituit cu cuvântul „pe”.
	“Paymaster” S.R.L.	24	Referitor la pct. 5 subpct. 1): Собственные списки или будет какой-то общий межбанковский портал ? Traducere: Liste proprii s-au va exista un fel de portal interbancar comun?	**Comentariu:** Liste proprii ale fiecărui prestator de servicii de plată, nu au cum să fie liste comune la nivel de piață fiind elemente de securitate ale fiecărui prestator de servicii de plată.
	„Paymaster” S.R.L.	25	Referitor la pct. 5 subpct. 6): Какие механизмы проверки условий закладывать в мониторинг, в случае использования VPN подключений ? Traducere: Ce mecanisme de verificare a condițiilor ar trebui incluse în monitorizare, în cazul utilizării conexiunilor VPN?	**Comentariu:** Reguli cu liste de utilizatori de servicii de plată care folosesc în mod normal VPN, iar cei care nu sunt în listă și apar că utilizează un VPN, să se genereze alerte și drept consecință confirmare suplimentară de la utilizatorul de servicii de plată.
	„Paymaster” S.R.L.	26	Referitor la pct. 5 subpct. 7):	**Comentariu:**

			Имеется ввиду список стран, предоставляемым Центром по Борьбе с Эконом.Преуступлениями и финансирования Терроризма? Или рекомендации НБМ ? Traducere: Se referă la lista de țări oferită de Centrul pentru Combaterea Crimelor Economice și Finanțării Terorismului? Sau recomandări ale BNM?	Liste care sunt stabilite de Serviciul Prevenirea și Combaterea Spălării Banilor, EUROPOL, VISA/Mastecard etc. sau țări care sunt clasificate chiar de către prestatorii de servicii de plată ca fiind cu risc.
6. Măsurile de securitate prevăzute la pct. 1 sunt documentate, testate, cel puțin odată pe an, la intervale regulate de timp, și auditate de către auditori cu experiență în domeniul securității informației și al plăților ce sunt independenți din punct de vedere operațional de prestatorul de servicii de plată. Perioada dintre auditurile menționate în prezentul punct se stabilește ținând seama de cadrul de contabilitate și de audit statutar relevant aplicabil prestatorului de servicii de plată.	OTP Bank S.A.	27	La pct. 6 prima propoziție, de revizuit necesitatea efectuării auditului anual. Propunerea o argumentăm prin necesitatea conformării cu prevederile Regulamentului 2018/389 care nu prevede o astfel de periodicitate, precum și prin excluderea exagerării numărului de audituri. În acest sens, se propune efectuarea auditului o dată la 3 ani sau la cererea BNM.	**Se acceptă**
	B.C. „Victoriabank” S.A.	28	Pct. 6, nu este clar care sunt cerințele de certificare a auditorilor în domeniul securității informației. În alte regulamente ale BNM se indică expres certificările necesare. La fel la pct. 6 nu este clar dacă acest audit trebuie să fie executat de auditul intern al băncii sau un auditor extern.	**Comentariu:** Daca auditorul intern poate face dovada îndeplinirii cerințelor de independență și experiență se poate utiliza acesta, în caz contrar este necesar un audit extern. Reglementarea are în vedere dimensiunea prestatorului de servicii de plată și regimul de proporționalitate în activitatea de supraveghere. În plus, regulamentul transpune dispozițiile Regulamentului UE 389 și nu prevede o listă a certificărilor, aceasta putând fi limitată și insuficientă în timp.
7. Prestatorii de servicii de plată care recurg la derogarea prevăzută la pct.32-35 fac obiectul unui audit, cel puțin o dată pe an, cu privire la metodologia de calculare a ratelor de fraudă, modelul utilizat în calculul ratei de fraudă și ratele de fraudă raportate, procesul de calculare a ratelor de fraude stabilit la pct. 35-37. Auditorul intern care efectuează acest audit are competențe în domeniul securității informației 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 pct. 32-35 și, ulterior, cel puțin o dată la trei ani sau mai frecvent, la cererea Băncii Naționale a Moldovei, acest audit este efectuat de către un auditor extern independent și calificat.	„Paymaster” S.R.L.	29	Referitor la „audit”: Считаю необходимым добавить «intern» для исключения неопределенности. Traducere: Consider că este necesar de adăugat „intern” pentru a elimina incertitudinea.	**Comentariu:** A se vedea pct. 28 din sinteză.
	„Paymaster” S.R.L.	30	Referitor la „auditor extern independent și calificat” какого уровня/сертификации должен быть специалист/компания ? Traducere: ce nivel/certificare ar trebui să fie un specialist/companie?	**Comentariu:** A se vedea pct. 28 din sinteză.

	Ministerul Justiției	31	Cu referire la pct. 7, propunem ca Banca Națională a Moldovei să desemneze, prin concurs, auditorului extern în vederea verificării procedurii metodologice și modelele utilizate de prestatorul de servicii de plată pentru a calcula ratele fraudelor, precum și ratele fraudelor raportate, cu respectarea principiilor asigurării concurenței, eficienței, transparenței, nediscriminării, or, potrivit normelor Constituționale consacrate la art. 126, statul trebuie să asigure libertatea comerțului și activității de întreprinzător, protecția concurenței loiale, crearea unui cadru favorabil valorificării tuturor factorilor de producție.	**Nu se acceptă** Regulamentul UE nu prevede o astfel de abordare. Auditorul extern este ales de către prestatorul de servicii de plată. Fiecare PSP trebuie să dispună de autonomie și să decidă independent privind compania ce urmează să efectueze auditul. BNM a stabilit deja (prin prezentul regulament) cerințele minime pe care compania de audit urmează să le întrunească.
		32	Punctele la care se face trimitere se vor indica prin enumerare, or, cratima se utilizează pentru a evita enumerarea a mai mult de 3 elemente structurale consecutive (observație valabilă și pentru restul trimiterilor similare).	**Se acceptă**
10. În sensul pct. 9, prestatorii de servicii de plată implementează măsuri de securitate, asigurându-se că este îndeplinită fiecare dintre următoarele cerințe: 1) nicio informație cu privire la oricare dintre elementele menționate la pct. 9 nu poate fi derivată din divulgarea codului de autentificare; 2) nu este posibilă generarea unui nou cod de autentificare bazat pe cunoașterea oricărui alt cod de autentificare generat anterior; 3) codul de autentificare nu poate fi falsificat; 4) codul poate fi utilizat o singură dată; 5) codul este valid o perioadă limitată de timp.	B.C. „Victoriabank” S.A.	33	Pct. 10, 5) considerăm că necesită o indicare expresă a termenului „codul este valid o perioadă limitată de timp”.	**Comentariu:** Fiecare prestator de servicii de plată va stabili în funcție de strategia proprie perioada de valabilitate a acestui cod.
11. Prestatorii de servicii de plată se asigură că autentificarea cu ajutorul unui cod de autentificare include fiecare dintre următoarele măsuri: 1) nu trebuie să fie posibil să se identifice care dintre elementele menționate la pct. 9 a fost incorect, 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 pct. 9; 2) numărul de încercări de autentificare eșuate care pot avea loc consecutiv, după care acțiunile menționate la art. 52^4 alin.(1) din lege sunt blocate temporar sau permanent, nu trebuie să depășească cinci într-o perioadă de 15 minute. În cazul în care blocarea 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 pct.5. În	OTP Bank S.A.	34	La pct. 11 subpct. 2), ultimele două propoziții care descriu situația de blocare permanentă se propune de indicat termenul recomandat de informare a plătitorului, precum și canalele de informare.	**Comentariu:** Se are în vedere abordarea generală de informare imediat sau în cel mai scurt timp posibil, iar canalele de informare se aleg de fiecare prestator de servicii de plată în parte în funcție de strategie și canalele disponibile (astfel de prevederi ar trebui incluse în contractul cu utilizatorul serviciilor de plată).
	Asociația Băncilor din Moldova		Pct.11 (1), nu este clar formulată măsura “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 contextul formulării enunțate nu este clar care sunt situațiile concrete aplicabile situației descrise.	**Comentariu:** Această prevedere a fost reformulată.

cazul în care blocarea a devenit permanentă, prestatorul de servicii de plată stabilește o procedură securizată care îi permite plătitorului să redobândească accesul la instrumentele electronice de plată. Plătitorul este informat înainte ca blocarea să devină permanentă; 3) sesiunile de comunicare sunt protejate împotriva capturării datelor de autentificare și împotriva manipulării de către părți neautorizate, în conformitate cu cerințele prevăzute în Capitolul V; 4) sesiunea de comunicare este invalidată dacă plătitorul nu desfășoară nicio activitate timp de cinci minute după autentificare.				
12. În cazul în care prestatorii de servicii de plată aplică autentificarea strictă a clienților în conformitate cu art. 52^4 alin.(2) din lege, în plus față de cerințele prevăzute la pct. 9-11 din prezentul regulament, aceștia adoptă și măsuri de securitate care îndeplinesc fiecare dintre cerințele următoare: 1) plătitorul este informat cu privire la valoarea operațiunii de plată și cu privire la beneficiarul plății; 2) codul de autentificare generat este specific valorii operațiunii de plată și beneficiarului plății asupra cărora plătitorul a convenit în momentul inițierii operațiunii; 3) 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; 4) orice modificare a valorii sau a beneficiarului plății duce la invalidarea codului de autentificare generat.	OTP Bank S.A.	35	La pct. 12 subpct. 1), se propune de indicat canalele de informare a plătitorului.	**Comentariu:** Canalele de informare se aleg de fiecare prestator de servicii de plată în funcție de canalele disponibile, strategie și tipul plății, spre exemplu: - La carduri – plăți online – se va afișa pe ecran înainte de autorizare; - La transfer credit – mobile banking – se va afișa în ecranul aplicației suma și beneficiarul, tot înainte de momentul autorizării.
13. În sensul pct.12, prestatorii de servicii de plată adoptă măsuri de securitate care să asigure, în toate fazele procesului de autentificare, confidențialitatea, autenticitatea, integritatea valorii operațiunii de plată, beneficiarului plății și a informațiilor afișate plătitorului, inclusiv generarea, transmiterea și utilizarea codului de autentificare.	Ministerul Finanțelor	36	Întru evitarea riscului de denaturare a sensului prevederilor art.5 alin.(2) din 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 (în continuare – Regulament UE), în transpunere, se propune expunerea pct.13 din proiect în următoarea redacție: “13. În sensul pct.12, prestatorii de servicii de plată adoptă măsuri de securitate care să asigure, în toate fazele procesului de autentificare, confidențialitatea, autenticitatea și integritatea fiecăruia dintre următoarele elemente: 1) valoarea operațiunii de plată și beneficiarului plății; 2) informațiile afișate plătitorului, inclusiv generarea, transmiterea și utilizarea codului de autentificare.”.	**Se acceptă**

14. În sensul pct. 12 subpct. 2) și în cazul în care prestatorii de servicii de plată aplică autentificarea strictă a clienților, în conformitate cu art. 52^4 alin.(2) din lege, se aplică următoarele cerințe pentru codul de autentificare: 1) 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 art. 601 alin.(1) din lege, 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; 2) în legătură cu operațiunile de plată pentru care plătitorul și-a exprimat consimțământul referitor la executarea unui lot (pachet de instrucțiuni) 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.	OTP Bank S.A.	37	La pct. 14 subpct. 2), solicităm explicarea prevederilor. În acest sens, nu este clar cum codul de autentificare aplicat pentru operațiunile de plata care conține un lot de operațiuni către mai mulți beneficiari (bulk payments si încărcat în SADD prin fișier și este autentificat cu un cod de autentificare) poate sa conțină cuantumul total al lotului de operațiuni de plată și beneficiarilor specificați ai plății. Care elemente ale operațiunilor trebuie sa conțină Codul de autentificare? Sau prestatorii de servicii de plată sunt împuterniciți să elaboreze / implementeze aceste mecanisme în baza spectrului de mecanisme/ capacitățile tehnice de care dispune și sa aplice propriile reguli și algoritme de formare a codului unic de autentificare.	**Comentariu:** În legătură cu operațiunile de plată pentru care plătitorul și-a exprimat consimțământul referitor la executarea unui lot (pachet de instrucțiuni) de operațiuni electronice de plată la distanță către unul sau mai mulți beneficiari, codul de autentificare în această situație trebuie să conțină următoarele elemente: - informații cu privire la cuantumului total al lotului de operațiuni de plată și beneficiarilor specificați ai plății.
17. Prestatorii de servicii de plată implementează 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 diminua riscul care ar rezulta din compromiterea acestui dispozitiv universal. Măsurile de atenuare includ fiecare dintre următoarele: 1) utilizarea unor medii de executare sigure, separate cu ajutorul programelor informatice instalate pe dispozitivul universal; 2) mecanisme prin care să se asigure că programele informatice sau dispozitivul nu au fost modificate de către plătitor sau de către un terț; 3) în cazul în care au avut loc modificări la nivelul sistemelor care gestionează elementele de autentificare strictă și ale codurilor de autentificare de pe dispozitivul universal, mecanisme pentru a atenua consecințele acestora.	OTP Bank S.A.	38	La pct. 17 subpct. 1), de concretizat dacă tokenul trebuie sa fie separat sau este validă și soluția cu token integrat în aplicație.	**Comentariu:** Sunt corecte ambele variante, fiecare prestator de servicii de plată va implementa ce este posibil din punct de vedere tehnic în raport cu sistemele sale, dar și cu strategia acestuia.
	Asociația Băncilor din Moldova		Pct.17, se impune o specificare/detaliere privind caracterul dispozitivului universal asupra căruia este necesar a implementa/aplica măsurile de securitate menționate la alineatele 1, 2, şi 3.	**Comentariu:** Dispozitiv universal reprezintă un dispozitiv care poate avea utilizări multiple pentru utilizatorul serviciilor de plată (de ex.: smartphone-ul).
18. Prestatorii de servicii de plată au dreptul să nu aplice autentificarea strictă a clienților, sub rezerva respectării cerințelor prevăzute la pct. 4, pct. 5 și la pct.19, în cazul în care accesul online a unui utilizator de servicii de plată este limitat, în lipsa divulgării de date sensibile privind plățile, exclusiv la una dintre următoarele două situații sau la ambele: 1) soldul unuia sau mai multor conturi de plată desemnate de către utilizator;	Ministerul Justiției	39	La pct. 18 se va ține cont că, potrivit regulilor tehnicii legislative, într-o enumerare de referințe, denumirea elementelor structurale ale actului normativ nu se repetă.	**Se acceptă**

2) operaţiunile de plată executate în ultimele 90 de zile prin intermediul unuia sau mai multor conturi de plată desemnate de utilizator.				
19. În sensul pct.18, prestatorii de servicii de plată nu sunt scutiţi de la aplicarea autentificării stricte a clienţilor în cazul în care oricare dintre următoarele condiţii este îndeplinită: 1) utilizatorul serviciilor de plată accesează online, pentru prima dată, informaţiile specificate la pct. 18; 2) s-au scurs mai mult de 90 de zile de când utilizatorul serviciilor de plată a accesat online ultima dată informaţiile menţionate la pct. 18 subpct. 2) şi de când a fost aplicată autentificarea strictă a clienţilor.	ATIC	40	Propunem 180 de zile în baza Regulamentului (UE) 2022/2360 din 3 August 2022 care amendează Regulamentul (UE) 2018/389. De asemenea, propunem completarea cu aceste amendamente cu scopul alinierii la modificările aduse de Regulamentul (UE) 2022/2360 din 3 August 2022 care amendează Regulamentul (UE) 2018/389. Propuneri de modificare: 19. În sensul pct.18, prestatorii de servicii de plată nu sunt scutiţi de la aplicarea autentificării stricte a clienţilor în cazul în care oricare dintre următoarele condiţii este îndeplinită: 1)utilizatorul serviciilor de plată accesează online, pentru prima dată, informaţiile specificate la pct. 18; 2) s-au scurs mai mult de 180 ~~90~~ de zile de când utilizatorul serviciilor de plată a accesat online ultima dată informaţiile menţionate la pct. 18 subpct. 2) şi de când a fost aplicată autentificarea strictă a clienţilor. X1. Prestatorii de servicii de plată sunt obligaţi să nu aplice autentificarea strictă a clienţilor, sub rezerva respectării cerinţelor prevăzute la pct. 4, pct. 5 şi la pct.19, în cazul în care utilizatorul de servicii de plată accesează contul său online prin intermediul unui prestator de servicii de informare cu privire la conturi şi accesul de date este limitat, în lipsa divulgării de date sensibile privind plăţile, exclusiv la una dintre următoarele două situaţii sau la ambele: 1)soldul unuia sau mai multor conturi de plată desemnate de către utilizator; 2)operaţiunile de plată executate în ultimele 90 de zile prin intermediul unui sau a mai multor conturi de plată desemnate de utilizator. X2. În sensul pct. X1, prestatorii de servicii de plată nu sunt scutiţi de la aplicarea autentificării stricte a clienţilor în cazul în care oricare dintre următoarele condiţii este îndeplinită: 1)utilizatorul serviciilor de plată accesează online, pentru prima dată, informaţiile specificate la pct. X1; 2)s-au scurs mai mult de 180 de zile de când utilizatorul serviciilor de plată a accesat online ultima dată informaţiile menţionate la pct. X1 subpct. 2) prin intermediul unui prestator de servicii de informare cu privire la conturi şi de când a fost aplicată autentificarea strictă a clienţilor. ~~2)~~ XX. Prin derogare de la pct. 18, prestatorii de servicii de plată pot să aplice autentificarea strictă a clienţilor în cazul în care utilizatorul de servicii de plată îşi accesează informaţia cu privire la conturi prin intermediul unui	**Se acceptă parţial**

			prestator de servicii de informare cu privire la conturi și prestatorul de servicii de plată are dovezi clare și obiectiv jusitificate a faptului de acces fraudulos sau neautorizat la contul de plată al utilizatorului de servicii de plată. În acest caz, prestatorul de plată va documenta aceste cazuri și va demonstra motivele de aplicare a autentificării stricte la cererea Băncii Naționale.	
24. Prestatorii de servicii de plată au dreptul să nu aplice autentificarea strictă a clienților, sub rezerva/cu condiția respectării cerințelor prevăzute la pct.4 și 5, în cazul în care plătitorul inițiază o operațiune electronică de plată contactless prin intermediul unui instrument de plată cu o funcționalitate contactless valoarea individuală a operațiunii electronice de plată contactless nu depășește 1000 lei ori echivalentul în valută străină la cursul oficial al leului moldovenesc dacă se asigură una din următoarele condiții: 1) valoarea cumulată a operațiunilor electronice de plată contactless, inițiate de un plătitor de la data ultimei aplicări a autentificării stricte a clienților nu depășește 3000 lei ori echivalentul în valută străină la cursul oficial al leului moldovenesc; 2) numărul operațiunilor electronice de plată contactless consecutive inițiate de la data ultimei aplicări a autentificării stricte a nu este mai mare de cinci.	VISA	41	Raising contactless limits on terminals at point of sales: We recommend a review of the current thresholds of setting the maximum per transaction and cumulative limits before SCA must be applied for contactless transactions, giving industry the flexibility to set higher limits in their respective countries.	**Comentariu:** Considerăm necesară menținerea limitelor prevăzute în Regulamentul UE 2018/389 pentru transpunerea fidelă. La fel, în acest sens, a fost efectuată o analiză, fiind chestionați toți prestatorii de servicii de plată, însă aceștia au susținut limitele actuale.
	B.C. „Victoriabank" S.A.	42	Pct. 20, considerăm necesară precizarea dacă PIN-ul aferent cardului se consideră element de autentificare strictă.	**Comentariu:** Elementele de autentificare strictă conforme cu prezentul proiect de regulament pot fi găsite accesând următorul document UE, acestea fiind clasificate în funcție de categorie: Link: Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2
	B.C. Comertbank S.A.	43	Pornind de la faptul că, cardurile de plată ca instrument de plată, sunt în circulație în Republica Moldova și peste hotare, se propune ca în pct. 20 al regulamentului să fie introduse următoarele modificări legate de aspecte importante care sunt aplicate și folosite în domeniul cardurilor cu succes, și anume: 1. se propune modificările în pct. 20 și pct. 20 subpct. 1) cu privire la cursul valutar pentru operațiunile cu carduri de plată prin utilizarea cursului comercial al băncii setat pentru operațiuni cu carduri de plată, în loc de „cursul oficial al leului moldovenesc". Argumentare: în domeniul de carduri, la utilizarea unui instrument de plată – card de plată, pentru tranzacțiile efectuate în altă valută decât contul de card, convertirea se efectuează prin aplicarea cursului valutar setat pentru operațiunile cu carduri de plată al băncii-emitent și Sistemelor Internaționale de Plăți, după caz. Clienții – deținători de carduri de plată înțeleg și sunt de acord cu aplicarea cursurilor asociate tranzacțiilor de carduri. Respectiv, suma care se debitează de pe contul de card se calculează conform cursului comercial pentru operațiunile cu carduri de plată. Utilizarea cursului oficial al leului moldovenesc în acest flux operațional va	**Se acceptă** Punctul 20 urmează a fi modificat, prin excluderea textului „la cursul oficial al leului moldovenesc".

			complica metodologia și setările care sunt aplicate la moment, la nivel de sisteme automatizate ale băncilor, centrelor de procesare și va crea necesitatea clarificărilor și explicațiilor suplimentare pentru deținătorii cardurilor de plată, care folosesc cardul în fiecare zi. Totodată, utilizarea a două tipuri de cursuri va complica fluxul operațional pentru operațiunile de card.	
		44	Se propun modificări în pct. 20 subpct. 1) cu privire la valoarea cumulată a operațiunilor electronice de plată contactless, inițiate de un plătitor de la data ultimei aplicări a autentificării stricte a clienților, care nu depășește 3000 lei prin modificarea sumei în 5000 lei. Argumentare: dacă în pct. 20 suppct. 2) este stipulat că numărul operațiunilor electronice de plată contactless consecutive inițiate de la data ultimei aplicări a autentificării stricte nu este mai mare de cinci și suma maximă a unei operațiuni contactless nu va depăși 1000 lei, respectiv valoarea cumulată a operaţiunilor electronice de plată contactless prin intermediul unui instrument de plată propunem să fie 5000 lei (5*1000).	**Comentariu:** Aceste două subpuncte nu sunt cumulative, prestatorii de servicii de plată trebuie să decidă pe care dintre acesta îl implementează ca măsură suplimentară pentru plățile contactless.

		45	Se propun modificările în pct. 20 subpct. 2) cu privire la numărul operațiunilor electronice de plată contactless consecutive inițiate de la data ultimei aplicări a autentificării stricte nu este mai mare de cinci prin adăugarea sintagmei la sfârșitul propoziției „per zi”. Argumentare: la moment se utilizează cu succes practica de 5-7 tranzacții per zi prin metoda contactless fără introducerea codului PIN la cardurile de plată. Astfel, în contextul celor menționate, se propune următoarea expunere a pct. 20: *„20. Prestatorii de servicii de plată au dreptul să nu aplice autentificarea strictă a clienților, sub rezerva/ cu condiția respectării cerințelor prevăzute la pct. 4 și 5, în cazul în care plătitorul inițiază o operațiune electronică de plată contactless prin intermediul unui instrument de plată cu o funcționalitate contactless valoarea individuală a operațiunii electronice de plată contactless nu depășește 1000 lei ori echivalentul în valută străină la cursul comercial al băncii setat pentru operațiuni cu carduri de plată dacă se asigură una din următoarele condiții:* *1) valoarea cumulată a operațiunilor electronice de plată contacltess, inițiate de un plătitor de la data ultimei aplicări a autentificării stricte a clienților nu depășește 5000 lei ori echivalentul în valută străină la cursul comercial al băncii setat pentru operațiuni cu carduri de plată;* *2) numărul operațiunilor electronice de plată contactless consecutive inițiate de la data ultimei aplicări a autentificării stricte nu este mai mare de cinci per zi.”*	**Comentariu:** Aceste situații sunt excepții, dacă un prestator de servicii de plată consideră că tranzacțiile contactless au un risc de fraudă mare pot stabili alte măsuri de securitate mai stricte decât cele prevăzute de Regulament (respectiv cele menționate de bancă). Atenție, schemele vor stabili prin reguli conforme cu Regulamentul 389 pentru a încuraja plățile contactless.
	Î.S.„Poșta Moldovei”	46	În pct. 20 este utilizată noțiunea „contactless” care nu este definită în proiectul Regulamentului și nici în Legea nr.114/2012. Considerăm necesară completarea pct.3 cu definiția acestei noțiuni.	**Comentariu:** Aceasta este o noțiune consacrată care nu trebuie definită (a se vedea regulile schemelor cu card).
		47	La pct. 20 subpct. 2) sintagma „autentificării stricte ~~a~~ nu este mai mare de cinci” de substituit cu sintagma „autentificării stricte nu este mai mare de cinci”.	**Se acceptă**
	Asociația Băncilor din Moldova	48	Capitolul III, pct. 20, estimăm ca restricțiile/limitele urmează a fi setate global de către sistemele de plăți VISA/Mastercard pentru cardurile emise în Repulica Moldova asociate tranzacțiilor contactless efectuate la POS terminale, inclusiv pentru plățile contactless de tip Apple Pay/Google Pay. Context în care prevederile proiectului de Regulament determină un impact pentru toți prestatorii de servicii de plată din Republica Moldova, astfel încât devine oportun/eficient ca limitările	**Comentariu:** Băncile și alți prestatori de servicii de plată, fiind subiecți al acestui proiect, vor urma să respecte prevederile acestuia și, respectiv, vor negocia resetările cu sistemele în care participă.

			respective să fie setate și testate de către sistemele de plăți VISA/Mastercard, decât de către fiecare bancă în parte.	
	Mastecard	49	Require time for technical implementation on ISS and ACQ/Merchants sides	Comentariu: Prezentul proiect de regulament a fost publicat pentru consultări publice pe data de 06.03.2023, iar intrarea în vigoarea a acestuia este prevăzută pentru data de 5 august 2024. Astfel, considerăm că este suficient timp pentru toți actorii pieței să depună eforturi în sensul pregătirii pentru conformare cu prevederile regulamentului (fiind o perioada similară cu cea alocata pentru piața UE). Mai mult ca atât, cât timp Mastercard este prezenta inclusiv pe piața UE, aceasta are experiența și pregătirea tehnică pentru a implementa SCA inclusiv pe piața din RM.
25. Prestatorii de servicii de plată au dreptul să nu aplice autentificarea strictă a clienților, sub rezerva respectării cerințelor prevăzute la pct. 4 și 5, în cazul în care plătitorul inițiază o operațiune electronică de plată la un terminal de plată neasistat (automate de plată neasistate), cu scopul de a plăti un bilet de transport sau o taxă de parcare.	Mastecard	50	Unattended terminals are defined as terminals for Transport or Parking. Proposition: Exclude the words combinations “a transport fare or a parking fee”. Define as for all unattended terminals.	**Comentariu:** Actualmente, nu există noțiune de terminal/automat neasistat. Totodată, regulamentul UE are drept scop aplicarea acestei exceptii de la implementarea SCA strict pentru terminalele neasistate pentru biletele de transport si taxele de parcare.
26. Prestatorii de servicii de plată urmează să aplice 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.	„Paymaster” S.R.L.	51	Пункт 22 «... când plătitorul creează sau modifică o listă a beneficiarilor agreați prin ...» что имеется ввиду ? Не совсем понятна формулировка. Зачем, как и когда? Перед началом изменения или при сохранении изменения ? Речь о шаблонах или запланированных платежах ? Traducere: Ce înseamnă ? Formularea nu este clară. De ce, cum și când? Înainte de a începe modificarea sau când salvați modificarea? Avem în vedere șabloane sau plăți programate?	**Comentariu:** Despre listele de beneficiari agreați către care se pot face ulterior plăți fără SCA, iar procesul de creare a acestor liste sau de modificare trebuie să fie cu SCA.
27. Prestatorii de servicii de plată au dreptul să nu aplice autentificarea strictă a clienților 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.	OTP Bank S.A.	52	La pct. 23, se solicită concretizarea cazurilor în care derogarea menționată la pct.23 poate fi aplicata beneficiarilor: beneficiarilor creați si salvați anterior de către plătitor sub forma ordinelor de plată de tip "Sablon"	**Comentariu:** Această situație este una nouă și care presupune că USP poate crea o listă de beneficiari agreați către care să facă ulterior plăți fără SCA și nu

			sau beneficiarilor creaţi si salvaţi în modulul separat creat în SADD de tip "Lista Beneficiari". Totodată, de concretizat faptul dacă aceasta derogare se aplică şi beneficiarilor creaţi / existenţi la alt prestator de servicii de plată în contextul conceptului de "open - banking", şi anume, plata este iniţiată de către plătitor la prestatorul de servicii de iniţiere a plăţii şi Ordinul de plată executat de către prestatorul de servicii de plată.	cum este azi o listă cu datele acestora, pentru a elimina povara introducerii datelor. Orice modificare a listei create în temeiul pct. 23 trebuie să se realizeze cu SCA, la fel şi crearea acesteia.
		53	La pct. 23-27, pentru asigurarea unui nivel de securitate mai înalt, se propune de specificat ca orice plată iniţiata în Internet Banking să fie validată de plătitor.	**Comentariu:** Pct. 23-27 au în vedere situaţii de excepţie pe care prestatorii de servicii de plată le pot implementa dacă apreciază oportun, în cazul în care nu le implementează trebuie să aplice autentificarea strictă a clienţilor (SCA), conform acestui regulament şi Legii nr.114/2012.
	Ministerul Finanţelor	54	La pct.23, după textul "să nu aplice autentificarea strictă a clienţilor" să se completeze cu textul "sub rezerva respectării cerinţelor generale în materie de autentificare", pentru a corespunde prevederilor art.13 alin.(2) din Regulament UE.	**Se acceptă**
	Asociaţia Băncilor din Moldova	55	Capitolul III, pct. 23, prin fraza "beneficiarul plăţii se află pe o listă a beneficiarilor agreaţi creată anterior de către plătitor" se are în vedere/se consideră lista de beneficiari salvaţi de către clienţii băncii în sistemele de autodeservire la distanţă Ebanking şi Mobile Banking?. Se impune specificare în textul regulamentului.	**Comentariu:** Prin beneficiar agreat nu se are în vedere cel salvat automat de către bancă. Această situaţie este una nouă şi care presupune că USP poate crea o listă de beneficiari agreaţi către care să facă ulterior plăţi fără SCA şi nu cum este azi o listă cu datele acestora, pentru a elimina povara introducerii datelor. Orice modificare a listei create în temeiul pct. 23 trebuie să se realizeze cu aplicarea SCA de către utilizator, la fel şi crearea acesteia.
	Mastecard	56	Need to be more clarified, is not define clear and is too complicated for implementation on ISS and ACQ/Merchants sides.	**Comentariu:** Prezenta normă are acelaşi sens ca şi art.13 din Regulamentul UE 2018/389, care este respectată de către Mastercard şi participanţii ei de pe piaţa europeană.
28. Prestatorii de servicii de plată aplică autentificarea strictă a clienţilor atunci când un plătitor creează, modifică sau iniţiază pentru prima dată o serie de operaţiuni recurente cu aceeaşi valoare şi cu acelaşi beneficiar al plăţii.	Asociaţia Băncilor din Moldova	57	Capitolul III, pct. 24, începând cu ce număr pentru astfel de plăţi recurente banca va urma să aplice autentificarea strictă a clienţilor? Se sugerează a indica numărul pentru asemenea tipuri de plăţi.	**Comentariu:** SCA se va aplica doar la crearea, modificarea sau iniţierea pentru prima dată.

29. Prestatorii de servicii de plată au dreptul să nu aplice autentificarea strictă a clienților în cazul în care se 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.	Î.S.„Poșta Moldovei”	58	La pct. 26, sintagma „care administrează contul” de substituit cu sintagma „care administrează aceste conturi”, deoarece prevederea se referă două conturi.	**Nu se acceptă** Denumirea recunoscută de Legea 114 este PSP care administrează contul de plăți.
	OTP Bank S.A.	59	În contextul prevederilor pct. 26, propunem autorului de specificat dacă Prestatorul are dreptul să aplice autentificarea strictă by default la toate operațiunile de transfer, inclusiv și în cazul când plătitorul și beneficiarul plății este aceeași persoană, iar ambele conturi de plăți sunt deținute de același prestator de servicii de plată.	**Comentariu:** Această practică se poate implementa, dacă prestatorul de servicii de plată apreciază că astfel de operațiuni implică un risc de fraudă care nu este acceptat de acesta, norma stabilește ca situație de excepție de la aplicarea SCA pentru astfel de plăți, având în vedere riscul redus de fraudă („nu mă fraudez pe mine”).
	Ministerul Finanțelor	60	La pct. 26, după textul “să nu aplice autentificarea strictă a clienților” să se completeze cu textul “sub rezerva respectării cerințelor prevăzute la pct.4 și pct.5,”, pentru a corespunde prevederilor art.15 din Regulamentul UE.	**Se acceptă**
31. 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 în valoare ce nu depășește 600 lei ori echivalentul în valută străină la cursul oficial al leului moldovenesc care întrunește una din următoarele condiții: 1) valoarea cumulată a operațiunilor electronice de plată la distanță inițiate de un plătitor de la ultima aplicare a autentificării stricte nu depășește 2000 lei ori echivalentul în valută străină la cursul oficial al leului moldovenesc; 2) numărul operațiunilor electronice de plată la distanță inițiate de plătitor de la ultima aplicare a autentificării stricte a clienților nu depășește 5 astfel de operațiuni individuale consecutive.	Asociația Băncilor din Moldova	61	Capitolul III, pct. 27, nu este evident/explicit - restrictiile/limitele menționate se vor aplica separat per tip de sistem de autodeservire la distanță sau cumulativ pentru ambele sisteme de autodeservire la distanță? Exemplu: clientul băncii, pe parcursul săptămânii, efectuează transferuri atât prin intermediul Ebanking cât și prin intermediul Mobile Banking. În context, apare o neclaritate, cum vor fi cuantificate limitele? Cuantificarea se va face separat per sistem de autodeservire la distanță sau cumulativ pentru ambele dintre cele enunțate?	**Comentariu:** Având în vedere noțiunea de operațiune de plată inițiată la distanță, exceptarea se va aplica cumulativ pentru toate tipurile de plăți inițiate prin intermediul internetului sau prin intermediul unui dispozitiv care poate fi folosit pentru comunicație la distanță.
	Mastecard	62	Require time for technical implementation on ISS and ACQ/Merchants sides	Comentariu: Prezentul proiect de regulament a fost publicat pentru consultări publice pe data de 06.03.2023, iar intrarea în vigoarea a acestuia este prevăzută pentru data de 5 august 2024. Astfel, considerăm că este suficient timp pentru toți actorii pieței să depună eforturi în sensul pregătirii pentru conformare cu prevederile regulamentului (fiind o perioada similară cu cea alocată pentru piața UE). Mai mult ca atât, cât timp Mastercard este prezenta inclusiv pe piața UE, aceasta are experiența și pregătirea tehnică pentru a implementa SCA inclusiv pe piața din RM.
32. Prestatorii de servicii de plată au dreptul să nu aplice autentificarea strictă a clienților în ceea ce	Ministerul Justiției	63	Având în vedere că pct. 1 prevede varianta scurtă (lege) a Legii cu privire la serviciile de plată și moneda electronică	**Se acceptă**

privește persoanele juridice care inițiază operațiuni electronice de plată prin utilizarea unor modalități de plată specifice ce sunt puse doar la dispoziția plătitorilor ce nu sunt consumatori, în cazul în care Banca Națională a Moldovei consideră că aceste procese sau protocoale garantează niveluri de securitate cel puțin echivalente cu cele prevăzute în Legea nr.114/2012. Pentru a beneficia de excepția de la obligația aplicării autentificării stricte a clienților, este necesar ca prestatorii de servicii de plată, care pun la dispoziția clienților modalități de plată specifice utilizate exclusiv de persoanele care nu sunt consumatori, să solicite de la Banca Națională a Moldovei acordarea acestei excepții.			nr. 114/2012, se va revizui în acest context proiectul (pct. 28, pct. 31 etc.).	
	Asociația Băncilor din Moldova	64	Capitolul III, pct. 28, se impun exemple pentru asemenea tipuri de plăți.(..modalități de plată specifice ce sunt puse doar la dispoziția plătitorilor ce nu sunt consumatori).	**Comentariu:** Se are în vedere orice operațiuni de plată efectuate de persoane juridice, dar specifice prin nivelul lor înalt al securității. A se vedea pct.29-31 din proiectul regulamentului.
	Asociația Băncilor din Moldova		Pct.28, nu există o claritate asupra tipului de plăți specificate (modalități de plată specifice ce sunt puse doar la dispoziția plătitorilor ce nu sunt consumatori)?	**Comentariu:** A fost modificat textul „modalități de plată specifice” în „procese sau protocoale de plată specifice”. De asemenea, a se vedea comentariul de la nr. 64 din sinteză.
34. Pentru a evalua și monitoriza conformarea prestatorilor de servicii de plată cu cerințele pct. 28, Banca Națională a Moldovei va lua în considerare ratele de fraudă înregistrate de prestatorii de servicii de plată în cauză. Rata fraudelor se va calcula raportând: 1) Valoarea cumulată a operațiunilor de plată efectuate la distanță considerate frauduloase, pentru care s-a aplicat autentificarea strictă și a operațiunilor de plată sau efectuate prin utilizarea unor procese sau protocoale de plată specifice care sunt puse la dispoziția plătitorilor ce nu sunt consumatori, la valoarea totală a operațiunii de plată efectuate la distanță, indiferent dacă s-a aplicat autentificarea strictă sau executate prin utilizarea proceselor sau protocoalelor de plată specifice care sunt puse la dispoziția plătitorilor ce nu sunt consumatori. Se vor include toate operațiunile de plată frauduloase, indiferent dacă fondurile au fost recuperate sau nu. Calculul se va efectua pe o bază trimestrială, iar cursul de referință utilizat pentru conversii valutare va fi cursul mediu de referință al Băncii Naționale a Moldovei din trimestrul pentru care se calculează ratele de fraudă.	Î.S. „Poșta Moldovei”	65	La pct. 30, după cuvintele „autentificarea strictă” de completat cu cuvintele „a clienților”, așa cum e specificat în pct. 28.	**Se acceptă**
36. În scopul acordării excepției menționate la pct. 28, prestatorul de servicii de plată trebuie să prezinte Băncii Naționale a Moldovei următoarele: 1) Un raport de audit detaliat care să conțină rezultatele evaluării conformității a modalităților de plată specifice care să releve conformitatea proceselor și protocoalelor de plată specifice cu cerințele stabilite la art. 32^1 și 32^2 din Legea nr. 114/2012 cu privire la serviciile de plată și	OTP Bank S.A.	66	La pct. 31 subpct. 2), propoziția a doua, se propune de exclus necesitatea raportării trimestriale către BNM a nivelului ratei de fraudă. Această obligație nu este prevăzută nici în Regulamentul UE 2018/389. Ca soluție de alternativă se propune raportarea la cerere.	**Comentariu:** Raportarea trimestrială reprezintă un element necesar în activitatea de monitorizare care indică robustețea mecanismului de autentificare implementat pentru care a fost acordată excepția.

moneda electronică, şi cerinţele regulatorii aplicabile din prezentul regulament şi din Regulamentul privind măsurile de securitate referitoare la riscurile operaţionale şi de securitate aferente serviciilor de plată. Pentru a demonstra conformarea cu prevederile pct. 6-8 din regulament din perspectiva cerinţelor instituite de prevederile acestui articol pentru auditor, prestatorii de servicii de plată solicitanţi trebuie să transmită Băncii Naţionale a Moldovei o declaraţie pe proprie răspundere a persoanei care a auditat procesele sau protocoalelor de plată specifice (ca parte a sistemului IT al prestatorului de servicii de plată sau independent) referitoare la independenţa sa operaţională faţă de prestatorul de servicii de plată şi certificările în domeniul securităţii IT deţinute, precum şi expertiza în domeniul plăţilor; 2) Nivelul ratei de fraudă pentru operaţiunile de plată iniţiate prin intermediul modalităţilor de plată specifice. Acestea se vor raporta Băncii Naţionale a Moldovei trimestrial.	B.C. „Victoriabank" S.A.	67	Pct. 31 subpct. 1) se face referinţă la Regulamentul privind măsurile de securitate referitoare la riscurile operaţionale şi de securitate aferente serviciilor de plată, un astfel de regulament nu a putut fi identificat.	**Comentariu:** Această reglementare urmează a fi supusă consultărilor publice în viitorul apropiat şi derivă din art. 32^1 şi 32^2 din Legea nr. 114/2012 cu privire la serviciile de plată şi moneda electronică.
	Î.S. „Poşta Moldovei"	68	La pct. 31 subpct. 1): - sintagma „Legea nr. 114/2012 cu privire la serviciile de plată şi moneda electronică" de substituit cu cuvântul „lege", aşa cum s-a stabilit în pct. 1; - sintagma „pct. 6-8 din regulament" de substituit cu sintagma „pct. 6-8 din prezentul regulament", deoarece se referă la acest regulament; - sintagma „acestui articol" de substituit cu sintagma „acestor articole", deoarece se referă la două art. 321 şi 322 din lege.	**Se acceptă**
	Asociaţia Băncilor din Moldova		Pct.31, se impune claritate asupra cerinţelor exacte privind auditorul care va efectua analiza menţionată în alineatul 1, poate fi auditor intern cu certificările corespunzătoare sau se impune obligativitatea unui audit extern?	**Comentariu:** Raportul de audit va trebui să fie elaborat de către un auditor intern, care să aibă experienţă în domeniul securităţii informatice şi al plăţilor şi să fie independent din punct de vedere operaţional de prestatorul de servicii de plată.
42. Prestatorii de servicii de plată au dreptul să nu aplice autentificarea strictă a clienţilor în cazul în care plătitorul iniţiază o operaţiune electronică de plată la distanţă care este identificată de către prestatorul de servicii de plată ca prezentând un nivel scăzut de risc în conformitate cu mecanismele de monitorizare a operaţiunilor implementate.	Ministerul Finanţelor	69	La pct. 32 cuvântul "implementate" să se substituie cu textul "menţionate la pct.4, pct.5 şi pct.33 subpct.3)", pentru a corespunde prevederilor art.18 alin.(1) din Regulamentul UE.	**Se acceptă**
	Mastecard	70	Need to be more clarified, is not define clear. Chapter III , we propose to review based on existing process or have a joint call for clarification.	A se vedea comentariul de la următorul punct (pct.33).
43. Se consideră că operaţiunile electronice de plată prezintă un nivel scăzut de risc în cazul în care sunt îndeplinite toate condiţiile următoare: 1) Rata de fraudă pentru un tip de operaţiuni, raportată de către prestatorul de servicii de plată şi calculată în conformitate cu pct.35-37, este egală sau mai mică decât rata de referinţă a fraudelor specificată în tabelul prevăzut în anexa nr.1; 2) valoarea operaţiunii nu depăşeşte valoarea relevantă a pragului de derogare menţionată în tabelul din anexa nr.1; 3) prestatorii de servicii de plată, în urma realizării unei analize de risc în timp real, mecanismele de monitorizare a operaţiunilor nu au identificat niciunul dintre următoarele elemente:	VISA	71	Clarifying fraud rate calculations: We believe further clarity is needed on the calculation of fraud rates. Payment service providers should only include in the fraud calculation the fraudulent transactions for which it is solely liable and have the flexibility to define what constitutes a "low risk" payment transaction.	**Comentariu:** Considerăm că textul prevederii urmează a fi păstrat, astfel cum prevede expres Regulamentul UE 2018/389, pentru a fi conform cadrului UE în sensul calculării ratelor de fraudă.
	„Paymaster" S.R.L.	72	Для пункта 33. 3) - должна быть другая субнумерация для пункта «3)» так как идет перечисление. Надо прописать, например 3.1.), 3.2.) ... или a), b), c) и d) Traducere: Pentru articolul 33. 3) - ar trebui să existe o subnumerotare diferită pentru articolul „3)", deoarece	**Se acceptă**

4) cheltuieli anormale sau un model anormal de comportament al plătitorului; 5) informații neobișnuite cu privire la accesul plătitorului la dispozitiv/programul informatic; 6) infectarea cu programe malware în oricare sesiune din procedura de autentificare; 7) scenarii de fraudă cunoscute în ceea ce privește furnizarea de servicii de plată.			transferul este în curs. Este necesar să scrieți, de exemplu, 3.1.), 3.2.) ... sau a), b), c) și d).	
	Î.S.„Poșta Moldovei”	73	Pct. 33, din context, trebuie să conţină trei subpuncte, dar nu şapte, iar subpunctul 3) trebuie să conţină 4 elemente: „a) cheltuieli anormale sau un model anormal de comportament al plătitorului; b) informaţii neobişnuite cu privire la accesul plătitorului la dispozitiv/programul informatic; c) infectarea cu programe malware în oricare sesiune din procedura de autentificare; d) scenarii de fraudă cunoscute în ceea ce priveşte furnizarea de servicii de plată.”.	**Se acceptă**
	Ministerul Finanțelor	74	Întru asigurarea obligativității luării în considerare a factorilor bazaţi pe riscuri de către prestatorii de servicii de plată care intenţionează să scutească operaţiunile electronice de plată la distanţă de la autentificarea strictă a clienţilor, se consideră oportun transpunerea şi a prevederilor art.18 alin (3) din Regulamentul UE, întrucât acestea nu se regăsesc în proiect.	**Comentariu:** Art. 18 alin. (3) din Regulamentul UE se regăsește la pct. 5 din proiectul regulamentului.
	Asociația Băncilor din Moldova		Formularea de la pct.33 (6) este una confuză, creând impresia că acest alineat (6) este în contradicție cu formularea expusă în pct. 33.	**Comentariu:** Această confuzie este una de natură redacțională/ de structură. Prin urmare, pct.33 a fost ajustat din punct de vedere structural. A se vedea propunerea și comentariul de la nr. 73 din sinteză.
45. Pentru fiecare tip de operațiune menționată în tabelul din anexa nr.1, prestatorul serviciilor de plată se asigură că ratele globale ale fraudelor pentru toate tipurile de operațiuni de plată.	B.C. „Victoriabank” S.A.	75	La pct. 35 nu este clară formularea.	**Se acceptă** Acest punct va avea următoarea redacție: 45. Pentru fiecare tip de operațiune prevăzută în tabelul din anexa nr.1, prestatorul de servicii de plată se asigură că ratele globale ale fraudelor pentru toate tipurile de operațiuni de plată sunt echivalente sau nu depășesc valorile ratelor de referință ale fraudelor pentru același tip de operațiune de plată indicată în tabelul din anexa nr.1.
	Î.S.„Poșta Moldovei”	76	La pct. 35 și 76 sintagma „prestatorul serviciilor de plată” de substituit cu sintagma „prestatorul de servicii de plată”, precum e definit în Legea nr.114/2012.	**Nu se acceptă**
	Ministerul Finanțelor	77	Pct. 35, să se completeze la final cu textul “sunt echivalente sau inferioare ratelor de referinţă ale fraudelor pentru acelaşi tip de operaţiune de plată	**Se acceptă**

			indicată în tabelul din anexa nr.1", întru redarea exhaustivă a prevederilor art.19 alin.(1) din Regulamentul UE.	
	Asociaţia Băncilor din Moldova	78	Capitolul III, pct. 35, se creează impresia că fraza nu este finisată, enunţul acesteia nefiind definitivat, impunându-se o claritate pentru conţinut.	**Se acceptă** Acest punct va avea următoarea redacţie: 45. Pentru fiecare tip de operaţiune prevăzută în tabelul din anexa nr.1, prestatorul de servicii de plată se asigură că ratele globale ale fraudelor pentru toate tipurile de operaţiuni de plată sunt echivalente sau nu depăşesc valorile ratelor de referinţă ale fraudelor pentru acelaşi tip de operaţiune de plată indicată în tabelul din anexa nr.1.
	Mastecard	79	Comment: Should be reviewing on compliance with EU SCA/Article 19. Calculation of fraud rates. 1.For each type of transaction referred to in the table set out in the Annex, the payment service provider shall ensure that the overall fraud rates covering both payment transactions authenticated through strong customer authentication and those executed under any of the exemptions referred to in Articles 13 to 18 are equivalent to, or lower than, the reference fraud rate for the same type of payment transaction indicated in the table set out in the Annex.	**Se acceptă** A se vedea comentariile de mai sus.
46. Rata globală a fraudelor pentru fiecare tip de operaţiune se calculează trimestrial ca fiind valoarea totală a operaţiunilor la distanţă neautorizate sau frauduloase, indiferent dacă fondurile au fost recuperate sau nu, împărţită la valoarea totală a tuturor operaţiunilor la distanţă de acelaşi tip.	Mastecard	80	Comment: Should be reviewing on compliance with EU SCA/Article 19. Calculation of fraud rates. "The overall fraud rate for each type of transaction shall be calculated as the total value of unauthorised or fraudulent remote transactions, whether the funds have been recovered or not, divided by the total value of all remote transactions for the same type of transactions, whether authenticated with the application of strong customer authentication or executed under any exemption referred to in Articles 13 to 18 on a rolling quarterly basis (90 days)."	**Comentariu:** Textul exclus din prevedere nu modifică sensul acesteia, având în vedere că la începutul prevederii este specificat că "pentru fiecare tip de operaţiune", ce ar include în sine operaţiunile cu SCA şi operaţiunile derogate.
53. Prestatorii de servicii de plată asigură confidenţialitatea şi integritatea elementelor de securitate personalizate ale utilizatorilor serviciilor de plată, inclusiv a codurilor de autentificare, în toate fazele autentificării implementând cel puţin următoarele cerinţe: 1) elementele de securitate personalizate sunt mascate pe măsura introducerii de către utilizatorul serviciilor de plată în cursul autentificării; 2) elementele de securitate personalizate în formatul datelor şi materialele criptografice legate de criptarea	Î.S. „Poşta Moldovei"	81	La pct. 42 subpct. 5) prevederea: „în conformitate cu standarde profesionale solide şi recunoscute pe scară largă" este ambiguă şi nu este în conformitate cu prevederea din Legea nr.114/2012. Astfel, în articolul 52^4 alineatul (7) din Legea nr.114/2912 se stipulează: „Prevederi suplimentare privind autentificarea strictă a clienţilor şi privind standardele deschise, comune şi sigure de comunicaţie care trebuie să fie aplicate de prestatorii de servicii de plată se stabilesc în actele normative ale Băncii Naţionale.". Deci, în proiectul regulamentului este necesar de a nominaliza standardele	**Comentariu:** Articolul indicat face referire la modul de prelucrare a datelor, respectiv, conform cu standardele internaţionale (pot să fie stabilite de schemă, de sistemul de plăţi, de bancă).

elementelor de securitate personalizate nu sunt stocate în text simplu; 3) materialele criptografice secrete sunt protejate împotriva divulgării neautorizate; 4) elementele de securitate personalizate sunt create într-un mediu sigur. Aceştia implementează măsuri de diminuare a riscurilor utilizării neautorizate a elementelor de securitate personalizate, dispozitivelor, sau aplicaţiilor informatice utilizate pentru autentificare; 5) prelucrarea şi transmiterea elementelor de securitate personalizate şi a codurilor de autentificare generate în conformitate cu Capitolul II au loc în medii sigure, în conformitate cu standarde profesionale solide şi recunoscute pe scară largă; 6) transmiterea elementelor de securitate personalizate şi a dispozitivelor şi programelor informatice de autentificare către utilizatorul serviciilor de plată se desfăşoară în condiţii de siguranţă menite să combată riscurile legate de utilizarea neautorizată a acestora în urma pierderii, furtului sau copierii lor. În acest sens, prestatorii de servicii de plată pun în aplicare, ca o cerinţă minimă, fiecare dintre următoarele măsuri: a) mecanisme de transmitere eficace şi sigure, care să garanteze că elementele de securitate personalizate şi dispozitivele şi 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) dispoziţii 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 distanţă: - nicio parte neautorizată nu poate obţine 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 aceluiaşi canal; - elementele de securitate personalizate sau dispozitivele ori programele informatice de autentificare transmise trebuie activate înainte de utilizare; d) dispoziţii 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 menţionate la pct. 43.			comune şi sigure de comunicaţie sau de a face trimitere la actele normative respective ale Băncii Naţionale.	
	OTP Bank S.A.	82	La pct. 42 subpct. 6) lit. d) de specificat dacă în cazul în care prestatorul de servicii de plată va selecta un program informatic de autentificare de tip „embedded” sau „incorporat” în SADD, se permite ca acest program informatic sa fie activat simultan cu aplicaţia SADD sau etapele de activare a programelor informatice de autentificare trebuie sa urmeze strict paşii descrişi în regulament.	**Comentariu:** Punctul 42 prevede obligaţiile prestatorului de servicii de plată în sensul asigurării confidenţialităţii şi integrităţii datelor, indiferent de modul de dezvoltare a aplicaţiei.

54. Prestatorii de servicii de plată documentează pe deplin procesul legat de gestionarea materialelor criptografice utilizate pentru a cripta sau a face ilizibile elementele de securitate personalizate. 55. Prestatorii de servicii de plată se asigură, în condiţii de siguranţă, că numai utilizatorul serviciilor de plată este asociat cu elemente de securitate personalizate, dispozitivele şi programele informatice de autentificare. În acest scop, prestatorii de servicii de plată se asigură că este îndeplinită fiecare dintre următoarele cerinţe: 1) asocierea identităţii utilizatorului serviciilor de plată cu elementele de securitate personalizate şi cu dispozitivele şi programele informatice de autentificare se desfăşoară în medii sigure, sub responsabilitatea prestatorului de servicii de plată; este vorba, cel puţin, 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 şi de serviciile de bancomate ale acestuia; trebuie avute în vedere riscurile asociate dispozitivelor şi componentelor acestora care sunt utilizate în timpul procesului de asociere şi care nu se află sub responsabilitatea prestatorului de servicii de plată; 2) asocierea printr-un canal la distanţă a identităţii utilizatorului serviciilor de plată cu elementele de securitate personalizate şi cu dispozitivele sau programele informatice de autentificare se efectuează prin intermediul autentificării stricte a clienţilor.	OTP Bank S.A.	83	La pct. 43 subpct. 1) de specificat dacă procesul de identificare a utilizatorului serviciilor de plată să fie efectuat pe mediul de tip „Mobile Banking” (ex. Prin intermediul unui dispozitiv mobil, smartphone etc.) sau identificarea trebuie efectuata strict pe mediul de tip Internet Payment, site-uri web securizate etc.	**Comentariu:** Pentru toate categoriile de plăţi, prestatorii de servicii de plată trebuie să asigure respectarea acestor cerinţe.
586. Prestatorii de servicii de plată se asigură că au fost create condiţii sigure de identificare pentru comunicarea dintre dispozitivul plătitorului şi dispozitivele beneficiarului plăţii prin care se acceptă plăţile electronice, inclusiv, dar nu numai, în cazul terminalelor de plată.	OTP Bank S.A.	84	Cu referire la pct. 46, prestatorul de servicii de plată nu poate asigura identificarea dispozitivului beneficiarului plăţii. Identificarea beneficiarului o poate face doar cel al beneficiarului. În acest context, propunem următoarea redacţie a punctului 46: ”46. Prestatorii de servicii de plată se asigură că au fost create condiţii sigure de identificare pentru comunicarea dintre dispozitivul plătitorului şi dispozitivele prestatorului de servicii de plată prin care se acceptă plăţile electronice, inclusiv, dar nu numai, în cazul terminalelor de plată.”.	**Comentariu:** Cerinţa vizează asigurarea unei comunicări sigure care să permită efectuarea plăţii.
60. Prestatorii de servicii de plată instituie proceduri prin care să se asigure că toate operaţiunile de plată şi alte interacţiuni, realizate în contextul prestării de servicii de plată, cu utilizatorul serviciilor de plată, cu alţi prestatori de servicii de plată şi cu alte entităţi, inclusiv comercianţi, pot fi urmărite, asigurând	„Paymaster” S.R.L.	85	Пункт 48 содержит фразу «... existenţa unor informaţii ex post...» - не понятен смысл с фразой «ex post». Что имеется ввиду ? Traducere:	**Comentariu:** Informaţii care să permită urmărirea operaţiunii după momentul realizării acesteia.

existența unor informații ex post cu privire la toate evenimentele relevante pentru operațiunea electronică, în orice etapă.			Punctul 48 conține sintagma „... existența unor informații ex post...” – sensul expresiei „ex post” nu este clar.	
63. În scopul autentificării utilizatorului serviciului de plată, interfața menționată la pct. 50 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.	OTP Bank S.A.	86	Conform pct. 51 și prin prisma conceptului „Open banking” reiese, ca plătitorul nu va fi obligat sa se autentifice adițional în una din interfețele (în interfața prestatorului de servicii de plată odată ce autentificarea a fost realizată de către prestatorii de servicii de informare cu privire la conturi și / sau prestatorii de servicii de inițiere a plății), deoarece aceasta comunicare între actori va fi asigurata în baza standardului național de comunicare (ex. API). În acest context, solicităm autorul să concretizeze prevederile.	**Comentariu:** Se are în vedere că prestatorul de servicii de plată care oferă servicii de administrare cont trebuie să implementeze în API toate metodele de SCA pe care le are în relația directă cu clientul (ex. biometrie sau elemente de cunoaștere și posesie).
65. Prestatorii de servicii de plată care oferă servicii de administrare cont se asigură că interfețele lor respectă standardul național aprobat/emis de Banca Națională a Moldovei.	Ministerul Finanțelor	87	La pct.53, pct.54 și pct.61, după textul „standardul național” și respectiv ”standardului național”, se completează cu cuvintele ”de comunicare”, pentru reflectarea exhaustivă a sensului prevederilor respective.	**Se acceptă parțial**
67. 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 Banca Națională a Moldovei pentru autorizația relevantă și pun rezumatul documentației la dispoziția publicului pe site-ul lor web.	OTP Bank S.A.	88	Cu referință la punctul 55, de specificat pentru care proces și/sau flux de business trebuie să se limiteze rezumatul documentației plasate pe site.	**Comentariu:** Pentru interfețele de acces la cont trebuie să ofere aceste informații, astfel încât AISP/PISP să știe elementele tehnice și funcționale pentru integrarea API-urilor dezvoltate de bancă.
74. În cazul în care un prestator de servicii de plată care oferă servicii de administrare cont nu respectă cerințele privind interfețele prevăzute în standardul național, Banca Națională a Moldovei 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 pct. 87 și 88.	OTP Bank S.A.	89	La pct. 61, de concretizat dacă există cerințe față de interfață sau prestatorii o vor stabili de sine stătător.	**Comentariu:** Va fi un standard național pe baza căruia se va dezvolta această interfață.
76. Sub rezerva respectării pct.62-75, 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.	ATIC	90	Propunere: *„63.Sub rezerva respectării pct.50-62, prestatorii de servicii de plată care oferă servicii de administrare cont și care au instituit o interfață specifică vor fi obligați să asigure ~~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*	**Nu se acceptă** Conform art. 54 alin. 1) lit. j) din *Legea cu privire la actele normative nr. 100 din 22.12.2017*, textul proiectului actului normativ se elaborează în limba română, cu respectarea următoarelor reguli: (...) verbele se utilizează, de regulă, la timpul prezent.

			plată pentru accesarea directă a contului său de plăți online."	
77. 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.	ATIC	91	Propunere: „65.Prestatorii de servicii de plată care oferă servicii de administrare cont și care au instituit o interfață specifică vor fi obligați să asigure ~~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."	**Nu se acceptă** Conform art. 54 alin. 1) lit. j) din Legea cu privire la actele normative nr. 100 din 22.12.2017, textul proiectului actului normativ se elaborează în limba română, cu respectarea următoarelor reguli: (...) verbele se utilizează, de regulă, la timpul prezent.
79. Obstacolele menționate la pct. 65 includ, printre altele, împiedicarea utilizării de către prestatorii de servicii de plată menționați la pct.50 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 Secțiunea 1 din Capitolul III al legii 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.	OTP Bank S.A.	92	La punctul 66, solicităm autorului concretizarea sintagmei "unei autorizații și înregistrări suplimentare". Pentru vizualizarea sau validarea unor plăti, de pe contul altui prestator de servicii decât cel de pe care este logat la moment utilizatorul, cu ce utilizator/parolă și mod de verificare se va face? Va fi necesar o logare suplimentar cu alte credențiale de la alt prestator? Sau se dorește sa fie un mod unic de autentificare, universal pentru toți, respectiv o singura baza de date?	**Comentariu:** Este vorba de Open Banking, când utilizatorul serviciilor de plată utilizează un AISP/PISP pentru accesul la cont, iar ASPSP nu trebuie să creeze obstacole în accesarea contului, cum ar fi cerințe de preînregistrare/autorizare a respectivului AISP/PISP care are o licență dată de BNM.
84. 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.	OTP Bank S.A.	93	La pct. 71, solicităm autorului concretizarea termenelor și căilor prin care va avea loc informarea dată.	**Comentariu:** Aceste informații trebuie să fie disponibile în cadrul documentației de conectare care este publicată de ASPSP.
85. Atât prestatorul de servicii de plată care oferă servicii de administrare cont, cât și prestatorii de servicii de plată menționați la pct. 50 transmit fără întârziere rapoarte Banca Națională a Moldovei privind problemele legate de interfețele specifice descrise la pct. 69, 70.	OTP Bank S.A.	94	Lapct. 72, de specificat periodicitatea expedierii rapoartelor, precum și formatul acestora.	**Comentariu:** Se aplică principiul de „imediat" sau „în cel mai scurt timp posibil".
88. În cazul în care utilizează interfața menționată la pct.73, prestatorii de servicii de plată menționați la pct.50: 1) 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;	Î.S. „Poșta Moldovei"	95	La pct.75 subpct. 3) și subpct. 4) este cazul ca în loc de sintagma „autorității lor naționale competente" de indicat autoritatea competentă concretă.	**Se acceptă**

2) continuă să respecte obligațiile care decurg din art. 522 alin.(3) și 523 alin.(2) din lege; 3) 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; 4) 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; 5) informează în acest sens prestatorul de servicii de plată care oferă servicii de administrare cont.				
91. În scopul identificării prevăzute la pct.50 subpct.1), prestatorii de servicii de plată se bazează pe certificatele calificate pentru sigiliile electronice sau pentru autentificarea unui site internet astfel cum sunt definite în Legea privind identificarea electronică și serviciile de încredere nr.124 din 19.05.2022.	Ministerul Justiției	96	Cu referire la pct. 78 și pct.80 și 81, se vor revizui cuvintele „autentificarea unui site internet” având în vedere că Legea privind identificarea electronică și serviciile de încredere nr. 124/2022 operează, în acest sens, cu noțiunea de „autentificarea paginii web”.	**Se acceptă**
92. În sensul prezentului regulament, numărul de înregistrare menționat în registrele oficiale, care este prevăzut de Legea privind identificarea electronică și serviciile de încredere nr.124 din 19.05.2022, 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 în temeiul art. 14 din Legea nr. 114/2012 sau care rezultă din autorizațiile acordate în temeiul Legii privind activitatea băncilor nr.202 din 06.10.2017.	Ministerul Finanțelor	97	La pct.79, textul ”în temeiul art.14 din Legea nr.114/2012” se substituie cu textul ”în temeiul art.23 din Legea nr.114/2012”, întrucât art.23 din Legea nr.114/2012 se referă la registru public al societăților de plată care au obținut licențe, care este ținut de către Banca Națională a Moldovei.	**Se acceptă**
103. În cazul în care prestatorul de servicii de plată care oferă servicii de administrare cont furnizează o interfață specifică în conformitate cu pct.63-68, 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.	OTP Bank S.A.	98	La pct. 90, de specificat dacă va fi un canal unic de comunicare între prestatori sau participanții singuri vor identifica canalele/modalitățile de comunicare. Tot aferent erorilor, internet banking este utilizat pentru comunicarea clienților despre anumite evenimente, inclusiv erori. În cazul în care clientul nu va mai utiliza aplicația prestatorului curent, dar numai conturile, cum se vor transmite notificările date? Întrebarea e si mai importantă în contextul în care se utilizează notificări POP-up din aplicație în loc de SMS Banking? Cum vor fi transmise clientului aceste notificări?	**Comentariu:** Această cerință vizează informarea prestatorilor de servicii de plată, nu a utilizatorilor de servicii de plată.

106. Prestatorii de servicii de informare cu privire la conturi sunt în măsură să acceseze informaţii provenind de la conturile de plată desemnate de utilizator şi de la operaţiunile de plată aferente deţinute 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 circumstanţe: 1) ori de câte ori utilizatorul serviciilor de plată solicită astfel de informaţii în mod activ; 2) în cazul în care utilizatorul serviciilor de plată nu solicită astfel de informaţii în mod activ, nu mai mult de patru ori într-o perioadă de 24 de ore, cu excepţia cazului în care prestatorul de servicii de informare cu privire la conturi şi prestatorul de servicii de plată care oferă servicii de administrare cont au convenit asupra unei frecvenţe mai ridicate, cu consimţământul utilizatorului serviciilor de plată.	OTP Bank S.A.	99	La pct. 93 de concretizat cum se vor stabili cazurile indicate în subpunctele 1-2) Prestatorul are dreptul sa aleagă de sine stator una din opţiuni?	**Comentariu:** Se implementează ambele situaţii şi se tratează diferit, respectiv atunci când sunt solicitate de client se poate face nelimitat, iar când sunt solicitate de AISP se furnizează în condiţiile prevăzute la pct. 2.
119. După aprobarea exceptării de la instituirea mecanismului de urgenţă potrivit pct. 76, Banca Naţională a Moldovei poate solicita oricând prestatorului de servicii de plată orice alte informaţii, date şi documente relevante pentru evaluarea respectării pe bază continuă a cerinţelor actelor normative.	Ministerul Justiţiei	100	La pct. 111, ţinem să menţionăm că, cuvintele „evaluarea pe bază continuă a cerinţelor actelor normative” ar putea determina apariţia unor situaţii de incoerenţă şi instabilitate pentru subiecţii vizaţi, contrare principiului securităţii raporturilor juridice în componenta sa referitoare la claritatea şi previzibilitatea actelor normative. Astfel, autorul proiectului trebuie să facă referire nemijlocit la actele normative relevante şi aplicabile de Banca Naţională a Moldovei ce includ cerinţele în cadrul evaluării respectării pe bază continuă la instituirea mecanismului de urgenţă potrivit pct. 76.	**Se acceptă** Punctul va avea următoarea redacţie: 119. După aprobarea exceptării de la obligaţia de a institui mecanismul de urgenţă prevăzut la pct. 82, Banca Naţională a Moldovei poate solicita oricând prestatorului de servicii de plată orice alte informaţii, date şi documente relevante pentru evaluarea respectării pe bază continuă a cerinţelor prezentului act normativ.
112. Banca Naţională a Moldovei poate revoca actul prin care a fost aprobată exceptarea de la mecanismul de urgenţă, în conformitate cu prevederile pct. 77.	Ministerul Justiţiei	101	Cu referire la pct. 112, în sensul evitării dublajului, considerăm oportună excluderea acestei propuneri, având în vedere că pct. 76 din proiect reglementează deja posibilitatea Băncii Naţionale a Moldovei de a revoca actul prin care a fost aprobată exceptarea de la mecanismul de urgenţă.	**Se acceptă** **Punctul a fost exclus**
Anexa nr.1	Ministerul Justiţiei	102	La anexa nr. 1, în vederea respectării normelor de tehnică legislativă, se va completa după textul „Anexa nr. 1” cu cuvintele „la Regulamentul cu privire la autentificarea strictă a clienţilor şi standardelor deschise, comune şi sigure de comunicare a presatorilor de servicii de plată”. Obiecţie valabilă şi pentru Anexele nr. 2 şi 3 din proiect.	**Se acceptă**
Anexa nr.3 15. Platforma de testare trebuie să permită prestatorilor de servicii de plată care oferă servicii de administrare cont, prestatorilor de servicii de iniţiere a plăţii, prestatorilor de servicii de informare cu privire la	„Paymaster” S.R.L.	103	Anexa 3, пункт 15. «să testeze interfaţa specifică într-un mediu de testare dedicat» - что имеется ввиду под «interfata specifica» ? Traducere:	**Comentariu:** Interfaţa specifică este interfaţa API dezvoltată de ASPSP pentru accesul la contul de plăţi accesibil online pentru AISP/PISP.

conturi și prestatorilor de servicii de plată care emit instrumente de plată bazate pe card autorizați și entităților care au remis o cerere la Banca Națională a Moldovei pentru autorizația relevantă să testeze interfața specifică într-un mediu de testare dedicat, securizat și cu date fictive ale utilizatorilor de servicii de plată, pentru următoarele: (...)			Anexa 3, paragraful 15: „să testeze interfața specifică într-un mediu de testare dedicat" – ce se înțelege prin „interfața specifică"?	
	Mastercard	104	Additional elements for consideration: · The draft Regulation includes the geographical locations of the payer and payee among the risk factors for transaction monitoring, which must be carried out for each and every transaction (Article 5, points 6 and 7). The RTS instead requires the check of these risk factors only for the application of the TRA exemption (Article 18(2)(c)(v-vi) RTS);	**Comentariu:** Într-adevăr, locația geografică urmează a fi monitorizată pentru toate plățile, nu doar cele derogate, ceea ce va fortifica măsurile de securitate contra fraudei, dar trebuie de luat în considerare că majoritatea băncilor deja monitorizează poziția geografică.
	Mastercard		· The draft Regulation requires that the authentication code is valid only for a limited period of time (Article 10, point 5). This requirement is instead not expressly envisaged in the RTS;	Comentariu: Necesitatea limitării perioadei de valabilitate a codului de autentificare este necesară pentru a întări măsurile de securitate în sensul prevenirii abuzului în lipsa termenului de valabilitate a codului. Cu toate acestea, nu există o perioadă concretă, astfel PSP va ajusta perioada pentru fiecare tip de operațiune, conform necesităților sale.
	Mastercard		· The draft Regulation envisages a number of detailed requirements for the use of the secure corporate payments (SCP) exemption, such as low fraud levels, audit requirements and technical security requirements (Articles 28-31);	Comentariu: În cadrul proiectului Twinning RM-UE, experții UE, care au susținut transpunerea Regulamentului 2018/389, au sugerat completarea prezentei norme pentru a fi posibilă aplicarea acesteia în sensul regulamentului UE.
	Mastercard		· The draft Regulation does not contain the new exemption for access to account through Account Information Service Providers (AISPs) recently introduced by Article 10a RTS provided in REGULATIONS COMMISSION DELEGATED REGULATION (EU) 2022/2360 of 3 August 2022 amending the regulatory technical standards laid down in Delegated Regulation (EU) 2018/389 as regards the 90-day exemption for account access (applicable as of July 25, 2023).	Se acceptă Prevederile modificate au fost incorporate în proiectul regulamentului.
	Mastercard	105	We strongly recommend that the implementation period of the provisions shall be applied similar as in the European Union country members with up to 24 months of transitional period for adjusting and implementing	**Comentariu:** Prezentul proiect de regulament a fost publicat pentru consultări publice pe data de 06.03.2023,

			new regulations, due to the necessary technical changes and adjustments of the services providers.	iar intrarea în vigoarea a acestuia este prevăzută pentru data de 5 august 2024. Astfel, considerăm că este suficient timp pentru toți actorii pieței să depună eforturi în sensul pregătirii pentru conformare cu prevederile regulamentului (fiind o perioada apropiată cu cea alocata pentru piața UE). Mai mult ca atât, cât timp Mastercard este prezentă inclusiv pe piața UE, aceasta are experiența și pregătirea tehnică pentru a implementa SCA inclusiv pe piața din RM.