ДЕЛЕГИРАН РЕГЛАМЕНТ (ЕС) 2018/389 НА КОМИСИЯТА

от 27 ноември 2017 година

за допълнение на Директива (ЕС) 2015/2366 на Европейския парламент и на Съвета по отношение на регулаторните технически стандарти за задълбоченото установяване на идентичността на клиента и общите и сигурни отворени стандарти на комуникация

(текст от значение за ЕИП)

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид Директива (ЕС) 2015/2366 на Европейския парламент и на Съвета от 25 ноември 2015 г. за платежните услуги във вътрешния пазар, за изменение на директиви 2002/65/ЕО, 2009/110/ЕО и 2013/36/ЕС и Регламент (ЕС) № 1093/2010 и за отмяна на Директива 2007/64/ЕО ([1]), и по-специално член 98, параграф 4, втора алинея от нея,

като има предвид, че:

(1) Платежните услуги, предлагани по електронен път, следва да се извършват по сигурен начин посредством технологии, които могат да гарантират безопасно установяване на идентичността на ползвателя и възможно най-голямо ограничаване на риска от измами. Процедурата за установяване на идентичността следва по принцип да включва механизми за мониторинг на операциите с цел откриване на опитите за използване на персонализираните средства за сигурност на ползвателя на платежни услуги, които са били изгубени, откраднати или незаконно присвоени, и следва също така да гарантира, че ползвателят на платежни услуги е законният ползвател, който чрез нормално използване на персонализирани средства за сигурност дава съгласие за прехвърляне на финансови средства и достъп до своята информация за сметка. Освен това е необходимо да се уточнят изискванията за задълбочено установяване на идентичността на клиента, които следва да бъдат прилагани всеки път, когато платецът получава достъп до своята платежна сметка онлайн, инициира електронна платежна операция или извършва дистанционно действие, което би могло да е свързано с риск от измама при плащането или други злоупотреби, като се изисква генерирането на код за удостоверяване на идентичността, който да е устойчив срещу риск от цялостно подправяне, или чрез оповестяване на някой от елементите, въз основа на които е генериран кодът.

(2) Тъй като методите на измама се променят непрекъснато, изискванията за задълбочено установяване на идентичността на клиента следва да дават възможност за иновации чрез технически решения за справяне с появата на нови заплахи за сигурността на електронните плащания. За да се гарантира, че изискванията, които следва да бъдат установени, се прилагат ефективно и без прекъсване, също така е целесъобразно да се изисква мерките за сигурност при прилагането на задълбоченото установяване на идентичността на клиента и освобождаванията от него, мерките за защита на поверителността и целостта на персонализираните средства за сигурност, както и мерките за създаване на общи и сигурни отворени стандарти на комуникация да се документират, периодично да се изпитват, оценяват и проверяват от оперативно независими одитори с опит в сигурността на информационните технологии и плащанията. С цел да се позволи на компетентните органи да наблюдават качеството на прегледа на тези мерки, резултатите от прегледите следва да им се предоставят при поискване.

(3) Тъй като електронните дистанционни платежни операции предполагат по-висок риск от измами, е необходимо да се въведат допълнителни изисквания за задълбочено установяване на идентичността на клиента при такива операции, за да се гарантира, че елементите свързват операцията по динамичен начин със стойността и получателя, посочен от платеца при иницииране на операцията.

(4) Динамичното свързване е възможно чрез генериране на кодове за установяване на идентичността, които се подчиняват на набор от строги изисквания за сигурност. За да се постигне запазване на неутралността в технологично отношение, не следва да се изисква конкретна технология за прилагане на кодове за установяване на идентичността. Поради това кодовете за установяване на идентичността следва да се основават на решения като генериране и валидиране на еднократни пароли, цифрови подписи или други проверки за валидност на основата на криптографски методи, използващи ключове или криптографски материал, съхраняван в елементите за установяване на идентичността, при условие че изискванията за сигурност са изпълнени.

([1]) ОВ L 337, 23.12.2015 г., стр. 35.

(5) Необходимо е да се определят специфични изисквания за случаите, когато окончателната стойност не е известна към момента, в който платецът инициира електронна дистанционна платежна операция, за да се гарантира, че задълбоченото установяване на идентичността на клиента съответства на максималната стойност, за която платецът е дал съгласие, както е посочено в Директива (ЕС) 2015/2366.

(6) С цел да се осигури прилагането на задълбоченото установяване на идентичността на клиента е необходимо също така да се изискват подходящи защитни характеристики за елементите на задълбочено установяване на идентичността на клиента, категоризирани като знание (нещо, което само ползвателят знае), например дължина и сложност, както и за елементите, категоризирани като притежание (нещо, което само ползвателят притежава), например спецификации на алгоритми, дължина на ключове и ентропия на информацията, както и за устройствата и софтуера, четящи елементи, категоризирани като характерни особености (нещо, което потребителят е), например спецификации на алгоритми, защитни функции, използващи биометрични датчици и биометрични шаблони, и по-специално, за намаляване на риска от разкриване, оповестяване и използване на тези елементи от неупълномощени страни. Необходимо е също така да бъдат определени изискванията, с които се гарантира, че тези елементи са независими един от друг, така че нарушаването на един елемент да не влияе на надеждността на останалите, по-специално когато някой от тези елементи се използва чрез устройство с много предназначения, а именно устройство като таблет или мобилен телефон, което може да се използва както за предоставяне на инструкция за извършване на плащането, така и в процеса на установяване на идентичността.

(7) Изискванията за задълбочено установяване на идентичността на клиента се прилагат за плащанията, инициирани от платеца, независимо от това дали платецът е физическо лице или правен субект.

(8) Поради естеството си плащанията, извършени чрез използването на анонимни платежни инструменти, не са предмет на задължението за задълбочено удостоверяване на идентичността на клиента. Когато анонимността на тези инструменти бъде отменена на договорни или законови основания, плащанията подлежат на изискванията за сигурност, предвидени в Директива (ЕС) 2015/2366 и настоящия регулаторен технически стандарт.

(9) В съответствие с Директива (ЕС) 2015/2366 са определени освобождавания от принципа за задълбочено установяване на идентичността на клиента въз основа на нивото на риска, размера, периодичността и канала на плащане, използван за изпълнение на платежната операция.

(10) Действия, които предполагат: достъп до салдото и последните операции по платежна сметка без оповестяване на чувствителни данни за плащанията; периодични плащания за същите получатели, които преди това са били създадени или потвърдени от платеца чрез използването на задълбочено установяване на идентичността на клиента; както и плащания към и от едно и също физическо лице или правен субект със сметки към един и същ доставчик на платежни услуги, представляват действия с ниска степен на риск, поради което на доставчиците на платежни услуги се дава възможност да не прилагат задълбочено установяване на идентичността на клиента. Горепосоченото не засяга обстоятелството, че в съответствие с членове 65, 66 и 67 от Директива (ЕС) 2015/2366 доставчиците на услуги по иницииране на плащане, доставчиците на платежни услуги, издаващи платежни инструменти, свързани с карти и доставчиците на услуги по предоставяне на информация за сметка следва да искат и получават необходима и важна информация единствено от доставчика на платежни услуги, обслужващ сметка, с цел предоставянето на дадена платежна услуга, със съгласието на ползвателя на платежни услуги. Подобно съгласие може да се предостави поотделно за всяко искане на информация или за всяко плащане, което ще бъде инициирано, или за доставчиците на услуги по предоставяне на информация за сметка — като мандат за определени платежни сметки и свързаните с тях платежни операции, както е определено в договорното споразумение с ползвателя на платежни услуги.

(11) Освобожданията за безконтактни плащания с ниска стойност на терминални устройства ПОС, които вземат предвид и максимален брой последователни операции или определен фиксирана максимална стойност на последователни операции, без да се прилага задълбочено установяване на идентичността на клиента, дават възможност за разработването на лесни за ползване платежни услуги с нисък риск и поради това следва да бъдат предвидени. Също така е целесъобразно да се установи освобождаване за случаите на електронни платежни операции, инициирани на необслужвани терминали, където използването на задълбочено установяване на идентичността на клиента може не винаги да бъде лесно приложимо поради оперативни причини (например, за да бъдат избегнати опашки и възможните инциденти на бариерите за пътни такси, или при други рискове за безопасността или сигурността).

(12) Подобно на освобождаването за безконтактни плащания с ниска стойност на терминални устройства ПОС, следва да се постигне правилен баланс между интереса от засилване на сигурността на дистанционните плащания и нуждата от улеснение и достъпност на плащанията в областта на електронната търговия. В съответствие с тези принципи праговете, под които не е необходимо да се прилага задълбочено установяване на идентичността на клиента, следва да се определят по разумен начин, за да покриват само онлайн покупки с ниска стойност. Праговете за онлайн покупки следва да се определят с по-голяма предпазливост, като се има предвид, че след като лицето не присъства физически, то при покупката възниква малко по-висок риск за сигурността.

(13) Изискванията за задълбочено установяване на идентичността на клиента се прилагат за плащанията, инициирани от платеца, независимо от това дали платецът е физическо лице или правен субект. Много корпоративни плащания се инициират чрез специални процеси или протоколи, гарантиращи високото ниво на сигурност на плащанията, което се цели чрез задълбоченото установяване на идентичността на клиента, предвидено в Директива (ЕС) 2015/2366. Когато компетентните органи определят, че с тези процеси и протоколи, които се предоставят единствено на платците, различни от потребители, се постигат целите на Директива (ЕС) 2015/2366 по отношение на сигурността, доставчиците на платежни услуги могат да бъдат освободени от изискванията за задълбочено установяване на идентичността на клиента във връзка с тези процеси и протоколи.

(14) Когато в реално време се извършва анализ на риска от операциите, в резултат на който дадена платежна операция е категоризирана като нискорискова, е целесъобразно също така да се предвиди освобождаване за доставчика на платежни услуги, който възнамерява да не прилага задълбочено установяване на идентичността на клиента въз основа на въвеждането на ефективни и основани на риска изисквания, които гарантират безопасността на средствата и личните данни на ползвателя на платежни услуги. Тези основани на риска изисквания следва да комбинират резултатите от анализа на риска, за да се потвърди, че не са установени необичайни модели на изразходване на средства или на поведение от страна на платеца, като се вземат под внимание други рискови фактори, включително информацията относно местоположението на платеца и на получателя на плащането с паричен праг въз основа на процента на измами, изчислен за дистанционните плащания. Ако въз основа на анализа на риска от операциите в реално време плащането не може да бъде поставено в категория с ниска степен на риск, доставчикът на платежни услуги трябва да премине към задълбочено установяване на идентичността на клиента. Максималната стойност за такова освобождаване въз основа на риска следва да се определи по начин, който гарантира много нисък съответен процент на измами, също и спрямо процента на измами при всички платежни операции на доставчика на платежни услуги, включително проверените чрез задълбочено установяване на идентичността на клиента периодично и в рамките на определен срок.

(15) С цел осигуряване на ефективно прилагане, доставчиците на платежни услуги, които желаят да се ползват от освобожданията от задълбочено установяване на идентичността на клиента, следва редовно да наблюдават и да предоставят на разположение на компетентните органи и на Европейския банков орган (ЕБО) — при поискване от тяхна страна и за всеки вид платежна операция — информация за стойността на неразрешените платежни операции или на платежните операции с цел измама, както и за наблюдавания процент на измами за всички техни платежни операции, независимо дали са установени чрез задълбочено установяване на идентичността на клиента или са изпълнени съгласно съответното освобождаване.

(16) Събирането на тези нови доказателства за минали периоди за процента на измами на електронни платежни операции също така ще допринесе за ефективен преглед от страна на ЕБО на праговете за освобождаване от задълбочено установяване на идентичността на клиента въз основа на анализ на риска от операциите в реално време. ЕБО следва да направи преглед и да представи на Комисията проекти за актуализация относно тези регулаторни технически стандарти, когато е целесъобразно, чрез представяне на нов проект за прагове и на информация за съответния процент на измами с цел засилване на сигурността на електронните дистанционни плащания, в съответствие с член 98, параграф 5 от Директива (ЕС) 2015/2366 и с член 10 от Регламент (ЕС) № 1093/2010 на Европейския парламент и на Съвета ([1]).

(17) Доставчиците на платежни услуги, които се възползват от предвидените освобождавания, следва по всяко време да имат право да прилагат задълбочено установяване на идентичността на клиента за действията и за платежните операции, посочени в тези разпоредби.

(18) С мерките, които защитават поверителността и целостта на персонализираните средства за сигурност, както и посредством устройствата и софтуера за установяване на идентичността, следва да се ограничават рисковете, свързани с измами чрез неразрешеното използване, или използване с цел измама, на платежни инструменти, включително неразрешения достъп до платежни сметки. За тази цел е необходимо да се въведат изисквания за сигурното създаване и предоставяне на персонализираните средства за сигурност и тяхното свързване с ползвателя на платежни услуги, както и да се осигурят условия за подновяването и дезактивирането на тези средства.

(19) С цел да се гарантира ефективна и сигурна комуникация между съответните участници в контекста на услугите по предоставяне на информация за сметка, услугите по иницииране на плащане и потвърждение относно наличността на средства, е необходимо да се определят изискванията за общи и сигурни отворени стандарти за комуникация, които да се спазват от всички засегнати доставчици на платежни услуги. С Директива (ЕС) 2015/2366 се предвижда достъп и използване на информацията за платежната сметка от доставчиците на услуги по предоставяне на информация за сметка. Следователно с настоящия регламент не се променят правилата за достъпа до сметки, различни от платежни сметки.

([1]) Регламент (ЕС) № 1093/2010 на Европейския парламент и на Съвета от 24 ноември 2010 г. за създаване на Европейски надзорен орган (Европейски банков орган), за изменение на Решение № 716/2009/ЕО и за отмяна на Решение 2009/78/ЕО на Комисията (ОВ L 331, 15.12.2010 г., стр. 12).

(20) Всеки доставчик на платежни услуги, обслужващ платежни сметки, които са достъпни онлайн, следва да предложат поне един интерфейс за достъп, който дава възможност за сигурна комуникация с доставчиците на услуги по предоставяне на информация за сметка, доставчиците на услуги по иницииране на плащане и доставчиците на платежни услуги, издаващи платежни инструменти, свързани с карти. Интерфейсът следва да дава възможност на доставчиците на услуги по предоставяне на информация за сметка, доставчиците на услуги по иницииране на плащане и доставчиците на платежни услуги, издаващи платежни инструменти, свързани с карти, да се идентифицират пред доставчика на платежни услуги, обслужващ сметка. Този интерфейс следва също така да позволява на доставчиците на услуги по предоставяне на информация за сметка и доставчиците на услуги по иницииране на плащане да разчитат на процедурите за установяване на идентичността, предоставени от доставчика на платежни услуги, обслужващ сметка, на ползвателя на платежни услуги. За да се осигури неутралност на технологиите и на моделите на стопанската дейност, доставчиците на платежни услуги, обслужващи сметка, следва да бъдат свободни да решат дали да предложат интерфейс, предназначен за комуникация с доставчиците на услуги по предоставяне на информация за сметка, доставчиците на услуги по иницииране на плащане и доставчиците на платежни услуги, издаващи платежни инструменти, свързани с карти, или да разрешат, за целите на тази комуникация, използването на интерфейс за идентификация и комуникация с ползвателите на платежни услуги на доставчиците на платежни услуги, обслужващи сметка.

(21) С цел да се позволи на доставчиците на услуги по предоставяне на информация за сметка, на доставчиците на услуги по иницииране на плащане, както и на доставчиците на платежни услуги, издаващи платежни инструменти, свързани с карти, да разработят свои технически решения, техническата спецификация на интерфейса следва да бъде документирана по подходящ начин и да се направи обществено достъпна. Освен това доставчикът на платежни услуги, обслужващ сметка, следва да предложи механизъм, който дава възможност на доставчиците на платежни услуги да изпробват техническите решения поне шест месеца преди датата, от която започва прилагането на тези регулаторни стандарти, или, ако те се въвеждат след датата на влизане в сила на тези стандарти, то преди датата, на която интерфейсът ще бъде пуснат на пазара. За да се гарантира оперативната съвместимост на различните технологични решения в областта на комуникацията, интерфейсът следва да използва стандарти за комуникация, разработени от международни или европейски организации по стандартизация.

(22) Качеството на услугите, предоставяни от доставчиците на услуги по предоставяне на информация за сметка и доставчиците на услуги по иницииране на плащане, зависи от правилното функциониране на интерфейсите, въведени или адаптирани от доставчиците на платежни услуги, обслужващи сметка. Поради това е важно, ако тези интерфейси не съответстват на разпоредбите, предвидени в тези стандарти, да се предприемат мерки за гарантиране на непрекъснатост на дейността в полза на ползвателите на тези услуги. Задача на националните компетентни органи е да гарантират, че доставчиците на услуги по предоставяне на информация за сметка и доставчиците на услуги по иницииране на плащане не са блокирани или възпрепятствани при предоставянето на своите услуги.

(23) Когато достъпът до платежни сметки се предлага чрез специален интерфейс, е необходимо да се изисква специалните интерфейси да имат същото равнище на достъпност и функциониране като интерфейса на разположение на ползвателя на платежни услуги, за да се гарантира правото на ползвателите на платежни услуги да се ползват от доставчиците на услуги по иницииране на плащане и услуги, които позволяват достъп до информация за сметка, както е предвидено в Директива (ЕС) 2015/2366. Доставчиците на платежни услуги, обслужващи сметка, следва също така да определят прозрачни ключови показатели за изпълнението и цели за нивото на обслужване, свързани с достъпността и функционирането на специалните интерфейси, които са поне толкова строги, колкото тези за интерфейса, използван за техните ползватели на платежни услуги. Тези интерфейси следва да се изпитват от доставчиците на платежни услуги, които ще ги използват, и следва да бъдат подложени на стрес тестове и да се наблюдават от компетентните органи.

(24) За да се гарантира, че доставчиците на платежни услуги, които разчитат на специалния интерфейс, могат да продължат да предоставят услугите си в случай на проблеми с достъпността или незадоволителната оперативност, е необходимо при съответните строги условия да се предвиди резервен механизъм, който ще позволи на такива доставчици да използват интерфейса, поддържан от доставчика на платежни услуги, обслужващ сметка, с цел идентификация и комуникация с неговите собствени ползватели на платежни услуги. Някои доставчици на платежни услуги, обслужващи сметка, ще бъдат освободени от задължението да предоставят такъв резервен механизъм чрез интерфейсите, предназначени за техните ползватели, в случаите, когато компетентните органи установяват, че специалните интерфейси отговарят на определени условия, които гарантират безпрепятствена конкуренция. В случай че освободените специални интерфейси не отговарят на необходимите условия, освобождаванията се отменят от съответните компетентни органи.

(25) За да могат компетентните органи да извършват ефективен надзор и мониторинг на изпълнението и управлението на комуникационните интерфейси, доставчиците на платежни услуги, обслужващи сметка, следва да предоставят обобщение на съответната документация на разположение на своя уебсайт, както и при поискване да предоставят на компетентните органи документация за решенията в случай на извънредни ситуации. Доставчиците на платежни услуги, обслужващи сметка, следва също така да направят обществено достъпни статистическите данни относно достъпността и функционирането на този интерфейс.

(26) С цел да се запази поверителността и целостта на данните е необходимо да се гарантира сигурността при предаването на информация между доставчици на платежни услуги, обслужващи сметка, доставчиците на услуги по предоставяне на информация за сметка, доставчиците на услуги по иницииране на плащане и доставчиците на

платежни услуги, издаващи платежни инструменти, свързани с карти. Необходимо е по-специално да се изисква прилагането на сигурно криптиране при обмена на данни между доставчиците на услуги по предоставяне на информация за сметка, доставчиците на услуги по иницииране на плащане, доставчиците на платежни услуги, издаващи платежни инструменти, свързани с карти и доставчиците на платежни услуги, обслужващи сметка.

(27) За да се повиши доверието на ползвателите и да се гарантира задълбоченото установяване на идентичността на клиента, използването на средства за електронна идентификация и удостоверителни услуги, както е посочено в Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета ([1]), следва да се вземе под внимание, по-специално във връзка с нотифицираните схеми за електронна идентификация.

(28) С цел да се осигури съгласуване на датите на влизане в сила, настоящият регламент следва да се прилага от същата дата, от която държавите членки са длъжни да гарантират прилагането на мерките за сигурност, посочени в членове 65, 66, 67 и 97 от Директива (ЕС) 2015/2366.

(29) Настоящият регламент е изготвен въз основа на проектите на регулаторни технически стандарти, представени на Комисията от ЕБО.

(30) ЕБО проведе открити и прозрачни обществени консултации по проектите на регулаторни технически стандарти, въз основа на които е изготвен настоящият регламент, анализира свързаните с тях потенциални разходи и ползи и поиска становище от Групата на участниците от банковия сектор, създадена с член 37 от Регламент (ЕС) № 1093/2010,

ПРИЕ НАСТОЯЩИЯ РЕГЛАМЕНТ:

ГЛАВА I

ОБЩИ РАЗПОРЕДБИ

Член 1

Предмет

В настоящия регламент се установяват изискванията, които трябва да бъдат изпълнени от доставчиците на платежни услуги за целите на прилагането на мерки за сигурност, даващи им възможност:

а) да прилагат процедурата за задълбочено установяване на идентичността на клиента в съответствие с член 97 от Директива (ЕС) 2015/2366;

б) да предоставят освобождаване от прилагането на изискванията за сигурност при задълбочено установяване на идентичността на клиента, при положение че са спазени определени ограничени условия, отчитащи нивото на риска, размера и периодичността на платежната операция, както и канала на плащане, използван за нейното изпълнение;

в) да защитават поверителността и целостта на персонализираните средства за сигурност на ползвателя;

г) да установят общи и сигурни отворени стандарти за комуникация между доставчиците на платежни услуги, обслужващи сметка, доставчиците на услуги по иницииране на плащане, доставчиците на услуги по предоставяне на информация за сметка, платците, получателите на плащането и други доставчици на платежни услуги във връзка с предоставянето и използването на платежни услуги в съответствие с дял IV от Директива (ЕС) 2015/2366.

Член 2

Общи изисквания за установяване на идентичността

1. С оглед прилагането на мерките за сигурност, посочени в член 1, букви а) и б), доставчиците на платежни услуги трябва да разполагат с действащи механизми за мониторинг на операциите, които им дават възможност да открият неразрешените платежни операции или платежните операции с цел измама.

([1]) Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 г. относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО (ОВ L 257, 28.8.2014 г., стр. 53).

Тези механизми се основават на анализ на платежните операции, като се вземат под внимание елементите, които са типични за ползвателя на платежни услуги в условията на обичайно ползване на персонализираните средства за сигурност.

2. Доставчиците на платежни услуги гарантират, че механизмите за мониторинг на операциите отчитат като минимум всеки от следните основани на риска фактори:

а) списъци на компрометирани или откраднати елементи за установяване на идентичността;

б) стойността на всяка платежна операция;

в) известни сценарии на измама при предоставянето на платежни услуги;

г) признаци на заразяване със опасен софтуер при предаването на информация за процедурата по установяване на идентичността;

д) ако устройството за достъп или софтуерът се предоставят от доставчика на платежни услуги — запис в дневника за използването на устройството за достъп или софтуера, предоставени на ползвателя на платежни услуги, и на необичайно използване на устройството за достъп или софтуера.

Член 3

Преглед на мерките за сигурност

1. Прилагането на мерките за сигурност, посочени в член 1, се документира, те периодично се изпитват, оценяват и проверяват в съответствие с приложимата правна уредба за доставчика на платежни услуги от одитори с опит в сигурността на информационните технологии и плащанията, които са оперативно независими в рамките на или извън доставчика на платежни услуги.

2. Периодът между одитите, посочени в параграф 1, се определя, като се вземат предвид приложимата счетоводна рамка и рамката на задължителния одит, приложима по отношение на доставчика на платежни услуги.

Доставчици на платежни услуги, които се ползват от освобождаването, посочено в член 18, обаче подлежат на одит на методологията, модела и докладвания процент на измами най-малко веднъж годишно. Одиторът, извършващ одита, трябва да има опит в сигурността на информационните технологии и плащанията, и да е оперативно независим в рамките на или извън доставчика на платежни услуги. Тази проверка се извършва от независим и квалифициран външен одитор през първата година на използване на освобождаването съгласно член 18 и най-малко на всеки три години след това или по-често по преценка на компетентния орган.

3. В този одит се представя оценка и доклад относно спазването от страна на доставчика на платежни услуги на мерките за сигурност в съответствие с изискванията, определени в настоящия регламент.

Целият доклад се предоставя на разположение на компетентния орган при поискване.

ГЛАВА II

МЕРКИ ЗА СИГУРНОСТ ПРИ ПРИЛАГАНЕТО НА ЗАДЪЛБОЧЕНО УСТАНОВЯВАНЕ НА ИДЕНТИЧНОСТТА

Член 4

Код за установяване на идентичността

1. Когато доставчиците на платежни услуги прилагат задълбочено установяване на идентичността на клиента в съответствие с член 97, параграф 1 от Директива (ЕС) 2015/2366, установяването на идентичността се основава на два или повече елемента, категоризирани като знание, притежание и принадлежност, и води до генерирането на код за установяване на идентичността.

Кодът за установяване на идентичността се приема само веднъж от доставчика на платежни услуги, когато платецът използва кода, за да получи достъп до своята платежна сметка онлайн, да инициира електронна платежна операция или да извършва каквото и да било действие дистанционно, което би могло да е свързано с риск от измама при плащането или други злоупотреби.

2. За целите на параграф 1 доставчиците на платежни услуги приемат мерки за сигурност, гарантиращи, че всяко от следните изисквания е спазено:

а) от оповестяването на кода за установяване на идентичността не е възможно извличането на информация по отношение на някой от елементите, посочени в параграф 1;

б) не е възможно да се генерира нов код за установяване на идентичността въз основа на познаването на друг такъв код, генериран преди това;

в) кодът за установяване на идентичността не може да бъде подправен.

3. Доставчиците на платежни услуги гарантират, че установяването на идентичността посредством създаването на съответния код включва всяка от следните мерки:

а) когато установяването на идентичността за достъп от разстояние, електронни плащания и всякакви други дистанционни действия, които биха могли да са свързани с риск от измама при плащането или с други злоупотреби, не е успяло да генерира код за установяване на идентичността за целите на параграф 1, не е възможно да се определи кой от елементите, изброени в посочения параграф, е бил неправилен;

б) броят последователни неуспешни опити за установяване на идентичността, след които действията, посочени в член 97, параграф 1 от Директива (ЕС) 2015/2366, се блокират временно или постоянно, не надвишава пет опита в рамките на определен период от време;

в) предаването на информация е защитено от прихващането на данни, предадени по време на установяване на идентичността, и от манипулиране от страна на неупълномощени лица в съответствие с изискванията на глава V;

г) максималното време на неактивност от страна на платеца след установяване на идентичността за достъп до неговата платежна сметка онлайн не надхвърля пет минути.

4. Когато блокирането, посочено в параграф 3, буква б) е временно, продължителността му и броят на повторните опити се определят въз основа на характеристиките на услугата, предоставяна на платеца, и на всички съответни рискове, като се вземат предвид най-малко факторите, посочени в член 2, параграф 2.

Платецът трябва да бъде информиран преди блокирането да бъде направено постоянно.

За случаите, когато блокирането е направено постоянно, се създава процедурата за сигурност, която позволява на платеца да възстанови използването на блокираните електронни платежни инструменти.

Член 5

Динамично свързване

1. Когато доставчиците на платежни услуги прилагат задълбочено установяване на идентичността на клиента в съответствие с член 97, параграф 2 от Директива (ЕС) 2015/2366, в допълнение към изискванията по член 4 от настоящия регламент, те също така трябва да приемат мерки за сигурност, които отговарят на всяко едно от следните изисквания:

а) платецът е осведомен за стойността на платежната операция и относно получателя;

б) кодът, генериран за установяване на идентичността, е специфичен за стойността на платежната операция и за получателя, посочен от платеца при иницииране на операцията;

в) кодът за установяване на идентичността, приет от доставчика на платежни услуги, съответства на първоначалната стойност на платежната операция и на идентичността на получателя, посочен от платеца;

г) всяка промяна в стойността или получателя на плащането води до анулиране на генерирания код за установяване на идентичността.

2. За целите на параграф 1 доставчиците на платежни услуги приемат мерки за сигурност, които гарантират поверителността, автентичността и целостта на всеки един от следните елементи:

а) стойността на операцията и получателя по време на всички фази на установяване на идентичността;

б) информацията, която платецът вижда по време на всички фази на установяването на идентичността, включително генерирането, предаването и използването на кодове за установяване на идентичността.

3. За целите на параграф 1, буква б) и когато доставчиците на платежни услуги прилагат задълбочено установяване на идентичността на клиента в съответствие с член 97, параграф 2 от Директива (ЕС) 2015/2366, се прилагат следните изисквания за кода за установяване на идентичността:

а) във връзка с платежна операция, свързана с карта, за която платецът е дал съгласието си за точния размер на средствата, които да бъдат блокирани, съгласно член 75, параграф 1 от тази директива, кодът за установяване на идентичността е специфичен за размера на средствата, за които платецът е дал съгласие да бъдат блокирани и които платецът е посочил при иницииране на операция;

б) във връзка с платежни операции, при които платецът е дал съгласие за изпълнение на поредица от дистанционни електронни платежни операции за един или няколко получатели, кодът за установяване на идентичността се отнася конкретно за общия размер на поредицата от платежни операции и за конкретните получатели.

Член 6

Изисквания за елементите, категоризирани като знание

1. Доставчиците на платежни услуги приемат мерки за намаляване на риска от това елементите на задълбочено установяване на идентичността на клиента, категоризирани като знание, да бъдат разкрити от или оповестени на неупълномощени страни.

2. Използването на тези елементи от платеца се подлежи на мерки за намаляване на риска, за да се предотврати тяхното оповестяване на неупълномощени страни.

Член 7

Изисквания за елементите, категоризирани като притежание

1. Доставчиците на платежни услуги приемат мерки за намаляване на риска от това елементите на задълбочено установяване на идентичността на клиента, категоризирани като притежание, да бъдат използвани от неупълномощени страни.

2. Използването на тези елементи от платеца се подлежи на мерки, предвидени да предотвратяват възпроизвеждането им.

Член 8

Изисквания за устройствата и софтуера, свързани с елементите, категоризирани като принадлежност

1. Доставчиците на платежни услуги приемат мерки за намаляване на риска от това елементите, категоризирани като принадлежност и прочетени от устройствата и софтуера за достъп, предоставени на платеца, да бъдат разкрити от неупълномощени страни. Доставчиците на платежни услуги най-малко гарантират, че рискът устройствата и софтуера за достъп да допуснат неупълномощени страни вместо платеца при процеса на установяване на идентичността е минимален.

2. Използването от платеца на тези елементи подлежи на мерки, с които се гарантира, че посочените устройства и софтуер осигуряват защита срещу неразрешено използване на елементите чрез достъп до устройствата и софтуера.

Член 9

Независимост на елементите

1. Доставчиците на платежни услуги гарантират, че използването на елементите на задълбочено установяване на идентичността на клиента, посочени в членове 6, 7 и 8, подлежи на мерки, които да гарантират, че от гледна точка на технологиите, алгоритмите и параметрите, нарушението на един от елементите не компрометира надеждността на останалите елементи.

2. В случаите, в които всеки от елементите на задълбоченото установяване на идентичността на клиента или самият код за установяване на идентичността се използва чрез устройство с много предназначения, доставчиците на платежни услуги приемат мерки за сигурност, насочени към намаляване на риска, който би възникнал при компрометирането на това устройство с много предназначения.

3. За целите на параграф 2 мерките за намаляване на риска трябва да включват всеки от следните елементи:

а) използването на отделни среди за сигурно изпълнение посредством софтуера, инсталиран в устройството с много предназначения;

б) механизми, които гарантират, че този софтуер или устройство не са били променяни от платеца или от трета страна;

в) при наличието на промени — механизми за намаляване на последствията от тях.

ГЛАВА III

ОСВОБОЖДАВАНИЯ ОТ ЗАДЪЛБОЧЕНОТО УСТАНОВЯВАНЕ НА ИДЕНТИЧНОСТТА НА КЛИЕНТА

Член 10

Информация за платежна сметка

1. На доставчиците на платежни услуги е позволено да не прилагат задълбочено установяване на идентичността на клиента при спазване на изискванията, посочени в член 2, както и изискванията по параграф 2 от настоящия член, когато достъпът на даден ползвател на платежни услуги е ограничен до онлайн достъп до един или два от следните елементи без оповестяване на чувствителни данни за плащанията:

а) салдото на една или повече определени платежни сметки;

б) платежните операции, изпълнени през последните 90 дни, чрез една или повече определени платежни сметки.

2. За целите на параграф 1 доставчиците на платежни услуги не могат да бъдат освободени от прилагането на задълбоченото установяване на идентичността на клиента, когато е изпълнено едно от следните условия:

а) ползвателят на платежни услуги осъществява онлайн достъп до информацията, посочена в параграф 1, за пръв път;

б) изтекли са повече от 90 дни след последния път, когато ползвателят на платежни услуги е осъществил онлайн достъп до информацията, посочена в параграф 1, буква б), и е било приложено задълбочено установяване на идентичността на клиента.

Член 11

Безконтактни плащания на терминални устройства ПОС

На доставчиците на платежни услуги е разрешено да не прилагат задълбочено установяване на идентичността на клиента при спазване на изискванията, определени в член 2, когато платецът инициира безконтактна електронна платежна операция, ако са изпълнени следните условия:

а) индивидуалната стойност на безконтактната електронна платежна операция не надвишава 50 EUR; както и

б) кумулативната стойност на предишните безконтактни електронни платежни операции, инициирани чрез платежен инструмент с безконтактна функция от датата на последното прилагане на задълбочено установяване на идентичността на клиента, не надвишава 150 EUR; или

в) броят на последователните безконтактни електронни платежни операции, инициирани чрез платежен инструмент с безконтактна функция от момента на последното прилагане на задълбочено установяване на идентичността на клиента, не надвишава пет операции;

Член 12

Необслужвани терминали за такси за транспорт и паркинг

На доставчиците на платежни услуги е разрешено да не прилагат задълбочено установяване на идентичността на клиента при спазване на изискванията, определени в член 2, когато платецът инициира електронна платежна операция на необслужван терминал с цел плащане на такса за транспорт или паркинг.

Член 13

Доверени бенефициери

1. Доставчиците на платежни услуги прилагат задълбочено установяване на идентичността на клиента, когато платецът създава или изменя списък с доверени бенефициери чрез доставчика на платежни услуги, обслужващ сметката.

2. На доставчиците на платежни услуги е разрешено да не прилагат задълбочено установяване на идентичността на клиента при спазване на общите изисквания за установяване на идентичността, когато платецът инициира платежна операция и получателят е включен в списък на доверени бенефициери, създаден преди това от платеца.

Член 14

Повтарящи се операции

1. Доставчиците на платежни услуги прилагат задълбочено установяване на идентичността на клиента, когато платецът създава, изменя или инициира за пръв път редица повтарящи се операции със същия размер и със същия получател.

2. На доставчиците на платежни услуги е разрешено да не прилагат задълбочено установяване на идентичността на клиента при спазване на общите изисквания за установяване на идентичността с цел иницииране на всички последващи платежни операции, включени в поредица от платежни операции, посочени в параграф 1.

Член 15

Кредитни преводи между сметки, държани от едно и също физическо лице или правен субект

На доставчиците на платежни услуги е разрешено да не прилагат задълбочено установяване на идентичността на клиента при спазване на изискванията, определени в член 2, когато платецът инициира кредитен превод при обстоятелства, при които платецът и получателят са едно и също физическо или юридическо лице, а двете платежни сметки се държат от един и същ доставчик на платежни услуги, обслужващ сметка.

Член 16

Операции с ниска стойност

На доставчиците на платежни услуги е разрешено да не прилагат задълбочено установяване на идентичността на клиента, когато платецът инициира дистанционна електронна платежна операция, ако са изпълнени следните условия:

а) размерът на дистанционната електронна платежна операция не надвишава 30 EUR; както и

б) кумулативната стойност на предишните дистанционни електронни платежни операции, инициирани от платеца от момента на последното използване на задълбочено установяване на идентичността на клиента, не надвишава 100 EUR; или

в) броят на предишните дистанционни електронни платежни операции, инициирани от платеца от момента на последното използване на задълбочено установяване на идентичността на клиента, не надвишава 5 последователни индивидуални дистанционни електронни платежни операции;

Член 17

Сигурност на корпоративните процеси и протоколи на плащане

На доставчиците на платежни услуги е разрешено да не прилагат задълбочено установяване на идентичността на клиента по отношение на юридически лица, инициирали електронни платежни операции чрез използването на специални процеси или протоколи на плащане, които се предоставят единствено на платци, различни от потребители, ако компетентните органи са уверени, че тези процеси или протоколи гарантират нива на сигурност, които са поне еквивалентни на тези, предвидени в Директива (ЕС) 2015/2366.

Член 18

Анализ на риска от операциите

1. На доставчиците на платежни услуги е разрешено да не прилагат задълбочено установяване на клиента, когато платецът инициира електронна дистанционна платежна операция, определена от доставчика на платежни услуги като операция с ниска степен на риск съгласно механизмите за мониторинг на операциите, посочени в член 2 и в параграф 2, буква в) от настоящия член.

2. Електронната платежна операция, посочена в параграф 1, се определя като операция с ниска степен на риск, когато са изпълнени всички изброени по-долу условия:

а) процентът на измами за такъв вид операции, докладван от доставчика на платежни услуги и изчислен в съответствие с член 19, е еквивалентен на или е под референтните проценти на измама, посочени в таблицата в приложението съответно за „дистанционни електронни плащания, свързани с карти“, и за „дистанционни електронни кредитни преводи“;

б) размерът на операцията не надвишава съответната прагова стойност за освобождаване („ПСО“), посочена в таблицата, поместена в приложението;

в) в резултат на извършването на анализ на риска в реално време доставчиците на платежни услуги не са установили нито едно от следните обстоятелства:

i) необичайни разходи или модел на поведение на платеца;

ii) необичайна информация за използването на устройството/софтуера за достъп на платеца;

iii) заразяване със опасен софтуер по време на сесията на процедурата по установяване на идентичността;

iv) известен сценарий на измама при предоставянето на платежни услуги;

v) необичайно местоположение на платеца;

vi) високорисково местоположение на получателя.

3. Доставчиците на платежни услуги, които възнамеряват да освобождават дистанционни електронни платежни операции от задълбочено установяване на идентичността на клиента на основание, че те представляват нисък риск, вземат предвид най-малко следните основани на риска фактори:

а) предишните модели на изразходване на средства на отделния ползвател на платежни услуги;

б) хронологията на извършените платежни операции на всеки от ползвателите на платежни услуги на доставчика на платежни услуги;

в) местоположението на платеца и на получателя към момента на платежната операция в случаите, когато устройството за достъп или софтуерът се предоставя от доставчика на платежни услуги;

г) установяването на необичайни модели на плащане на ползвателя на платежни услуги спрямо хронологията на платежните му операции.

Оценката, направена от доставчик на платежни услуги, съчетава всички тези основани на риска фактори в оценка на риска за всяка отделна операция, за да се определи дали конкретно плащане следва да бъде разрешено без задълбоченото установяване на идентичността на клиента.

Член 19

Изчисляване на процента на измами

1. За всеки вид операция, посочена в таблицата в приложението, доставчикът на платежни услуги гарантира, че общият процент на измами, обхващащ както платежните операции, извършени чрез задълбочено установяване на идентичността на клиента, както и тези, извършени съгласно някое от освобожданията, посочени в членове 13—18, е еквивалентен на или по-нисък от референтния процент на измами за съответния вид платежна операция, посочена в таблицата в приложението.

Общият процент на измами за всеки вид операция се изчислява като общата стойност на дистанционните неразрешени операции или дистанционните операции с цел измама, независимо дали средствата са възстановени или не, се раздели на общата стойност на всички дистанционни операции за един и същ вид операции, независимо дали за тях е приложено задълбоченото установяване на идентичността на клиента или са извършени съгласно освобождаване, посочено в членове 13—18 за всяко тримесечие (90 дни).

2. Изчисляването на процента на измами и получените стойности се оценяват при одита, посочен в член 3, параграф 2, който гарантира, че те са пълни и точни.

3. Методологията и всички модели, използвани от доставчика на платежни услуги за изчисляване на процента на измами, както и самият процент на измами, се документират надлежно и се предоставят в тяхната цялост на компетентните органи и на ЕБО, с предварително известие до съответния компетентен орган (или органи), при поискване от тяхна страна.

Член 20

Преустановяване на освобождаванията, основани на анализ на риска от операциите

1. Доставчиците на платежни услуги, които се ползват от освобождаването, посочено в член 18, незабавно докладват на компетентните органи, когато един от наблюдаваните проценти на измами, за всеки вид платежна операция, посочена в таблицата в приложението, надвишава приложимия референтен процент на измамите, като предоставят на компетентните органи описание на мерките, които те възнамеряват да предприемат, за да се възстанови съответствието на наблюдавания процент на измамите с приложимите референтни проценти.

2. Доставчиците на платежни услуги незабавно престават да се ползват от освобождаването, посочено в член 18, за всеки вид платежна операция, посочена в таблицата в приложението за съответния праг на освобождаване, когато наблюдаваният процент на измамите надвишава за две последователни тримесечия референтните стойности, приложими за този платежен инструмент или вид платежна операция за съответния праг на освобождаване.

3. След прекратяване на освобождаването, посочено в член 18, в съответствие с параграф 2 от настоящия член, доставчиците на платежни услуги нямат право да използват това освобождаване отново, докато техният процент на измамите не стане равен на или спадне под референтните проценти на измами, приложими за този вид платежна операция за съответния праг на освобождаване, в продължение на едно тримесечие.

4. Когато доставчиците на платежни услуги възнамеряват отново да използват освобождаването, посочено в член 18, те уведомяват компетентните органи в рамките на разумен срок и преди отново да използват освобождаването предоставят доказателство за възстановяване на съответствието на техния наблюдаван процент на измамите с приложимия референтен процент на измамите за съответния праг на освобождаване съгласно параграф 3 от настоящия член.

Член 21

Мониторинг

1. За да използват освобожданията, предвидени в членове 10—18, доставчиците на платежни услуги отчитат и наблюдават следните данни за всеки вид платежни операции, с разбивка за дистанционните и другите плащания поне веднъж на всяко тримесечие:

а) общата стойност на неразрешените платежни операции или на платежните операции с цел измама в съответствие с член 64, параграф 2 от Директива (ЕС) 2015/2366, общата стойност на всички платежни операции и полученият процент на измами, включително разбивка на платежни операции, инициирани чрез задълбочено установяване на идентичността на клиента и съгласно всяко от освобожданията;

б) средната стойност на операциите, включително разбивка на платежни операции, инициирани чрез задълбочено установяване на идентичността на клиента и съгласно всяко от изключенията;

в) броя на платежните операции, при които всяко от освобожданията е било приложено, и техния процент по отношение на общия брой платежни операции.

2. Доставчиците на платежни услуги предоставят резултатите от мониторинга в съответствие с параграф 1 на компетентните органи и на ЕБО, с предварително известие до съответния компетентен орган (или органи), при поискване от тяхна страна.

ГЛАВА IV

ПОВЕРИТЕЛНОСТ И ЦЯЛОСТ НА ПЕРСОНАЛИЗИРАНИТЕ СРЕДСТВА ЗА СИГУРНОСТ НА ПОЛЗВАТЕЛЯ НА ПЛАТЕЖНИ УСЛУГИ

Член 22

Общи изисквания

1. Доставчиците на платежни услуги гарантират поверителността и целостта на персонализираните средства за сигурност на ползвателя на платежни услуги, включително кодовете за установяване на идентичността, по време на всички фази на установяването на идентичността.

2. За целите на параграф 1 доставчиците на платежни услуги гарантират, че всяко от следните изисквания е спазено:

а) персонализираните средства за сигурност не са видими при изобразяване и не са четими в своята цялост, когато ползвателят на платежни услуги ги въвежда по време на установяване на идентичността;

б) персонализираните средства за сигурност във формат на данни, както и на криптографски материали, свързани с криптирането на персонализираните средства за сигурност, не се съхраняват в открит текст;

в) секретният криптографски материал е защитен от неразрешено оповестяване.

3. Доставчиците на платежни услуги документират целия процес, свързан с управлението на криптографски материал, използван за криптиране или за скриване по друг начин на персонализираните средства за сигурност.

4. Доставчиците на платежни услуги гарантират, че обработката и пренасочването на персонализирани средства за сигурност и на кодовете за установяване на идентичността, генерирани в съответствие с глава II, се осъществяват в сигурна среда в съответствие със строги и широко признати промишлени стандарти.

Член 23

Създаване и предаване на средствата за сигурност

Доставчиците на платежни услуги гарантират, че създаването на персонализирани средства за сигурност се осъществява в сигурна среда.

Те намаляват рисковете от неразрешено използване на персонализираните средства за сигурност и на устройствата и софтуера за установяване на идентичността, ако те бъдат изгубени, откраднати или копирани, преди да бъдат доставени на платеца.

Член 24

Свързване с ползвателя на платежни услуги

1. Доставчиците на платежни услуги гарантират, че само ползвателят на платежни услуги е асоцииран по сигурен начин с персонализираните средства за сигурност, устройствата и софтуера за установяване на идентичността.

2. За целите на параграф 1 доставчиците на платежни услуги гарантират, че всяко от следните изисквания е спазено:

а) свързването на идентичността на ползвателя на платежни услуги с персонализираните средства за сигурност, устройствата и софтуера за установяване на идентичността се извършва в сигурна среда, под контрола на доставчика на платежни услуги; това обхваща най-малко помещенията на доставчика на платежни услуги, интернет средата, предоставена от доставчика на платежни услуги, или други подобни сигурни уебсайтове, използвани от доставчика на платежни услуги и неговите терминални устройства АТМ, като се вземат под внимание рисковете, свързани с устройствата и свързаните с тях компоненти, използвани по време на процеса на свързване, които не се контролират от доставчика на платежни услуги;

б) свързването посредством дистанционен канал на идентичността на ползвателя на платежни услуги с персонализираните средства за сигурност и устройствата или софтуера за установяване на идентичността се извършва, като се използва задълбочено установяване на идентичността на клиента.

Член 25

Предоставяне на средства за сигурност и на устройства и софтуер за установяване на идентичността

1. Доставчиците на платежни услуги гарантират, че предоставянето на персонализирани средства за сигурност, устройства и софтуер за установяване на идентичността на ползвателя на платежни услуги се извършва по сигурен начин, с който се свежда до минимум рискът, свързан с неразрешеното им използване в резултат от тяхната загуба, кражба или копиране.

2. За целите на параграф 1 доставчиците на платежни услуги прилагат най-малко всяка от следните мерки:

а) ефективни и сигурни механизми на предоставяне, които гарантират, че персонализираните средства за сигурност, устройствата и софтуерът за установяване на идентичността са доставени на законния ползвател на платежни услуги;

б) механизми, които позволяват на доставчика на платежна услуга да провери автентичността на софтуера за установяване на идентичността на ползвателя на платежни услуги с помощта на интернет;

в) когато предоставянето на персонализирани средства за сигурност се осъществява извън помещенията на доставчика на платежни услуги или дистанционно — мерки, гарантиращи, че:

i) неупълномощени страни не могат да получат повече от една характеристика на персонализираните средства за сигурност, устройствата или софтуера за установяване на идентичността, когато се предоставят чрез един и същи канал;

ii) предоставените персонализирани средства за сигурност, устройствата или софтуера за установяване на идентичността изискват активиране преди употреба;

г) мерки, гарантиращи, че в случаите, когато персонализираните средства за сигурност, устройствата или софтуерът за установяване на идентичността трябва да бъдат активирани преди първото използване, активирането се извършва в сигурна среда в съответствие с процедурите за свързване, посочени в член 24.

Член 26

Подновяване на персонализираните средства за сигурност

Доставчиците на платежни услуги гарантират, че при подновяването или повторното активиране на персонализирани средства за сигурност се спазват процедурите за създаването, свързването и предоставянето на средствата за сигурност и на устройствата за установяване на идентичността в съответствие с членове 23, 24 и 25.

Член 27

Унищожаване, деактивиране и оттегляне

Доставчиците на платежни услуги гарантират, че разполагат с ефективни процедури, за да прилагат всяка от следните мерки за сигурност:

а) сигурното унищожаване, деактивиране или оттегляне на персонализираните средства за сигурност, устройствата и софтуера за установяване на идентичността;

б) когато доставчикът на платежни услуги разпространява устройства и софтуер за установяване на идентичността с цел повторна употреба, сигурното повторно използване на устройството или софтуера се установяват, документират и въвеждат преди предоставянето им на друг ползвател на платежни услуги;

в) деактивирането или оттеглянето на информация, свързана с персонализираните средства за сигурност, съхранявани в системите и базите данни на доставчика на платежни услуги и, когато е уместно, в публичните регистри.

ГЛАВА V

ОБЩИ И СИГУРНИ ОТВОРЕНИ СТАНДАРТИ ЗА КОМУНИКАЦИЯ

Раздел 1

Общи изисквания за комуникация

Член 28

Изисквания за идентификация

1. Доставчиците на платежни услуги гарантират сигурна идентификация при комуникацията между устройството на платеца и устройствата на получателя за приемане на електронни плащания, включително, но без да са ограничени до платежни терминали.

2. Доставчиците на платежни услуги гарантират, че рисковете, свързани с неправилното насочване на съобщение към неупълномощени страни при мобилните приложения и други видове интерфейси за ползватели на платежни услуги, в рамите на които се предлагат електронни платежни услуги, се намаляват успешно.

Член 29

Проследимост

1. Доставчиците на платежни услуги следва да разполагат с действащи процедури, които гарантират, че всички платежни операции и други взаимодействия с ползвател на платежни услуги, с други доставчици на платежни услуги, както и с други субекти, включително търговци, в контекста на предоставянето на платежни услуги, са проследими и осигуряват впоследствие знание за всички събития, които имат отношение към електронната операция във всичките ѝ различни етапи.

2. За целите на параграф 1 доставчиците на платежни услуги гарантират, че при всяко предаване на информация на ползвателя на платежни услуги, другите доставчици на платежни услуги и други субекти, включително търговци, са спазени всички изброени по-долу условия:

а) единния идентификационен код при предаване на информацията;

б) механизми за сигурност за подробното регистриране на операцията, включително номер на операцията, времеви печати и всички съответни данни за операцията;

в) времеви печати, които се основават на единна времева система и които са синхронизирани спрямо официален времеви сигнал.

Раздел 2

Специфични изисквания за общи и сигурни отворени стандарти за комуникация

Член 30

Общи задължения за интерфейсите за достъп

1. Доставчиците на платежни услуги, обслужващи сметка, които предлагат на даден платец платежна сметка, която е достъпна онлайн, трябва да разполагат с поне един интерфейс, който отговаря на всяко от следните изисквания:

а) доставчиците на услуги по предоставяне на информация за сметка, доставчиците на услуги по иницииране на плащане и доставчиците на платежни услуги, издаващи платежни инструменти, свързани с карти, са в състояние да се идентифицират пред доставчика на платежни услуги, обслужващ сметка;

б) доставчиците на услуги по предоставяне на информация за сметка са в състояние да комуникират в сигурна среда при искане и получаване на информация относно една или повече определени платежни сметки и свързаните с тях платежни операции;

в) доставчиците на услуги по иницииране на плащане са в състояние да комуникират по сигурен начин, за да инициират платежно нареждане от платежната сметка на платеца и да получават цялата информация относно инициирането на платежната операция и цялата информация, достъпна за доставчиците на платежни услуги, обслужващи сметка, във връзка с изпълнението на платежната операция.

2. За целите на установяването на идентичността на ползвателя на платежна сметка интерфейсът, посочен в параграф 1, позволява на доставчиците на услуги по предоставяне на информация за сметка и доставчиците на услуги по иницииране на плащане да използват всички процедури за установяване на идентичността, предоставени от доставчика на платежни услуги, обслужващ сметка, на ползвателя на платежни услуги.

Интерфейсът трябва най-малко да отговаря на всички посочени по-долу изисквания:

а) доставчикът на услуги по иницииране на плащане или доставчикът на услуги по предоставяне на информация за сметка трябва да са в състояние да възложат на доставчика на платежни услуги, обслужващ сметка, да започне установяването на идентичността въз основа на съгласието на ползвателя на платежни услуги;

б) предаването на информация между доставчика на платежни услуги, обслужващ сметка, и доставчика на услуги по предоставяне на информация за сметка, доставчика на услуги по иницииране на плащане и всеки съответен ползвател на платежни услуги се осъществява и поддържа по време на целия процес на установяване на идентичността;

в) поверителността и целостта на персонализираните средства за сигурност и на кодовете за установяване на идентичността, предавани от или чрез доставчика на услуги по иницииране на плащане или доставчика на услуги по предоставяне на информация за сметка, трябва да бъдат гарантирани.

3. Доставчиците на платежни услуги, обслужващи сметка, гарантират, че техните интерфейси следват стандарти за комуникация, които са издадени от международни или европейски организации по стандартизация.

Доставчиците на платежни услуги, обслужващи сметка, също така гарантират, че техническата спецификация на интерфейсите е документирана, като се посочва набор от рутинни действия, протоколи и инструменти, необходими на доставчиците на услуги по иницииране на плащане, доставчиците на услуги по предоставяне на информация за сметка и доставчиците на платежни услуги, издаващи платежни инструменти, свързани с карти, за да може техният софтуер и приложения да бъдат оперативно съвместими със системите за доставчиците на платежни услуги, обслужващи сметка.

Доставчиците на платежни услуги, обслужващи сметка — не по-малко от шест месеца преди датата на прилагане, посочена в член 38, параграф 2, или преди предвидената дата за пускането на пазара на интерфейса за достъп, когато пускането се извършва след датата, посочена в член 38, параграф 2 — трябва най-малко безплатно да предоставят документацията при поискване от упълномощените доставчици на услуги по иницииране на плащане и доставчиците на услуги по предоставяне на информация за сметка, или доставчиците на платежни услуги, издаващи платежни инструменти, свързани с карти, или доставчиците на платежни услуги, които са подали заявление до своите компетентни органи за съответния лиценз, както и да изготвят обобщение на документацията, публично достъпна на техния уебсайт.

4. В допълнение към параграф 3 доставчиците на платежни услуги, обслужващи сметка, гарантират, че, с изключение на извънредни ситуации, всяка промяна в техническата спецификация на техния интерфейс е достъпна за упълномощените доставчици на услуги по иницииране на плащане, доставчиците на услуги по предоставяне на информация за сметка и доставчиците на платежни услуги, издаващи платежни инструменти, свързани с карти, или доставчиците на платежни услуги, които са подали заявление до своите компетентни органи за издаване на съответния лиценз, възможно най-рано и не по-малко от 3 месеца преди промяната да бъде извършена.

Доставчиците на платежни услуги документират извънредните ситуации, възникващи при извършването на промените, и предоставят тази документация на компетентните органи при поискване.

5. Доставчиците на платежни услуги, обслужващи сметка, предоставят механизъм за изпитване, включително поддръжка, за изпитване на връзката и оперативно изпитване, за да се даде възможност на упълномощените доставчици на услуги по иницииране на плащане, доставчиците на платежни услуги, издаващи платежни инструменти, свързани с карти и на доставчиците на услуги по предоставяне на информация за сметка, или на доставчиците на платежни услуги, които са подали заявление за издаване на съответния лиценз, да изпитат своя софтуер и приложения, използвани за предоставянето на платежни услуги на ползвателите. Този механизъм следва да се предоставя не по-късно от шест месеца преди датата на прилагане, посочена в член 38, параграф 2, или преди предвидената дата за пускането на пазара на интерфейса за достъп, когато пускането се извършва след датата, посочена в член 38, параграф 2.

Механизмът за изпитване обаче не може да се използва за споделяне на чувствителна информация.

6. Компетентните органи гарантират, че доставчиците на платежни услуги, обслужващи сметка, спазват непрекъснато задълженията, включени в настоящите стандарти във връзка с интерфейса(ите), които те са въвели. В случай че доставчикът на платежни услуги не спазва изискванията за интерфейси, залегнали в настоящите стандарти, компетентните органи гарантират, че предоставянето на услуги по иницииране на плащане и услуги по предоставяне на информация за сметка не е възпрепятствано или нарушено дотолкова, доколкото съответните доставчици на такива услуги отговарят на условията, определени в член 33, параграф 5.

Член 31

Варианти на интерфейс за достъп

Доставчиците на платежни услуги, обслужващи сметка, създават интерфейса(ите), посочен(и) в член 30, чрез специален интерфейс или като позволят на доставчиците на платежни услуги, посочени в член 30, параграф 1, да използват интерфейсите, предназначени за установяване на идентичността и за комуникация с ползвателите на платежни услуги, предоставяни от доставчика на платежни услуги, обслужващ сметка.

Член 32

Задължения за специален интерфейс

1. При спазване на разпоредбите на членове 30 и 31 доставчиците на платежни услуги, обслужващи сметка, които са въвели специален интерфейс, гарантират, че този интерфейс предлага по всяко време същото ниво на достъпност и функциониране, включително поддръжка, като интерфейсите на разположение на ползвателя на платежни услуги за директен достъп до неговата платежна сметка онлайн.

2. Доставчиците на платежни услуги, обслужващи сметка, които са въвели специален интерфейс, определят прозрачни ключови показатели за изпълнението и цели за нивото на обслужване, които са поне толкова строги, колкото тези за интерфейса, използван от техните ползватели на платежни услуги както по отношение на достъпността, така и на данните, предоставени в съответствие с член 36. Тези интерфейси, показатели и цели се наблюдават от компетентните власти и се подлагат на стрес тестове.

3. Доставчиците на платежни услуги, обслужващи сметка, които са въвели специален интерфейс гарантират, че този интерфейс не създава пречки за предоставянето на услуги по иницииране на плащане и услуги по предоставяне на информация за сметка. Такива пречки могат да включват, наред с другото, предотвратяване на използването от страна на доставчиците на платежни услуги, посочени в член 30, параграф 1, на средствата за сигурност, издадени от доставчиците на платежни услуги, обслужващи сметка, на техните клиенти, налагане на пренасочване към процедурите по установяване на идентичността на доставчика на платежни услуги, обслужващ сметка, или към други функции, които изискват допълнителни лицензи и регистрации в допълнение към предвидените в членове 11, 14 и 15 от Директива (ЕС) 2015/2366, или които изискват допълнителни проверки на съгласието, предоставено от ползвателите на платежни услуги пред доставчиците на услуги по иницииране на плащане и доставчиците на услуги по предоставяне на информация за сметка.

4. За целите на параграфи 1 и 2 доставчиците на платежни услуги, обслужващи сметка, наблюдават достъпността и функционирането на специалния интерфейс. Доставчиците на платежни услуги, обслужващи сметка, публикуват на своя уебсайт на всеки три месеца статистически данни относно достъпността и функционирането на специалния интерфейс и интерфейса, използван от техните ползватели на платежни услуги.

Член 33

Извънредни мерки за специалния интерфейс

1. При проектирането на специалния интерфейс доставчиците на платежни услуги, обслужващи сметка, включват стратегия и планове за извънредни мерки, в случай че интерфейсът не работи в съответствие с член 32 и се стигне до непланирана недостъпност на интерфейса и прекъсване на работата на системите. Приема се, че непланирана недостъпност или прекъсване на работата на системите възникват при пет последователни искания за достъп до информация за предоставянето на услуги по иницииране на плащане или по предоставяне на информация за сметка, за които не е получен отговор в рамките на 30 секунди.

2. Извънредните мерки включват комуникационни планове, чрез които доставчиците на платежни услуги, използващи специалния интерфейс, биват уведомявани за мерките за възстановяване на системата и получават описание на непосредствено достъпните алтернативни възможности, които те могат да използват междувременно.

3. Както доставчиците на платежни услуги, обслужващи сметка, така и доставчиците на платежни услуги, посочени в член 30, параграф 1, докладват незабавно на съответните компетентни национални органи за проблеми със специалните интерфейси, както е посочено в параграф 1.

4. Като част от резервен механизъм, на доставчиците на платежни услуги, посочени в член 30, параграф 1, се разрешава да използват интерфейсите на разположение на ползвателите на платежни услуги за установяване на идентичността и за комуникация със своя доставчик на платежни услуги, обслужващ сметка, до момента на възстановяването на специалния интерфейс до нивото на достъпност и функциониране, предвидени в член 32.

5. За тази цел доставчиците на платежни услуги, обслужващи сметка, следва да гарантират, че доставчиците на платежни услуги, посочени в член 30, параграф 1, могат да бъдат идентифицирани и могат да използват процедурите за установяване на идентичността, предоставени от доставчика на платежни услуги, обслужващ сметка, на ползвателя на платежни услуги. Когато доставчиците на платежни услуги, посочени в член 30, параграф 1, използват интерфейса, посочен в параграф 4, те:

а) предприемат необходимите мерки, за да гарантират, че нямат достъп, не съхраняват или обработват данни за цели, различни от предоставянето на услугата, поискана от ползвателя на платежни услуги;

б) продължават да спазват задълженията, произтичащи съответно от член 66, параграф 3 и член 67, параграф 2 от Директива (ЕС) 2015/2366;

в) регистрират данните, до които е получен достъп чрез интерфейса, управляван от доставчика на платежни услуги, обслужващ сметка, за неговите ползватели на платежни услуги, и при поискване предоставят незабавно регистрационните файлове на своите компетентни национални органи;

г) при поискване надлежно и незабавно обосновават пред своя компетентен национален орган използването на интерфейса на разположение на ползвателите на платежни услуги за директен онлайн достъп до тяхната платежна сметка онлайн;

д) информират доставчика на платежни услуги, обслужващ сметка.

6. Компетентните органи, след консултация с ЕБО с цел да се гарантира последователно прилагане на следните условия, освобождават доставчиците на платежни услуги, обслужващи сметка, избрали специален интерфейс, от задължението за създаване на резервен механизъм, описано в параграф 4, когато този интерфейс отговаря на всички изброени по-долу условия:

а) той е в съответствие с всички задължения за специални интерфейси, както са посочени в член 32;

б) интерфейсът е проектиран и изпитан в съответствие с член 30, параграф 5, като отговаря на посочените в него изисквания на доставчиците на платежни услуги;

в) в продължение най-малко на три месеца доставчиците на платежни услуги са използвали активно интерфейса за предоставянето на услуги за информация за сметка, иницииране на плащане и предоставяне на потвърждение за наличието на средства за плащания, свързани с карти;

г) всички проблеми, свързани със специалния интерфейс, са незабавно отстранени.

7. Компетентните органи отнемат освобождаването, посочено в параграф 6, когато условията по букви а) и г) не са изпълнени от доставчиците на платежни услуги, обслужващи сметка, за повече от две последователни календарни седмици. Компетентните органи информират ЕБО за това оттегляне и гарантират, че доставчикът на платежни услуги, обслужващ сметка, във възможно най-кратък срок и най-късно в рамките на два месеца, ще създаде резервния механизъм, посочен в параграф 4.

Член 34

Удостоверения

1. За целите на идентификацията, както е предвидено в член 30, параграф 1, буква а), доставчиците на платежни услуги използват квалифицираните удостоверения за електронни печати, както е посочено в член 3, параграф 30 от Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета, или квалифицирано удостоверение за автентичност на уебсайт, посочено в член 3, параграф 39 от посочения регламент.

2. За целите на настоящия регламент регистрационният номер, както е посочено в официалните регистри в съответствие с приложение III, буква в) или приложение IV, буква в) към Регламент (ЕС) № 910/2014, е номерът на лиценза на доставчика на платежни услуги, издаващ платежни инструменти, свързани с карти, доставчиците на услуги по предоставяне на информация за сметка и доставчиците на услуги по иницииране на плащане, включително доставчиците на платежни услуги, обслужващи сметка, предоставящи такива услуги, вписани в публичния регистър на държавата членка по произход съгласно член 14 от Директива (ЕС) 2015/2366, или произтичащи от уведомленията за всеки лиценз, издаден съгласно член 8 от Директива 2013/36/ЕС на Европейския парламент и на Съвета ([1]), в съответствие с член 20 от посочената директива.

3. За целите на настоящия регламент квалифицираните удостоверения за електронни печати или за автентичност на уебсайт, посочени в параграф 1, включват (на езика, обичайно използван в сферата на международните финанси) допълнителни специфични характеристики във връзка с всички изброени по-долу аспекти:

а) ролята на доставчик на платежни услуги, която може да се изразява в една или повече от следните функции:

i) обслужване на сметка;

ii) иницииране на плащане;

iii) информация за платежна сметка;

iv) издаване на платежни инструменти, свързани с карти;

б) наименованието на компетентните органи, от които е регистриран доставчикът.

4. Характеристиките, посочени в параграф 3, не засягат оперативната съвместимост и признаването на квалифицираните удостоверения за електронни печати или за автентичност на уебсайт.

([1]) Директива 2013/36/ЕС на Европейския парламент и на Съвета от 26 юни 2013 г. относно достъпа до осъществяването на дейност от кредитните институции и относно пруденциалния надзор върху кредитните институции и инвестиционните посредници, за изменение на Директива 2002/87/ЕО и за отмяна на директиви 2006/48/ЕО и 2006/49/ЕО (ОВ L 176, 27.6.2013 г., стр. 338).

Член 35

Сигурност при предаването на информация

1. Доставчиците на платежни услуги, обслужващи сметка, доставчиците на платежни услуги, издаващи платежни инструменти, свързани с карти, доставчиците на услуги по предоставяне на информация за сметка и доставчиците на услуги по иницииране на плащане гарантират, че когато се обменят данни по интернет, се прилага сигурно криптиране между участниците в съобщението по време на съответното предаване на информация, за да се запази поверителността и целостта на данните, използвайки стабилни и широко признати техники за криптиране.

2. Доставчиците на платежни услуги, издаващи платежни инструменти, свързани с карти, доставчиците на услуги по предоставяне на информация за сметка и доставчиците на услуги по иницииране на плащане поддържат сесиите за достъп, предлагани от доставчиците на платежни услуги, обслужващи сметка, възможно най-кратки и от своя страна ги прекратяват в момента на приключване на исканото действие.

3. При поддържането на паралелни мрежови сесии с доставчика на платежни услуги, обслужващ сметка, доставчиците на услуги по предоставяне на информация за сметка и доставчиците на услуги по иницииране на плащане гарантират, че тези сесии са сигурно свързани със съответните сесии на ползвателя(ите) на платежни услуги, за да се предотврати възможността съобщение или информация, предавана между тях, да бъде погрешно пренасочена.

4. В комуникацията си с доставчика на платежни услуги, обслужващ сметка, доставчиците на услуги по предоставяне на информация за сметка, доставчиците на услуги по иницииране на плащане и доставчиците на платежни услуги, издаващи платежни инструменти, свързани с карти, посочват ясни позовавания на всеки един от следните елементи:

а) ползвателят или ползвателите на платежни услуги и съответното предаване на информация, за да се разграничат няколко искания от един и същ ползвател или ползватели на платежни услуги;

б) за услугите по иницииране на плащане — инициираната платежна операция с индивидуален номер;

в) за потвържденията за наличие на средства — искането с индивидуален номер, свързано със стойността, необходима за изпълнението на платежната операция, свързана с карти.

5. Доставчиците на платежни услуги, обслужващи сметка, доставчиците на услуги по предоставяне на информация за сметка, доставчиците на услуги по иницииране на плащане и доставчиците на платежни услуги, издаващи платежни инструменти, свързани с карти, гарантират, че когато съобщават персонализирани средства за сигурност и кодове за установяване на идентичността, те не са четими, пряко или косвено, в нито един момент от нито един служител.

В случай на нарушаване на поверителността на персонализираните средства за сигурност в рамките на тяхната компетентност, тези доставчици незабавно информират ползвателя на платежни услуги, асоцииран с тях, както и издателя на персонализирани средства за сигурност.

Член 36

Обмен на данни

1. Доставчиците на платежни услуги, обслужващи сметка, спазват всяко от следните изисквания:

а) те предоставят на доставчиците на услуги по предоставяне на информация за сметка същата информация от определени платежни сметки и свързаните с тях платежни операции на разположение на ползвателя на платежни услуги при пряко искане на достъп до информация за сметка, при условие че тази информация не включва чувствителни данни за плащанията;

б) незабавно след получаването на платежното нареждане, те предоставят на доставчиците на услуги по иницииране на плащане предоставят същата информация относно инициирането и изпълнението на платежната операция, предоставена или на разположение на ползвателя на платежни услуги, когато операцията е иницииранa директно от ползвателя;

в) при поискване те незабавно предоставят на доставчиците на платежни услуги потвърждение във формат „да“ или „не“ дали стойността, необходима за изпълнението на платежната операция, е налична по платежната сметка на платеца.

2. В случай на непредвидено събитие или грешка, възникнала по време на процеса на идентификация, установяване на идентичността или обмен на елементи от данни, доставчикът на платежни услуги, обслужващ сметка, изпраща уведомление до доставчика на услуги по иницииране на плащане, или на доставчика на услуги по предоставяне на информация за сметка, както и на доставчика на платежни услуги, който издава платежен инструмент, свързан с карта, в което се обяснява причината за непредвиденото събитие или грешка.

Когато доставчикът на платежни услуги, обслужващ сметка, предлага специален интерфейс в съответствие с член 32, интерфейсът следва да предоставя уведомления относно настъпването на непредвидени събития или грешки, които се съобщават от всеки доставчик на платежни услуги, който открива събитието или грешката, на другите доставчици на платежни услуги, участващи в предаването на информация.

3. Доставчиците на услуги по предоставяне на информация за сметка са длъжни да разполагат с подходящи и ефективни механизми за предотвратяване на достъпа до информация, различна от тази по определените платежни сметки и свързаните с тях платежни операции, в съответствие с изричното съгласие на ползвателя.

4. Доставчиците на услуги по иницииране на плащане предоставят на доставчиците на платежни услуги, обслужващи сметка, същата информация, поискана от ползвателя на платежни услуги при пряко иницииране на платежната операция.

5. Доставчиците на услуги по предоставяне на информация за сметка имат право на достъп до информация от определени платежни сметки и свързаните с тях платежни операции, с която доставчиците на платежни услуги, обслужващи сметка, разполагат за целите на услугите по предоставяне на информация за сметка, в един от следните два случая:

а) когато ползвателят на платежни услуги от своя страна е поискал такава информация;

б) когато ползвателят на платежни услуги от своя страна не е поискал такава информация — не повече от четири пъти за период от 24 часа със съгласието на ползвателя на платежни услуги, освен ако е договорена по-голяма честота между доставчика на услуги по предоставяне на информация за сметка и доставчика на платежни услуги, обслужващ сметката.

ГЛАВА VI

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Член 37

Преглед

Без да се засягат разпоредбите на член 98, параграф 5 от Директива (ЕС) 2015/2366 ЕБО извършва преглед до 14 март 2021 г. на процентите на измами, посочени в приложението към настоящия регламент, както и на освобождаванията, предоставени по силата на член 33, параграф 6, във връзка със специалните интерфейси и, ако е необходимо, представя на Комисията проекти за актуализация на тази информация в съответствие с член 10 от Регламент (ЕС) № 1093/2010.

Член 38

Влизане в сила

1. Настоящият регламент влиза в сила в деня след деня на публикуването му в *Официален вестник на Европейския съюз*.

2. Настоящият регламент се прилага от 14 септември 2019 г.

3. Член 30, параграфи 3 и 5 обаче се прилагат, считано от 14 март 2019 г.

Настоящият регламент е задължителен в своята цялост и се прилага пряко във всички държави членки.

Съставено в Брюксел на 27 ноември 2017 г.

За Комисията

Председател

Jean-Claude JUNCKER

ПРИЛОЖЕНИЕ

	Минимален референтен процент (%) на измами:	
Прагова стойност за освобождаване (ПСО)	Дистанционни електронни платежни операции, свързани с карти	Дистанционни електронни кредитни преводи
500 EUR	0,01	0,005
250 EUR	0,06	0,01
100 EUR	0,13	0,015