FRAMSELD REGLUGERÐ FRAMKVÆMDASTJÓRNARINNAR (ESB) 2018/389 2021/EES/66/05

frá 27. nóvember 2017

um viðbætur við tilskipun Evrópuþingsins og ráðsins (ESB) 2015/2366 að því er varðar tæknilega eftirlitsstaðla um sterka sannvottun viðskiptavina og almenna og örugga opna staðla vegna samskipta (*)

FRAMKVÆMDASTJÓRN EVRÓPUSAMBANDSINS HEFUR,

með hliðsjón af sáttmálanum um starfshætti Evrópusambandsins,,

með hliðsjón af tilskipun Evrópuþingsins og ráðsins (ESB) 2015/2366 frá 25. nóvember 2015 um greiðsluþjónustu á innri markaðnum, um breytingar á tilskipunum 2002/65/EB, 2009/110/EB og 2013/36/ESB og á reglugerð (ESB) nr. 1093/2010 og niðurfellingu á tilskipun 2007/64/EB ([1]), einkum annarri undirgrein 4. mgr. 98. gr.,

og að teknu tilliti til eftirfarandi:

1) Greiðsluþjónusta sem er boðin rafrænt ætti að vera framkvæmd á öruggan hátt með tækni sem getur tryggt örugga sannvottun notandans og dregið úr hættu á svikum, að því marki sem mögulegt er. Tilhögun sannvottunar ætti alla jafnan að fela í sér greiðsluvöktunarkerfi sem greina tilraunir til að nota persónubundin öryggisskilríki notanda greiðsluþjónustu sem hafa týnst, þeim stolið eða þau nýtt með ólöglegum hætti og ætti einnig að tryggja að notandi greiðsluþjónustu sé lögmætur notandi og veiti þar af leiðandi samþykki fyrir yfirfærslu fjármuna og aðgengi að upplýsingum um reikning sinn með venjulegri notkun á persónubundnum öryggisskilríkjum. Enn fremur er nauðsynlegt að tilgreina kröfurnar um sterka sannvottun viðskiptavina sem ætti að beita í hvert sinn sem greiðandi fer inn á greiðslureikning sinn á Netinu, virkjar rafræna greiðslu eða framkvæmir hvers konar aðgerð í gegnum fjarskipti, sem kann að hafa í för með sér hættu á greiðslusvikum eða annars konar misnotkun, með því að krefjast þess að búinn sé til sannvottunarkóði sem ekki er hægt að falsa, hvorki í heild eða með því að ljóstra upp um einhverja þá þætti sem liggja honum til grundvallar.

2) Þar sem sviksamlegar aðferðir taka stöðugum breytingum ættu kröfurnar um sterka sannvottun viðskiptavina að gera ráð fyrir nýsköpun í tæknilausnum til að bregðast við nýrri ógn hvað varðar öryggi rafrænna greiðslna. Til að tryggja að kröfurnar sem mæla skal fyrir um séu framkvæmdar á áframhaldandi skilvirkan hátt er einnig rétt að krefjast þess að öryggisráðstafanir vegna beitingar sterkrar sannvottunar viðskiptavina og undanþágur frá henni, ráðstafanir til að vernda trúnað og heilleika persónubundinna öryggisskilríkja og ráðstafanir sem koma á almennum og öruggum opnum samskiptastöðlum, séu skráð, þau prófuð með reglubundnum hætti, metin og endurskoðuð af rekstrarlega óháðum úttektaraðilum með sérfræðiþekkingu á öryggi í upplýsingatækni og rafrænum greiðslum. Til að heimila lögbærum yfirvöldum að vakta gæði úttektarinnar á þessum ráðstöfunum ætti að láta þeim slíkar úttektir í té samkvæmt beiðni.

3) Þar sem meiri hætta er á svikum þegar kemur að rafrænum fjargreiðslum er nauðsynlegt að gera frekari kröfur um sterka sannvottun viðskiptavina vegna slíkra greiðslna og tryggja þannig að þættirnir tengi greiðsluna með beinum hætti við tiltekna fjárhæð og tiltekinn viðtakanda sem greiðandinn tilgreinir þegar hann virkjar greiðsluna.

4) Beintenging er möguleg með myndun sannvottunarkóða sem falla undir strangar öryggiskröfur. Til að viðhalda tæknilegu hlutleysi ætti ekki að krefjast sérstakrar tækni við framkvæmd sannvottunarkóða. Því ættu sannvottunarkóðar að vera byggðir á lausnum líkt og myndun og sannreyningu einnota aðgangsorða, stafrænum undirskriftum eða öðrum áreiðanleikasönnunum með dulmáli með notkun lykla eða dulmálsefni sem geymt er í sannvottunarþáttum, svo fremi að öryggiskröfurnar séu uppfylltar.

(*) Þessi ESB-gerð birtist í Stjtíð. ESB L 69, 13.3.2018, bls. 23. Hennar var getið í ákvörðun sameiginlegu EES-nefndarinnar nr. 159/2020 frá 23. október 2020 um breytingu á IX. viðauka (Fjármálaþjónusta) við EES-samninginn (bíður birtingar).

([1]) Stjtíð. ESB L 337, 23.12.2015, bls. 35.

5) Nauðsynlegt er að mæla fyrir um sértækar kröfur með tilliti til aðstæðna þar sem lokafjárhæð er óþekkt á því augnabliki þegar greiðandi virkjar rafræna greiðslu í gegnum fjarskipti, til að tryggja að sterk sannvottun viðskiptavina eigi sérstaklega við um hámarksfjárhæðina sem greiðandi hefur gefið heimild fyrir eins og um getur í tilskipun (ESB) 2015/2366.

6) Til að tryggja að viðskiptavinir noti sterka sannvottun er einnig nauðsynlegt að krefjast viðeigandi öryggisráðstafana vegna þeirra þátta sterkrar sannvottunar sem flokkaðir eru sem „vitneskja“ (eitthvað sem einungis notandinn veit), svo sem lengd eða flækjustig, vegna þeirra þátta sem flokkaðir eru sem „umráð“ (eitthvað sem einungis eigandinn á), svo sem forskriftir algríms, lengd lykla og upplýsingaóreiða og vegna búnaðar og hugbúnaðar sem lesa þætti sem flokkaðir eru sem „eðlislægni“ (eitthvað sem notandinn er) svo sem algrímsforskriftir, líftölulegir nemar og búnaður til að vernda sniðmát, einkum til að milda áhættuna á að þessir þættir séu greindir, afhjúpaðir og notaðir af óviðkomandi aðilum. Einnig er nauðsynlegt að mæla fyrir um kröfur til að tryggja að þessir þættir séu sjálfstæðir þannig að brot á einum þætti hafi ekki áhrif á áreiðanleika hinna þáttanna, einkum þar sem einhverjir þessara þátta eru notaðir gegnum fjölnota tæki, einkum tæki s.s. spjaldtölvur eða farsíma sem bæði er hægt að nota til að veita leiðbeiningar um framkvæmd greiðslunnar og við sannvottunarferlið.

7) Kröfurnar um sterka sannvottun viðskiptavina eiga við um greiðslur sem greiðandi virkjar, óháð því hvort greiðandinn er einstaklingur eða lögaðili.

8) Greiðslur sem gerðar eru með notkun nafnlausra greiðslumiðla falla eðli sínu samkvæmt ekki undir kvöðina um stranga sannvottun. Þegar nafnleynd slíkra miðla er aflétt á grundvelli samninga eða löggjafar, falla greiðslur undir öryggiskröfurnar sem leiða af tilskipun (ESB) 2015/2366 og þessum tæknilega eftirlitsstaðli.

9) Í samræmi við tilskipun (ESB) 2015/2366 hafa undanþágur á meginreglunni um sterka sannvottun viðskiptavina verið skilgreindar á grundvelli áhættu, fjárhæðar, endurtekningar og greiðsluleiðarinnar sem notuð er við framkvæmd færslunnar.

10) Aðgerðir sem fela í sér aðgang að stöðu og nýlegum greiðslum greiðslureiknings án þess að ljóstra upp um viðkvæm greiðslugögn, endurteknar greiðslur til sömu viðtakenda greiðslna sem hafa áður verið myndaðar eða staðfestar af greiðanda með notkun sterkrar sannvottunar viðskiptavina og greiðslur til og frá sama einstaklingi eða lögaðila með reikninga hjá sama greiðsluþjónustuveitanda, valda lítilli áhættu og því þurfa greiðsluþjónustuveitendur ekki að nota sterka sannvottun í slíkum tilvikum. Þrátt fyrir litla áhættu er rétt að nefna að í samræmi við 65., 66. og 67. gr. tilskipunar (ESB) 2015/2366 ættu greiðsluvirkjendur, greiðsluþjónustuveitendur sem gefa út kortatengda greiðslumiðla og reikningsupplýsingaþjónustuveitendur einungis að biðja um og fá nauðsynlegar og mikilvægar upplýsingar hjá greiðsluþjónustuveitanda sem veitir reikningsþjónustu til að veita tiltekna greiðsluþjónustu með samþykki notanda greiðsluþjónustu. Gefa má slíkt samþykki fyrir hverja upplýsingabeiðni eða fyrir hverja greiðslu sem á að virkja eða, fyrir reikningsupplýsingaþjónustuveitendur, sem umboð fyrir tiltekna greiðslureikninga og tengdar greiðslur eins og kveðið er á um í bindandi samningi við notanda greiðsluþjónustu.

11) Undanþágur vegna lágra upphæða snertilausra greiðslna á sölustað, sem einnig taka tillit til hámarksfjölda samfelldra greiðslna eða tiltekinnar fastrar hámarksfjárhæðar samfelldrar greiðslna án þess að til komi sterk sannvottun viðskiptavina, gera kleift að þróa notendavæna og áhættulitla greiðsluþjónustu og því ætti að gera ráð fyrir þeim. Einnig er rétt að kveða á um undanþágur þegar um er að ræða rafrænar greiðslur sem virkjaðar eru við ómannaðar skjástöðvar þar sem ekki er alltaf auðvelt að nota sterka sannvottun viðskiptavina vegna rekstrarlegra ástæðna (t.d. til að forðast biðraðir og möguleg slys við tollhlið eða vegna annarrar öryggisáhættu).

12) Eins og fyrir undanþáguna fyrir lágar upphæðir snertilausra greiðslna á sölustað er nauðsynlegt að finna jafnvægi milli annars vegar áhuga á auknu öryggi við fjargreiðslur og notendavænleika og hins vegar aðgengis að greiðslum á sviði rafrænnar verslunar. Samkvæmt þessum meginreglum ætti að setja viðmiðunarmörk, á varfærinn hátt, um að ekki þurfi að nota sterka sannvottun viðskiptavina vegna fjárhæða undir þeim, þannig að þau takmarkist við verslun á netinu fyrir lágar fjárhæðir. Viðmiðunarmörk fyrir kaup á Netinu ættu að vera sett af varfærni, með það í huga að einstaklingurinn er ekki sjálfur á staðnum þegar kaupin eru gerð, sem veldur aðeins meiri öryggisáhættu.

13) Kröfurnar um sterka sannvottun viðskiptavina gilda um greiðslur sem greiðandi virkjar, óháð því hvort greiðandinn er einstaklingur eða lögaðili. Margar fyrirtækjagreiðslur eru virkjaðar gegnum sérnota ferli eða samskiptareglur sem tryggja öflugt greiðsluöryggi sem tilskipun (ESB) 2015/2366 er ætlað að ná með sterkri sannvottun viðskiptavina. Ef lögbær yfirvöld komast að raun um að þessi ferli og samskiptareglur, sem eru einungis aðgengilegar greiðendum sem eru ekki neytendur, fullnægi markmiðum tilskipunar (ESB) 2015/2366 að því er varðar öryggi, geta greiðsluþjónustuveitendur, að því er varðar þessi ferli og samskiptareglur, verið undanþegnir kröfunum um sterka sannvottun viðskiptavina.

14) Ef um er að ræða áhættugreiningu greiðslna í rauntíma sem flokkar greiðslu sem litla áhættu, er einnig viðeigandi að innleiða undanþágu fyrir greiðsluþjónustuveitandann sem ætlar ekki að nota sterka sannvottun viðskiptavina með því að taka upp skilvirkar og áhættutengdar kröfur sem tryggja öryggi fjármuna og persónuupplýsinga notanda greiðsluþjónustu. Þessar áhættutengdu kröfur ættu að sameina niðurstöður áhættugreininga og staðfesta að ekki hafi greinst óeðlilegt útgjalda- eða hegðunarmynstur greiðanda, að teknu tilliti til annarra áhættuþátta, þ.m.t. upplýsinga um staðsetningu greiðanda og viðtakanda greiðslu með viðmiðunarmörk fjárhæða sem byggjast á svikahlutfalli sem reiknað er fyrir fjargreiðslur. Þegar ekki er hægt að skilgreina greiðslu með litla áhættu á grundvelli áhættugreiningar greiðslna í rauntíma skulu greiðsluþjónustuveitendur taka aftur upp sterka sannvottun viðskiptavina. Hámarksfjárhæð slíkra áhættutengdra undanþága ætti að ákveða þannig að það tryggi samsvarandi mjög lágt hlutfall svika, einnig í samanburði við svikahlutföll allra greiðslna greiðsluþjónustuveitandans, þ.m.t. þeirra sem eru sannvottaðir með sterkri sannvottun viðskiptavina, innan tiltekins tímabils og á áframhaldandi grundvelli.

15) Til að tryggja skilvirka framkvæmd ættu greiðsluþjónustuveitendur sem vilja nýta sér undanþágu frá sterkri sannvottun að vakta reglulega og láta lögbærum yfirvöldum og Evrópsku bankaeftirlitsstofnuninni í té, óski þeir þess, virði sviksamlegra eða óheimilla greiðslna og hlutfall svika sem hafa orðið uppvís fyrir allar greiðslufærslur þeirra, brotið niður á hverja tegund greiðslu, hvort sem þær eru sannvottaðar með sterkri sannvottun viðskiptavina eða framkvæmdar á grundvelli viðeigandi undanþágu.

16) Söfnun á þessum nýju gögnum byggðum á sögu um svikahlutföll rafrænna greiðslna mun einnig stuðla að skilvirkri endurskoðun af hálfu Evrópsku bankaeftirlitsstofnunarinnar á fjárhæðarmörkum undanþágu frá sterkri sannvottun viðskiptavina byggðri á áhættugreiningu greiðslna í rauntíma. Evrópska bankaeftirlitsstofnunin ætti að endurskoða þessa tæknilegu eftirlitsstaðla og eftir því sem við á leggja drög að uppfærslu á þeim fyrir framkvæmdastjórnina í formi nýrra draga að fjárhæðarmörkum og samsvarandi svikahlutföllum með það í huga að auka öryggi rafrænna fjargreiðslna, í samræmi við 5. mgr. 98. gr. tilskipunar (ESB) 2015/2366 og 10. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 1093/2010 ([1]).

17) Greiðsluþjónustuveitendur sem nýta sér einhverja af undanþágunum sem heimilar eru ættu ætíð að geta valið að nota sterkra sannvottun viðskiptavina vegna aðgerðanna og greiðslufærslnanna sem um getur í þessum ákvæðum.

18) Ráðstafanirnar sem vernda trúnað og heilleika persónubundinna öryggisskilríkja sem og sannvottunarbúnað og -hugbúnað ættu að takmarka áhættuna í tengslum við svik í gegnum óheimila eða sviksama notkun á greiðslumiðli og óheimilan aðgang að greiðslureikningum. Í þessu skyni er nauðsynlegt að innleiða kröfur um örugga myndun og afhendingu persónubundinna öryggisskilríkja og tengingu þeirra við notanda greiðsluþjónustu og til að kveða á um skilyrði fyrir endurnýjun og afturköllun þessara skilríkja.

19) Til að tryggja skilvirk og örugg samskipti milli viðeigandi þátttakenda í tengslum við reikningsupplýsingaþjónustu, greiðsluvirkjun og staðfestingu á tiltækileika fjármuna er nauðsynlegt að tilgreina kröfurnar um almenna og örugga opna samskiptastaðla sem allir viðkomandi greiðsluþjónustuveitendur eiga að uppfylla. Í tilskipun (ESB) 2015/2366 er kveðið á um aðgengi að og notkun greiðsluþjónustuveitenda á upplýsingum um greiðslureikning. Reglugerð þessi breytir þar af leiðandi ekki reglunum um aðgengi að reikningum öðrum en greiðslureikningum.

([1]) Reglugerð Evrópuþingsins og ráðsins (ESB) nr. 1093/2010 frá 24. nóvember 2010 um að koma á fót evrópskri eftirlitsstofnun (Evrópska bankaeftirlitsstofnunin), um breytingu á ákvörðun nr. 716/2009/EB og niðurfellingu ákvörðunar framkvæmdastjórnarinnar 2009/78/EB (Stjtíð. ESB L 331, 15.12.2010, bls. 12).

20) Hver greiðsluþjónustuveitandi sem veitir reikningsþjónustu með greiðslureikninga sem eru aðgengilegir á Netinu ætti að bjóða a.m.k. einn aðgangsskilflöt sem tryggir örugg samskipti við reikningsupplýsingaþjónustuveitendur, greiðsluvirkjendur og greiðsluþjónustuveitendur sem gefa út kortatengda greiðslumiðla. Skilflöturinn ætti að gera reikningsupplýsingaþjónustuveitendum, greiðsluvirkjendum og greiðsluþjónustuveitendum sem gefa út kortatengda greiðslumiðla kleift að auðkenna sig hjá greiðsluþjónustuveitanda sem veitir reikningsþjónustu. Hann ætti einnig að gera reikningsupplýsingaþjónustuveitendum og greiðsluvirkjendum kleift að treysta á sannvottunarferlið sem greiðsluþjónustuveitandi sem veitir reikningsþjónustu veitir notanda greiðsluþjónustu. Til að tryggja hlutleysi tækni og viðskiptalíkans ætti greiðsluþjónustuveitendum sem veita reikningsþjónustu að vera frjálst að ákveða hvort þeir bjóði skilflöt sem er sérstaklega ætlaður fyrir samskipti við reikningsupplýsingaþjónustuveitendur, greiðsluvirkjendur og greiðsluþjónustuveitendur sem gefa út kortatengda greiðslumiðla, eða að heimila, fyrir þessi samskipti, notkun skilflatar til auðkenningar og samskipta við notendur greiðsluþjónustu greiðsluþjónustuveitanda sem veitir reikningsþjónustu.

21) Til að gera reikningsupplýsingaþjónustuveitendum, greiðsluvirkjendum og greiðsluþjónustuveitendum sem gefa út kortatengda greiðslumiðla kleift að þróa tæknilausnir sínar, ættu tækniforskriftir skilflatarins að vera skjalfestar á fullnægjandi hátt og gerðar aðgengilegar öllum. Auk þess ætti greiðsluþjónustuveitandi sem veitir reikningsþjónustu að bjóða aðstöðu sem gerir greiðsluþjónustuveitendum kleift að prófa tæknilausnirnar a.m.k. 6 mánuðum fyrir gildistökudag þessara eftirlitsstaðla eða, ef útgáfa skilflatarins á sér stað eftir gildistökudag þessara staðla, fyrir dagsetninguna þegar skilflöturinn verður settur á markað. Til að tryggja samvirkni ólíkra tæknilegra samskiptalausna ætti skilflöturinn að nota samskiptastaðla sem þróaðir eru af alþjóðlegum- eða evrópskum staðlastofnunum.

22) Gæði þjónustunnar sem reikningsupplýsingaþjónustuveitendur og greiðsluvirkjendur veita mun fara eftir réttri starfsemi skilflatarins sem greiðsluþjónustuveitendur sem veita reikningsþjónustu koma á eða aðlaga. Því er nauðsynlegt að grípa til aðgerða til að tryggja rekstrarsamfellu sem nýtist notendum þessarar þjónustu uppfylli slíkur skilflötur ekki kröfur þessara staðla. Það er á ábyrgð lögbærra landsyfirvalda að tryggja að reikningsupplýsingaþjónustuveitendur og greiðsluvirkjendur séu ekki stöðvaðir eða hindraðir við veitingu þjónustu sinnar.

23) Þegar aðgengi að greiðslureikningum er veitt um sérhæfða skilfleti er nauðsynlegt að krefjast þess að sérhæfðu skilfletirnir séu jafn aðgengilegir og afköstin jafn góð og í skilfletinum sem er tiltækur notanda greiðsluþjónustu til að tryggja rétt notenda greiðsluþjónustu til að nota greiðsluvirkjendur og þjónustu sem veita aðgang að reikningsupplýsingum eins og kveðið er á um í tilskipun (ESB) 2015/2366. Greiðsluþjónustuveitendur sem veita reikningsþjónustu ættu einnig að skilgreina gagnsæja lykilárangursvísa og markmið þjónustunnar fyrir aðgengileika og afkastagetu sérhæfðra skilflata sem eru a.m.k. jafnstrangir og þeir sem settir fyrir skilflötinn sem notaður er fyrir notendur greiðsluþjónustu þeirra. Greiðsluþjónustuveitendur sem munu nota þessa skilfleti ættu að prófa þá og lögbær yfirvöld ættu að framkvæma álagspróf á þeim og hafa eftirlit með þeim.

24) Til að tryggja að greiðsluþjónustuveitendur sem treysta á sérhæfðan skilflöt geti haldið áfram að veita þjónustu ef upp koma vandamál við aðgengileika eða ófullnægjandi afköst er nauðsynlegt að kveða á um, með ströngum skilyrðum, varabúnað sem myndi gera slíkum veitendum kleift að nota skilflötinn sem greiðsluþjónustuveitandinn sem veitir reikningsþjónustu viðheldur fyrir auðkenningu á og samskiptum við eigin notendur greiðsluþjónustu. Tilteknir greiðsluþjónustuveitendur sem veita reikningsþjónustu verða undanþegnir frá því að þurfa að láta í té slíkan varabúnað um notendaskilfleti sína þegar lögbær yfirvöld þeirra staðreyna að sérhæfðu skilfletirnir uppfylla sértæk skilyrði sem tryggja óhindraða samkeppni. Ef sérhæfðu skilfletirnir sem eru undanþegnir uppfylla ekki sett skilyrði skulu lögbær yfirvöld fella veitta undanþágu úr gildi.

25) Til að gera lögbærum yfirvöldum kleift að hafa eftirlit með og vakta á skilvirkan hátt framkvæmd og stjórnun samskiptaskilflata ættu greiðsluþjónustuveitendur sem veita reikningsþjónustu að gera samantekt á viðkomandi skjölum aðgengilega á vefsetri sínu og, ef þess er óskað, miðla til lögbærra yfirvalda upplýsingaskjölum um lausnir ef brýn þörf krefur. Greiðsluþjónustuveitendur sem veita reikningsþjónustu ættu einnig að gera tölfræðilegar upplýsingar um aðgengi og afköst þess skilflatar aðgengilegar öllum.

26) Til að vernda trúnað og heilleika gagna er nauðsynlegt að tryggja öryggi samskiptalota milli greiðsluþjónustuveitenda sem veita reikningsþjónustu, reikningsupplýsingaþjónustuveitenda, greiðsluvirkjenda og greiðsluþjónustuveitenda sem gefa út kortatengda greiðslumiðla. Einkum er nauðsynlegt að krefjast þess að öruggri dulkóðun sé beitt milli

reikningsupplýsingaþjónustuveitenda, greiðsluvirkjenda, greiðsluþjónustuveitenda sem gefa út kortatengda greiðslumiðla og greiðsluþjónustuveitenda sem veita reikningsþjónustu þegar gagnaskipti eiga sér stað.

27) Til að efla traust notenda og tryggja sterka sannvottun viðskiptavina ætti að taka tillit til notkunar rafrænnar auðkenningar og traustþjónustu eins og hún er sett fram í reglugerð Evrópuþingsins og ráðsins (ESB) nr. 910/2014 ([1]), einkum að því er varðar tilkynnt rafræn auðkenningarkerfi.

28) Til að tryggja samræmda gildistökudaga ætti þessi reglugerð að gilda frá sömu dagsetningu og þeirri þegar aðildarríki þurfa að tryggja að öryggisráðstöfunum sem um getur í 65., 66., 67. og 97. gr. tilskipunar (ESB) 2015/2366 sé beitt.

29) Reglugerð þessi byggist á drögum að tæknilegum eftirlitsstöðlum sem Evrópska bankaeftirlitsstofnunin (EBA) hefur lagt fyrir framkvæmdastjórnina.

30) Evrópska bankaeftirlitsstofnunin hefur haft opið og gagnsætt samráð við almenning um drögin að tæknilegum eftirlitsstöðlunum sem þessi reglugerð byggist á, greint mögulegan tengdan kostnað og ávinning og óskað eftir áliti hagsmunahópsins um bankastarfsemi í samræmi við 37. gr. reglugerðar (ESB) nr. 1093/2010.

SAMÞYKKT REGLUGERÐ ÞESSA:

I. KAFLI

ALMENN ÁKVÆÐI

1. gr.

Viðfangsefni

Í þessari reglugerð eru settar fram kröfur sem greiðsluþjónustuveitendur eiga að fara að í þeim tilgangi að koma á öryggisráðstöfunum sem gera þeim kleift að gera eftirfarandi:

a) beita ferli sterkrar sannvottunar viðskiptavina í samræmi við 97. gr. tilskipunar (ESB) 2015/2366,

b) veita undanþágu frá beitingu öryggiskrafna um sterka sannvottun viðskiptavina, með fyrirvara um tilgreind og takmörkuð skilyrði á grundvelli áhættu, fjárhæðar og endurtekningar á greiðslu og greiðsluleiðar sem notuð er við framkvæmdina,

c) vernda trúnað og heilleika persónubundinna öryggisskilríkja notanda greiðsluþjónustu,

d) koma á almennum og öruggum opnum stöðlum vegna samskipta milli greiðsluþjónustuveitenda sem veita reikningsþjónustu, greiðsluvirkjenda, reikningsupplýsingaþjónustuveitenda, greiðenda, viðtakenda greiðslu og annarra greiðsluþjónustuveitenda í tengslum við veitingu og notkun greiðsluþjónustu við beitingu IV. bálks tilskipunar (ESB) 2015/2366.

2. gr.

Almennar sannvottunarkröfur

1. Greiðsluþjónustuveitendur skulu hafa til staðar greiðsluvöktunarkerfi sem gera þeim kleift að greina óheimilar eða sviksamlegar greiðslur í þeim tilgangi að framkvæma þær öryggisráðstafanir sem um getur í a- og b-lið 1. gr.

([1]) Reglugerð Evrópuþingsins og ráðsins (ESB) nr. 910/2014 frá 23. júlí 2014 um rafræna auðkenningu og traustþjónustu fyrir rafræn viðskipti á innri markaðinum og um niðurfellingu á tilskipun 1999/93/EB (Stjtíð. ESB L 257, 28.8.2014, bls. 53).

Þessi kerfi skulu byggjast á greiningu á greiðslum að teknu tilliti til þátta sem eru einkennandi fyrir notendur greiðsluþjónustu við þessar aðstæður þar sem persónubundin öryggisskilríki eru notuð með venjubundnum hætti.

2. Greiðsluþjónustuveitendur skulu tryggja að greiðsluvöktunarkerfi taki að lágmarki tillit til allra eftirfarandi áhættutengdra þátta:

a) skráa yfir sannvottunarþætti sem eru í röngum höndum eða stolnir,

b) fjárhæðar hverrar greiðslu,

c) þekktra sviðsmynda svika í sambandi við veitingu greiðsluþjónustu,

d) ummerkja um árás spilliforrita í lotum sannvottunarferlisins,

e) ef aðgangsbúnaður eða hugbúnaður kemur frá greiðsluþjónustuveitanda, skráa yfir notkun aðgangsbúnaðarins eða hugbúnaðarins sem veittur er notanda greiðsluþjónustu og óeðlilegrar notkunar aðgangsbúnaðarins eða hugbúnaðarins.

3. gr.

Úttekt á öryggisráðstöfunum

1. Framkvæmd öryggisráðstafana sem um getur í 1. gr. skal skjalfest, hún prófuð með reglubundnum hætti, metin og tekin út í samræmi við viðeigandi lagaramma greiðsluþjónustuveitanda, af úttektaraðilum með sérfræðiþekkingu á sviði öryggis í upplýsingatækni og greiðslum og eru rekstrarlega óháðir greiðsluþjónustuveitandanum.

2. Tímabilið á milli úttekta sem um getur í 1. mgr. skal ákvarðað með tilliti til viðeigandi umgjarðar um reikningsskil og lögboðna endurskoðun sem gildir um greiðsluþjónustuveitandann.

Greiðsluþjónustuveitendur sem nota undanþáguna sem um getur í 18. gr. skulu að minnsta kosti árlega sæta úttekt á aðferðafræði sinni, líkaninu sem notað er og svikahlutfallinu sem tilkynnt er um. Úttektaraðilinn sem framkvæmir úttektina skal hafa sérfræðiþekkingu á sviði öryggis í upplýsingatækni og greiðslum og vera rekstrarlega óháður greiðsluþjónustuveitandanum. Á fyrsta ári þegar undanþágan í 18. gr. er nýtt og a.m.k. á 3 ára fresti eftir það, eða oftar ef lögbært yfirvald óskar eftir því, skal úttektin framkvæmd af óháðum, utanaðkomandi úttektaraðila sem hefur réttindi og er til þess hæfur.

3. Í þeirri úttekt skal meta og skýra frá því hvort öryggisráðstafanir greiðsluþjónustuveitanda fullnægja kröfunum sem settar eru fram í þessari reglugerð.

Skýrslan í heild sinni skal gerð aðgengileg lögbærum yfirvöldum að beiðni þeirra.

II. KAFLI

ÖRYGGISRÁÐSTAFANIR VEGNA NOTKUNAR STERKRAR SANNVOTTUNAR VIÐSKIPTAVINA

4. gr.

Sannvottunarkóði

1. Þegar greiðsluþjónustuveitendur notast við sterka sannvottun viðskiptavina í samræmi við 1. mgr. 97. gr. tilskipunar 2015/2366 skal sannvottunin grundvallast á tveimur eða fleiri þáttum sem eru flokkaðir sem vitneskja, umráð og eðlislægni og skal leiða til myndunar sannvottunarkóða.

Sannvottunarkóðinn skal einungis samþykktur einu sinni af greiðsluþjónustuveitanda þegar greiðandi notar sannvottunarkóða til að fá aðgang að greiðslureikningi sínum í gegnum Netið, til að hefja rafræna greiðslu eða til að nota einhverja aðra aðgerð í gegnum fjarskipti sem kann að hafa í för með sér hættu á greiðslusvikum eða annars konar misnotkun.

2. Að því er varðar 1. mgr. skulu greiðsluþjónustuveitendur gera öryggisráðstafanir sem tryggja að öll eftirfarandi skilyrði séu uppfyllt:

a) ekki sé hægt að fá upplýsingar um neina þá þætti sem um getur í 1. mgr. út frá birtingu sannvottunarkóðans,

b) ekki sé mögulegt að mynda nýjan sannvottunarkóða byggðan á vitneskju um aðra sannvottunarkóða sem áður hafa verið myndaðir,

c) ekki sé hægt að falsa sannvottunarkóðann.

3. Greiðsluþjónustuveitendur skulu tryggja að sannvottun með myndun sannvottunarkóða feli í sér allar eftirfarandi ráðstafanir:

a) þegar sannvottun fyrir fjaraðgang, rafrænar fjargreiðslur og einhverjar aðrar aðgerðir í gegnum fjarskipti sem kann að hafa í för með sér hættu á greiðslusvikum eða annars konar misnotkun, hefur ekki náð að mynda sannvottunarkóða að því er varðar 1. mgr., sé ekki mögulegt að greina hver þáttanna sem um getur í þeirri málsgrein var rangur,

b) hámarksfjöldi misheppnaðra tilrauna til sannvottunar sem hægt er að framkvæma í röð, en eftir það skal tímabundið eða endanlega lokað á aðgerðirnar sem um getur í 1. mgr. 97. gr. tilskipunar (ESB) 2015/2366, sé fimm skipti á tilgreindu tímabili,

c) samskiptaloturnar séu varðar stuldi á sannvottunargögnum sem miðlað er við sannvottun og gegn misnotkun óviðkomandi aðila í samræmi við kröfurnar í 5. kafla,

d) hámarkstími án aðgerða af hálfu greiðanda eftir sannvottun hans til að fá aðgang að reikningi sínum á Netinu fari ekki yfir 5 mínútur.

4. Ef lokunin sem um getur í b-lið 3. mgr. er tímabundin skal tímalengd þeirrar lokunar og fjöldi endurtekinna tilrauna vera staðfestur á grundvelli einkenna þjónustunnar sem veitt er greiðanda og allri viðkomandi áhættu, að teknu tilliti til, að lágmarki, þáttanna sem um getur í 2. mgr. 2. gr.

Greiðanda skal gera viðvart áður en lokun er gerð varanleg.

Þegar lokun hefur verið gerð varanleg skal komið á öruggri verklagsreglu sem gerir greiðanda kleift að nota aftur lokaða rafræna greiðslumiðla.

5. gr.

Beintenging

1. Ef greiðsluþjónustuveitendur nota sterka sannvottun viðskiptavina í samræmi við 2. mgr. 97. gr. tilskipunar (ESB) 2015/2366 skulu þeir einnig gera öryggisráðstafanir sem uppfylla allar eftirfarandi kröfur, til viðbótar við kröfurnar í 4. gr. þessarar reglugerðar:

a) greiðandinn er upplýstur um fjárhæð greiðslunnar og viðtakanda greiðslunnar,

b) sannvottunarkóðinn sem er myndaður er sértækur fyrir fjárhæð greiðslunnar og viðtakanda greiðslunnar sem greiðandinn samþykkti þegar hann virkjaði greiðsluna,

c) sannvottunarkóðinn sem greiðsluþjónustuveitandinn samþykkir samsvarar upphaflegri sértækri fjárhæð greiðslunnar og auðkenni viðtakanda greiðslunnar sem greiðandinn samþykkir,

d) allar breytingar á fjárhæðinni eða viðtakanda greiðslu leiða til ógildingar á sannvottunarkóðanum sem myndaður var.

2. Að því er varðar 1. mgr. skulu greiðsluþjónustuveitendur taka upp öryggisráðstafanir sem tryggja leynd, sannvottaðan uppruna og heilleika alls eftirfarandi:

a) fjárhæð greiðslunnar og viðtakanda greiðslunnar gegnum alla áfanga sannvottunarinnar,

b) upplýsingarnar sem birtar eru greiðanda gegnum alla áfanga sannvottunarinnar, þ.m.t. myndun, miðlun og notkun sannvottunarkóðans.

3. Að því er varðar b-lið 1. mgr. og þegar greiðsluþjónustuveitendur notast við sterka sannvottun viðskiptavina í samræmi við 2. mgr. 97. gr. tilskipunar (ESB) 2015/2366, skulu eftirfarandi kröfur fyrir sannvottunarkóða gilda:

a) í tengslum við kortatengdar greiðslur þar sem greiðandi hefur gefið samþykki fyrir nákvæmlega þeirri fjárhæð sem fyrirhugað er að frysta skv. 1. mgr. 75. gr. þeirrar tilskipunar skal sannvottunarkóðinn vera sértækur fyrir fjárhæðina sem greiðandi hefur gefið samþykki fyrir að frysta og samþykkt af greiðanda þegar hann virkjar greiðsluna,

b) í tengslum við greiðslur þar sem greiðandi hefur gefið samþykki fyrir framkvæmd bunka af rafrænum fjargreiðslum til eins eða fleiri viðtakenda greiðslu skal sannvottunarkóðinn vera sértækur fyrir heildarfjárhæð greiðslubunkans og fyrir tilgreinda viðtakenda greiðslu.

6. gr.

Kröfur vegna þátta sem flokkast sem vitneskja

1. Greiðsluþjónustuveitendur skulu gera ráðstafanir til að milda áhættuna á því að óviðkomandi aðilar geti greint þætti sterkrar sannvottunar viðskiptavina, sem flokkast sem vitneskja, eða að þeir séu upplýstir um þá.

2. Þegar greiðandi notar þessa þætti eiga mildunarráðstafanirnar að koma í veg fyrir að óviðkomandi aðilar séu upplýstir um þá.

7. gr.

Kröfur vegna þátta sem flokkast sem umráð

1. Greiðsluþjónustuveitendur skulu gera ráðstafanir til að milda áhættuna á því að óviðkomandi aðilar noti þætti sterkrar sannvottunar sem flokkast sem umráð.

2. Þegar greiðandi notar þessa þætti eiga til þess gerðar ráðstafanir að koma í veg fyrir eftirmyndun þeirra.

8. gr.

Kröfur vegna búnaðar og hugbúnaðar sem tengjast þáttum sem flokkast sem eðlislægni

1. Greiðsluþjónustuveitendur skulu gera ráðstafanir til að milda áhættuna á því að sannvottunarþættir sem flokkast sem eðlislægni og eru lesnir af búnaði og hugbúnaði sem greiðandanum er látið í té séu greindir af óviðkomandi aðilum. Að lágmarki skulu greiðsluþjónustuveitendur tryggja að mjög litlar líkur séu á því að þessi aðgangsbúnaður og hugbúnaður sannvotti óviðkomandi aðila sem greiðanda.

2. Þegar greiðandi notar þessa þætti skulu þessar ráðstafanir tryggja að þessi búnaður og hugbúnaður hindri óheimila notkun þáttanna gegnum aðgang að búnaðinum og hugbúnaðinum.

9. gr.

Óhæði þáttanna

1. Greiðsluþjónustuveitendur skulu tryggja að notkun þáttanna í sterkari sannvottun viðskiptavina sem um getur í 6., 7. og 8. gr. sé háð ráðstöfunum sem tryggja að brot á einum þætti hafi ekki áhrif á áreiðanleika hinna þáttanna, með tilliti til tækni, algríms og kennistærða.

2. Greiðsluþjónustuveitendur skulu innleiða öryggisráðstafanir þegar einhver þáttur í sterkri sannvottun viðskiptavina eða sannvottunarkóðinn sjálfur er notaður í gegnum fjölnotabúnað til að milda áhættuna sem gæti stafað af þeim fjölnotabúnaði ef áreiðanleika hans er stefnt í tvísýnu.

3. Að því er varðar 2. mgr. skulu mildunarráðstafanir taka til alls eftirfarandi:

a) notkunar á aðskildu, öruggu framkvæmdarumhverfi í gegnum hugbúnað sem er komið fyrir innan í fjölnotabúnaðinum,

b) kerfa sem tryggja að greiðandi eða þriðji aðili hafi ekki breytt hugbúnaðinum eða búnaðinum,

c) ef breytingar hafa átt sér stað, kerfa til að milda afleiðingar þess.

III. KAFLI

UNDANÞÁGUR FRÁ STERKRI SANNVOTTUN VIÐSKIPTAVINA

10. gr.

Upplýsingar um greiðslureikninga

1. Greiðsluþjónustuveitendur þurfa ekki að nota sterka sannvottun viðskiptavina, með fyrirvara um að farið sé að kröfunum sem mælt er fyrir um í 2. gr. og 2. mgr. þessarar greinar, þegar notandi greiðsluþjónustu hefur takmarkaðan aðgang að öðrum hvorum eða báðum eftirfarandi þáttum á Netinu án þess að gefa upp viðkvæmar greiðsluupplýsingar:

a) stöðunni á einum eða fleiri tilteknum greiðslureikningum,

b) greiðslunum sem framkvæmdar eru á undanförnum 90 dögum í gegnum einn eða fleiri tiltekinn greiðslureikning.

2. Að því er varðar 1. mgr. skulu greiðsluþjónustuveitendur ekki vera undanþegnir því að nota sterka sannvottun viðskiptavina þegar annaðhvort eftirfarandi skilyrða er uppfyllt:

a) notandi greiðsluþjónustu er að nálgast upplýsingarnar sem tilgreindar eru í 1. mgr., í fyrsta sinn á Netinu,

b) meira en 90 dagar eru liðnir frá því notandi greiðsluþjónustunnar nálgaðist síðast upplýsingarnar sem tilgreindar er í b-lið 1. mgr. á Netinu og sterk sannvottun viðskiptavinavar var notuð.

11. gr.

Snertilausar greiðslur á sölustað

Greiðsluþjónustuveitendur þurfa ekki að nota sterka sannvottun viðskiptavina, með fyrirvara um að farið sé að kröfunum sem mælt er fyrir um í 2. gr., þegar greiðandinn virkjar snertilausa rafræna greiðslu, að því tilskildu að eftirfarandi skilyrði séu uppfyllt:

a) að stök fjárhæð snertilausrar rafrænnar greiðslu sé ekki hærri en 50 evrur og

b) að uppsöfnuð fjárhæð fyrri snertilausra rafrænna greiðslna sem virkjaðar voru með greiðslumiðli með snertilausri virkni frá dagsetningu síðustu beitingar sterkrar sannvottunar viðskiptavina er ekki hærri en 150 evrur eða

c) að fjöldi snertilausra rafrænna greiðslna í röð sem virkjaðar voru með greiðslumiðli sem býður upp á snertilausa virkni frá dagsetningu síðustu beitingar sterkrar sannvottunar viðskiptavina er ekki hærri en fimm.

12. gr.

Ómannaðir posar fyrir samgöngufargjöld og bílastæðagjöld

Greiðsluþjónustuveitendur þurfa ekki að nota sterka sannvottun viðskiptavina, með fyrirvara um að farið sé að kröfunum sem mælt er fyrir um í 2. gr., þegar greiðandinn virkjar rafræna greiðslu í ómönnuðum posa í þeim tilgangi að greiða fyrir samgöngufargjald eða bílastæðagjald.

13. gr.

Traustir aðilar

1. Greiðsluþjónustuveitendur skulu nota sterka sannvottun viðskiptavina þegar greiðandi býr til eða breytir skrá yfir trausta aðila gegnum greiðsluþjónustuveitanda sem veitir greiðandanum reikningsþjónustu.

2. Greiðsluþjónustuveitendur þurfa ekki að nota sterka sannvottun viðskiptavina, með fyrirvara um að farið sé að almennum sannvottunarkröfum, þegar greiðandinn virkjar greiðslu og viðtakandi greiðslu er á skrá yfir trausta aðila sem greiðandinn bjó til áður.

14. gr.

Endurteknar greiðslur

1. Greiðsluþjónustuveitendur skulu nota sterka sannvottun viðskiptavina þegar greiðandi býr til, breytir eða virkjar í fyrsta sinn röð endurtekinna greiðslna af sömu fjárhæð og til sama viðtakanda greiðslu.

2. Greiðsluþjónustuveitendur þurfa ekki að nota sterka sannvottun viðskiptavina, með fyrirvara um að farið sé að almennum sannvottunarkröfum, vegna virkjunar allra greiðslna sem eru hluti af röð greiðslna sem um getur í 1. mgr.

15. gr.

Millifærsla fjármuna á milli reikninga í eigu sama einstaklings eða lögaðila

Greiðsluþjónustuveitendur þurfa ekki að nota sterka sannvottun viðskiptavina, með fyrirvara um að farið sé að kröfunum sem mælt er fyrir um í 2. gr., þegar greiðandinn virkjar millifærslu fjármuna við aðstæður þar sem greiðandinn og viðtakandi greiðslu er sami einstaklingur eða lögaðili og báðir greiðslureikningarnir eru í vörslu sama greiðsluþjónustuveitanda sem veitir reikningsþjónustu.

16. gr.

Lágar greiðslur

Greiðsluþjónustuveitendur þurfa ekki að nota sterka sannvottun viðskiptavina, þegar greiðandinn virkjar rafræna fjargreiðslu, að því tilskildu að eftirfarandi skilyrði séu uppfyllt:

a) að fjárhæð rafrænnar fjargreiðslu sé ekki hærri en 30 evrur og

b) að uppsöfnuð fjárhæð fyrri rafrænna fjargreiðslna sem virkjaðar hafa verið af greiðandanum frá því að sterk sannvottun var notuð síðast sé ekki hærri en 100 evrur eða

c) að fjöldi fyrri rafrænna fjargreiðslna sem virkjaðar hafa verið af greiðandanum frá því að sterk sannvottun var notuð síðast fari ekki yfir fimm stakar rafrænar fjargreiðslur í röð.

17. gr.

Öruggt ferli og samskiptareglur fyrir fyrirtækjagreiðslur

Greiðsluþjónustuveitendur þurfa ekki að nota sterka sannvottun viðskiptavina, að því er varðar lögaðila sem virkja rafrænar greiðslur með sérnota ferli eða samskiptareglum sem eru einungis aðgengilegar greiðendum sem eru ekki neytendur, þegar lögbær yfirvöld eru fullviss um að þessi ferli og samskiptareglur tryggi a.m.k. sambærilegt öryggisstig og þau sem kveðið er á um í tilskipun (ESB) 2015/2366.

18. gr.

Áhættugreining færslna

1. Greiðsluþjónustuveitendur þurfa ekki að nota sterka sannvottun viðskiptavina þegar greiðandinn virkjar rafræna fjargreiðslu sem er auðkennd af greiðsluþjónustuveitanda sem greiðsla með lítilli áhættu samkvæmt greiðsluvöktunarkerfinu sem um getur í 2. gr. og í c-lið 2. mgr. þessarar greinar.

2. Rafræn greiðsla sem um getur í 1. mgr. skal talin hafa litla áhættu þegar öll eftirfarandi skilyrði eru uppfyllt:

a) svikahlutfall fyrir þá tegund greiðslu, tilkynnt af greiðsluþjónustuveitandanum og reiknað út í samræmi við 19. gr., er jafnt eða lægra en viðmiðunarhlutfall svika sem tilgreint er í töflunni sem sett er fram í viðaukanum fyrir „rafrænar kortatengdar fjargreiðslur“ og „rafrænar fjarmillifærslur fjármuna“, eftir því sem við á,

b) fjárhæð greiðslunnar fer ekki yfir viðeigandi fjárhæðarmörk undanþágu (*e. exemption threshold value*) sem tilgreint er í töflunni sem sett er fram í viðaukanum,

c) greiðsluþjónustuveitendur hafa ekki auðkennt eftirfarandi, við framkvæmd á áhættugreiningu í rauntíma:

   i. óeðlileg útgjalda- eða hegðunarmynstur greiðanda,

   ii. óvenjulegar upplýsingar um aðgengi greiðanda að aðbúnaði/hugbúnaði,

   iii. árás spilliforrita í einhverjum lotum sannvottunarferlisins,

   iv. þekkta sviðsmynd svika við veitingu greiðsluþjónustu,

   v. óeðlilega staðsetningu greiðandans,

   vi. áhættusama staðsetningu viðtakanda greiðslu.

3. Greiðsluþjónustuveitendur sem ætla að undanskilja rafrænar fjargreiðslur frá sterkri sannvottun viðskiptavina á grundvelli þess að af þeim stafi lítil áhætta skulu, að lágmarki, taka mið af eftirfarandi áhættutengdum þáttum:

a) útgjaldamynstri einstakra notenda greiðsluþjónustu fram til þessa,

b) greiðslusögu hvers notanda greiðsluþjónustu greiðsluþjónustuveitanda,

c) staðsetningu greiðanda og viðtakanda greiðslu þegar greiðsla á sér stað í þeim tilvikum þegar aðgangsbúnaðurinn eða hugbúnaðurinn kemur frá greiðsluþjónustuveitanda,

d) auðkenningu á óeðlilegum greiðslumynstrum notanda greiðsluþjónustu í tengslum við greiðslusögu notandans.

Mat greiðsluþjónustuveitanda skal taka mið af öllum þessum áhættutengdu þáttum til að greina áhættustig fyrir hverja staka greiðslu og ákvarða hvort heimila eigi tiltekna greiðslu án sterkrar sannvottunar viðskiptavina.

19. gr.

Útreikningur á svikahlutföllum

1. Fyrir hvora tegund greiðslu sem um getur í töflunni sem sett er fram í viðaukanum skal greiðsluþjónustuveitandinn tryggja að heildarhlutfall svika sem nær bæði yfir greiðslur sem sannvottaðar eru með sterkri sannvottun og þær sem framkvæmdar eru á grundvelli þeirra undanþága sem um getur í 13.–18. gr. sé jafnt, eða lægra en, viðmiðunarhlutfall svika fyrir sömu tegund greiðslu sem vísað er til í töflunni sem sett er fram í viðaukanum.

Heildarhlutfall svika fyrir hvora tegund greiðslu skal reiknað út sem heildarvirði óheimilla eða sviksamlegra fjargreiðslna, hvort sem fjármunir hafa verið endurheimtir eða ekki, deilt með heildarvirði allra fjargreiðslna fyrir sömu tegund greiðslna, hvort sem þær eru sannvottaðar með notkun sterkrar sannvottunar viðskiptavina eða framkvæmdar á grundvelli þeirra undanþága sem um getur í 13.–18. gr. á hlaupandi ársfjórðungsgrundvelli (90 dagar).

2. Útreikningur svikahlutfalla og niðurstöðutölur skulu metnar í úttektinni sem um getur í 2. mgr. 3. gr., sem skal tryggja að þau séu fullnægjandi og rétt.

3. Aðferðafræðin og öll líkön sem greiðsluþjónustuveitandi notar til að reikna út svikahlutföll, ásamt svikahlutföllunum sjálfum, skal vera skjalfest með viðunandi hætti og gert að fullu aðgengilegt lögbærum yfirvöldum og Evrópsku bankaeftirlitsstofnuninni, með fyrirframtilkynningu til viðkomandi lögbærra yfirvalda, að beiðni þeirra.

20. gr.

Afturköllun undanþága sem byggjast á áhættugreiningu greiðslna

1. Greiðsluþjónustuveitendur sem nota undanþáguna sem um getur í 18. gr. skulu tafarlaust tilkynna lögbærum yfirvöldum fari eitt af svikahlutföllunum sem þeir vakta, fyrir hverja tegund greiðslu sem vísað er til í töflunni í viðaukanum, yfir gildandi viðmiðunarhlutfall svika og skal veita lögbærum yfirvöldum lýsingu á þeim ráðstöfunum sem þeir hyggjast gera til að svikahlutfallið sem þeir vakta samrýmist aftur því gildandi hlutfalli svika sem miðað er við.

2. Greiðsluþjónustuveitendur skulu tafarlaust hætta að nota undanþáguna sem um getur í 18. gr. fyrir hvora tegund greiðslu, sem tilgreind er í töflunni í viðaukanum innan ramma sérstakrar hámarksundanþágu, þegar hlutfall þeirra svika sem eru vöktuð fer tvo ársfjórðunga í röð yfir gildandi hlutfall svika sem miðað er við fyrir þann greiðslumiðil eða tegund greiðslu innan ramma þeirrar hámarksundanþágu.

3. Í kjölfar afturköllunar undanþágunnar sem um getur í 18. gr. í samræmi við 2. mgr. þessarar greinar skulu greiðsluþjónustuveitendur ekki nota þá undanþágu aftur fyrr en útreiknað svikahlutfall er jafnt og, eða lægra en, viðmiðunarhlutfall svika sem við á fyrir þá tegund greiðslu innan ramma þeirrar hámarksundanþágu fyrir einn ársfjórðung.

4. Þegar greiðsluþjónustuveitendur ætla að nota undanþáguna sem um getur í 18. gr. aftur, skulu þeir tilkynna lögbærum yfirvöldum það með nægum fyrirvara og skulu áður en þeir nota undanþáguna aftur, leggja fram sönnun á því að svikahlutfall þeirra sem vaktað er samrýmist aftur því gildandi hlutfalli svika sem miðað er við fyrir téða hámarksundanþágu í samræmi við 3. mgr. þessarar greinar.

21. gr.

Vöktun

1. Til að nýta undanþágurnar sem settar eru fram í 10.–18. gr. skulu greiðsluþjónustuveitendur skrá og vakta eftirfarandi gögn fyrir hverja tegund greiðslu, með sundurliðun fyrir bæði fjargreiðslur og staðgreiðslur, á ársfjórðungsgrundvelli hið minnsta:

a) heildarvirði óheimilla eða sviksamlegra greiðslna í samræmi við 2. mgr. 64. gr. tilskipunar (ESB) 2015/2366, heildarvirði allra greiðslna og svikahlutfalla sem þar af leiða, þ.m.t. sundurliðun á greiðslum sem virkjaðar eru með strangri sannvottun og samkvæmt hverri undanþágu,

b) meðaltal greiðsluvirðis, þ.m.t. sundurliðun á greiðslum sem virkjaðar eru með sterkri sannvottun viðskiptavina og samkvæmt hverri undanþágu,

c) fjöldi greiðslna þar sem hverri undanþágu var beitt og prósenta þeirra að því er varðar heildarfjölda greiðslna.

2. Greiðsluþjónustuveitendur skulu gera niðurstöður vöktunarinnar í samræmi við 1. mgr. aðgengilegar lögbærum yfirvöldum og Evrópsku bankaeftirlitsstofnuninni með fyrirframtilkynningu til viðkomandi lögbærra yfirvalda, að beiðni þeirra.

IV. KAFLI

TRÚNAÐUR OG HEILLEIKI VEGNA PERSÓNUBUNDINNA ÖRYGGISSKILRÍKJA GREIÐSLUÞJÓNUSTUNOTENDA

22. gr.

Almennar kröfur

1. Greiðsluþjónustuveitendur skulu tryggja trúnað og heilleika vegna persónubundinna öryggisskilríkja notanda greiðsluþjónustu, þ.m.t. sannvottunarkóða, á öllum stigum sannvottunar.

2. Að því er varðar 1. mgr. skulu greiðsluþjónustuveitendur tryggja að öll eftirfarandi skilyrði séu uppfyllt:

a) persónubundin öryggisskilríki eru hulin þegar þau birtast og ekki lesanleg í heild sinni þegar notandi greiðsluþjónustunnar notar þau við sannvottun,

b) persónubundin öryggisskilríki á gagnasniði, ásamt dulkóðunarefni sem tengist dulkóðun persónubundinna öryggisskilríkja, eru ekki vistuð sem venjulegur texti,

c) leynilegt dulkóðunarefni er varið óheimilli birtingu.

3. Greiðsluþjónustuveitendur skulu skrásetja allt ferlið í tengslum við stýringu dulkóðunarefnis sem notað er til að dulkóða eða gera persónubundin öryggisskilríki ólesanleg á annan hátt.

4. Greiðsluþjónustuveitendur skulu tryggja að úrvinnsla og sending persónubundinna öryggisskilríkja og sannvottunarkóða sem myndaðir eru í samræmi við II. kafla eigi sér stað í öruggu umhverfi í samræmi við stranga og viðurkennda staðla innan greinarinnar.

23. gr.

Gerð og afhending skilríkjanna

Greiðsluþjónustuveitendur skulu tryggja að gerð persónubundinna öryggisskilríkja fari fram í öruggu umhverfi.

Þeir skulu milda áhættuna af óheimilli notkun persónubundinna öryggisskilríkja og sannvottunarbúnaðar og hugbúnaðar ef þau týnast, þeim stolið eða þau afrituð áður en þau hafa borist greiðandanum.

24. gr.

Tenging við notanda greiðsluþjónustu

1. Greiðsluþjónustuveitendur skulu tryggja að einungis notandi greiðsluþjónustu sé tengdur, á öruggan hátt, við persónubundin öryggisskilríki, sannvottunarbúnað og hugbúnað.

2. Að því er varðar 1. mgr. skulu greiðsluþjónustuveitendur tryggja að öll eftirfarandi skilyrði séu uppfyllt:

a) tenging auðkennis notanda greiðsluþjónustu við persónubundin öryggisskilríki, sannvottunarbúnað og hugbúnað fari fram á ábyrgð greiðsluþjónustuveitandans í öruggu umhverfi sem samanstendur a.m.k. af athafnasvæði greiðsluþjónustuveitandans, netumhverfi sem greiðsluþjónustuveitandinn lætur í té eða öðrum sambærilegum, öruggum vefsetrum sem greiðsluþjónustuveitandinn notar og hraðbankaþjónustu hans þannig að tekið sé mið af áhættunni sem tengist búnaði og undirliggjandi þáttum sem notaðir eru í tengingarferlinu sem eru ekki á ábyrgð greiðsluþjónustuveitanda,

b) tenging í gegnum fjarskipti á auðkenni notanda greiðsluþjónustu við persónubundin öryggisskilríki og við sannvottunarbúnað eða hugbúnað sé framkvæmd með sterkri sannvottun viðskiptavina.

25. gr.

Afhending skilríkja, sannvottunarbúnaðar og hugbúnaðar

1. Greiðsluþjónustuveitendur skulu tryggja að afhending persónubundinna öryggisskilríkja, sannvottunarbúnaðar og hugbúnaðar til notanda greiðsluþjónustu sé framkvæmd á öruggan máta sem geri kleift að bregðast við hættunni sem tengist óheimilli notkun þeirra ef þau týnast, þeim stolið eða þau afrituð.

2. Að því er varðar 1. mgr. skulu greiðsluþjónustuveitendur að lágmarki beita öllum eftirfarandi ráðstöfunum:

a) skilvirkum og öruggum afhendingarkerfum sem tryggja að persónubundin öryggisskilríki, sannvottunarbúnaður og hugbúnaður séu afhent lögmætum notanda greiðsluþjónustu,

b) kerfum sem gera greiðsluþjónustuveitanda kleift að sannreyna áreiðanleika sannvottunarhugbúnaðarins sem afhentur er notanda greiðsluþjónustu gegnum Netið,

c) fyrirkomulagi sem tryggir að þegar afhending persónubundinna öryggisskilríkja fer fram utan athafnasvæðis greiðsluþjónustuveitanda eða í gegnum fjarskipti:

   i. að enginn óviðkomandi aðili geti fengið fleiri en einn þátt af persónubundnum öryggisskilríkjum, sannvottunarbúnaði eða hugbúnaði þegar þau eru afhent í gegnum sömu rás,

   ii. að virkja þurfi persónubundin öryggisskilríki, sannvottunarbúnað eða hugbúnað áður en hann er notaður.

d) fyrirkomulagi sem tryggir að virkjunin eigi sér stað í öruggu umhverfi í samræmi við verklagið fyrir tengingu sem um getur í 24. gr., í tilvikum þar sem virkja þarf persónubundin öryggisskilríki, sannvottunarbúnað eða hugbúnað fyrir fyrstu notkun.

26. gr.

Endurnýjun persónubundinna öryggisskilríkja

Greiðsluþjónustuveitendur skulu tryggja að endurnýjun eða endurvirkjun persónubundinna öryggisskilríkja fylgi verklagi við myndun, tengingu og afhendingu skilríkjanna og sannvottunarbúnaðarins í samræmi við 23., 24. og 25. gr.

27. gr.

Eyðing, afvirkjun og afturköllun

Greiðsluþjónustuveitendur skulu tryggja að þeir hafi til staðar skilvirk verkferli til að beita eftirfarandi öryggisráðstöfunum:

a) öruggri eyðingu, afvirkjun eða afturköllun persónubundinna öryggisskilríkja, sannvottunarbúnaðar og hugbúnaðar,

b) þegar greiðsluþjónustuveitandinn dreifir endurnotanlegum sannvottunarbúnaði og hugbúnaði skal koma á öruggri endurnotkun búnaðar eða hugbúnaðar, skrá og framkvæma áður en aðrir notendur greiðsluþjónustu fá aðgang að honum,

c) afvirkjun eða afturköllun upplýsinga sem tengjast persónubundnum öryggisskilríkjum sem vistuð eru í kerfum og gagnagrunnum greiðsluþjónustuveitenda og, þar sem við á, í opinberum gagnasöfnum.

V. KAFLI

ALMENNIR OG ÖRUGGIR OPNIR SAMSKIPTASTAÐLAR

1. liður

Almennar kröfur varðandi samskipti

28. gr.

Kröfur sem varða auðkenningu

1. Greiðsluþjónustuveitendur skulu tryggja örugga auðkenningu þegar upplýsingum er miðlað úr búnaði greiðanda til viðtökubúnaðar viðtakanda rafrænnar greiðslu, sem er einkum en ekki endilega takmarkað við posa.

2. Greiðsluþjónustuveitendur skulu tryggja að áhættan af því að miðlun upplýsinga, sem beint er inn á ranga braut til óviðkomandi aðila með smáforritum fyrir snjalltæki og öðrum skilflötum greiðsluþjónustuveitenda sem bjóða upp á rafræna greiðsluþjónustu, sé milduð.

29. gr.

Rekjanleiki

1. Greiðsluþjónustuveitendur skulu hafa til staðar verkferli sem tryggja að allar greiðslur og önnur samskipti við notendur greiðsluþjónustu, aðra greiðsluþjónustuveitendur og aðra aðila, þ.m.t. söluaðila, í tengslum við veitingu greiðsluþjónustu, séu rekjanleg, þannig að tryggt sé að vitneskja sé til eftir á um alla atburði sem varða rafrænu greiðsluna á öllum mismunandi stigum hennar.

2. Að því er varðar 1. mgr. skulu greiðsluþjónustuveitendur tryggja að allar samskiptalotur við notanda greiðsluþjónustu, aðra greiðsluþjónustuveitendur og aðra aðila, þ.m.t. söluaðila, styðjist við alla eftirfarandi þætti:

a) sérstakt auðkenni lotunnar,

b) öryggiskerfi fyrir ítarlega aðgerðaskráningu, þ.m.t. færslunúmer, tímastimplar og öll viðeigandi færslugögn,

c) tímastimpla sem skulu byggðir á sameiginlegu tímaviðmiðunarkerfi og sem eru samstilltir samkvæmt opinberu tímamerki.

2. hluti

Sértækar kröfur í tengslum við almenna og örugga opna samskiptastaðla

30. gr.

Almennar kröfur varðandi aðgangsskilfleti

1. Greiðsluþjónustuveitendur sem veita reikningsþjónustu sem bjóða greiðanda greiðslureikning sem er aðgengilegur á Netinu skulu hafa a.m.k. einn skilflöt til staðar sem uppfyllir allar eftirfarandi kröfur:

a) reikningsupplýsingaþjónustuveitendum, greiðsluvirkjendum og greiðsluþjónustuveitendum sem gefa út kortatengda greiðslumiðla sé gert kleift að auðkenna sig hjá greiðsluþjónustuveitanda sem veitir reikningsþjónustu,

b) reikningsupplýsingaþjónustuveitendur geti haft samskipti á öruggan hátt til að óska eftir og taka við upplýsingum um einn eða fleiri tiltekna greiðslureikninga og tengdar greiðslur,

c) greiðsluvirkjendur geti haft örugg samskipti til að virkja greiðslufyrirmæli frá greiðslureikningi greiðanda og tekið við öllum upplýsingum um virkjun greiðslunnar og öllum upplýsingum sem aðgengilegar eru greiðsluþjónustuveitendunum sem veita reikningsþjónustu að því er varðar framkvæmd greiðslunnar.

2. Að því er varðar sannvottun notanda greiðsluþjónustu skal skilflöturinn sem um getur í 1. mgr. gera reikningsupplýsingaþjónustuveitendum og greiðsluvirkjendum kleift að treysta á sannvottunarferlið sem greiðsluþjónustuveitendur sem veita reikningsþjónustu veita notanda greiðsluþjónustunnar.

Skilflöturinn skal uppfylla eftirfarandi kröfur hið minnsta:

a) greiðsluvirkjandi eða reikningsupplýsingaþjónustuveitandi skal geta gefið greiðsluþjónustuveitanda sem veitir reikningsþjónustu fyrirmæli um að hefja sannvottun byggða á samþykki notanda greiðsluþjónustu,

b) samskiptalotum milli greiðsluþjónustuveitanda sem veitir reikningsþjónustu, reikningsupplýsingaþjónustuveitanda, greiðsluvirkjanda og viðkomandi notanda greiðsluþjónustu skal komið á og viðhaldið í gegnum sannvottunina,

c) heilleiki og trúnaður persónubundinna öryggisskilríkja og sannvottunarkóða sem sendir eru með eða í gegnum greiðsluvirkjanda eða reikningsupplýsingaþjónustuveitanda skal tryggður.

3. Greiðsluþjónustuveitendur sem veita reikningsþjónustu skulu tryggja að skilfletir þeirra fullnægi samskiptastöðlum sem alþjóðlegar eða evrópskar staðlastofnanir gefa út.

Greiðsluþjónustuveitendur sem veita reikningsþjónustu skulu einnig tryggja að tækniforskriftir allra skilflata séu skráðar og tilgreina röð starfsvenja, samskiptareglna og verkfæra sem nauðsynleg eru fyrir greiðsluvirkjendur, reikningsupplýsingaþjónustuveitendur og greiðsluþjónustuveitendur sem gefa út kortatengda greiðslumiðla til þess að hugbúnaður þeirra og búnaður sé rekstrarsamhæfður kerfum greiðsluþjónustuveitenda sem veita reikningsþjónustu.

Greiðsluþjónustuveitendur sem veita reikningsþjónustu skulu að lágmarki, og eigi síðar en 6 mánuðum fyrir gildistökudaginn sem um getur í 2. mgr. 38. gr., eða fyrir þann dag þegar aðgangsskilflöturinn er settur á markað, þegar hann á sér stað eftir dagsetninguna sem um getur í 2. mgr. 38. gr., gera upplýsingarnar aðgengilegar, að kostnaðarlausu, að beiðni greiðsluvirkjenda með starfsleyfi, reikningsupplýsingaþjónustuveitenda og greiðsluþjónustuveitenda sem gefa út kortatengda greiðslumiðla, eða greiðsluþjónustuveitenda sem sótt hafa um viðeigandi leyfi til lögbærra yfirvalda sinna, og gera samantekt upplýsinganna aðgengilega á vefsetri sínu.

4. Til viðbótar við 3 mgr. skulu greiðsluþjónustuveitendur sem veita reikningsþjónustu tryggja, nema ef neyðarástand skapast, að allar breytingar á tækniforskriftum skilflatar þeirra séu gerðar aðgengilegar greiðsluvirkjendum með starfsleyfi, reikningsupplýsingaþjónustuveitendum og greiðsluþjónustuveitendum sem gefa út kortatengda greiðslumiðla, eða greiðsluþjónustuveitendur sem hafa sótt um viðeigandi leyfi frá lögbærum yfirvöldum sínum, fyrirfram eins fljótt og auðið er og eigi síðar en 3 mánuðum áður en breytingin er framkvæmd.

Greiðsluþjónustuveitendur skulu skjalfesta neyðartilvik þegar breytingum var hrundið í framkvæmd og gera þær upplýsingar aðgengilegar lögbærum yfirvöldum að beiðni þeirra.

5. Greiðsluþjónustuveitendur sem veita reikningsþjónustu skulu gera prófunarstöð. þ.m.t. aðstoð, aðgengilega fyrir prófanir á tengingu og starfrænar prófanir til að gera greiðsluvirkjendum með starfsleyfi, greiðsluþjónustuveitendum sem gefa út kortatengda greiðslumiðla og reikningsupplýsingaþjónustuveitendum, eða greiðsluþjónustuveitendum sem hafa sótt um viðeigandi leyfi, kleift að prófa hugbúnað sinn og forrit sem notuð eru til að bjóða notendum greiðsluþjónustu. Prófunarstöðin skal gerð aðgengileg eigi síðar en 6 mánuðum fyrir gildistökudaginn sem um getur í 2. mgr. 38. gr. eða fyrir dagsetningu þegar aðgangsskilflötur er settur á markað, ef markaðssetningin á sér stað eftir dagsetninguna sem um getur í 2. mgr. 38. gr.

Þó skal ekki deila neinum viðkvæmum upplýsingum í gegnum prófunarstöðina.

6. Lögbær yfirvöld skulu tryggja að greiðsluþjónustuveitendur sem veita reikningsþjónustu fari ávallt að skuldbindingunum sem felast í þessum stöðlum í tengslum við skilflötinn eða skilfletina sem þau taka í notkun. Ef greiðsluþjónustuveitendur sem veita reikningsþjónustu fullnægja ekki kröfunum um skilfleti sem mælt er fyrir um í þessum stöðlum skulu lögbær yfirvöld tryggja að ekki sé komið í veg fyrir veitingu greiðsluvirkjunar og reikningsupplýsingaþjónustu né hún trufluð þannig að viðkomandi veitendur slíkrar þjónustu fullnægi skilyrðunum sem skilgreind eru skv. 5. mgr. 33. gr.

31. gr.

Valkostir með tilliti til aðgangsskilflata

Greiðsluþjónustuveitendur sem veita reikningsþjónustu skulu setja upp skilflötinn eða skilfletina sem um getur í 30. gr. með sérhæfðum skilflötum eða með því að heimila greiðsluþjónustuveitendunum sem um getur í 1. mgr. 30. gr. að nota skilfleti sem notaðir eru til sannvottunar og samskipta greiðsluþjónustuveitenda sem veita notendum greiðsluþjónustu reikningsþjónustu.

32. gr.

Skuldbindingar vegna sérhæfðra skilflata

1. Með fyrirvara um að farið sé að 30. og 31. gr. skulu greiðsluþjónustuveitendur sem veita reikningsþjónustu og hafa tekið í notkun sérhæfðan skilflöt tryggja að skilflöturinn veiti að staðaldri sama aðgang og hafi jafn mikla afkastagetu, þ.m.t. stuðningsþjónustu, og skilflöturinn sem notandi greiðsluþjónustunnar hefur fengið fyrir beinan aðgang að greiðslureikningi sínum á Netinu.

2. Greiðsluþjónustuveitendur sem veita reikningsþjónustu og hafa tekið í notkun sérhæfðan skilflöt skulu skilgreina gagnsæja lykilárangursvísa og markmið þjónustunnar sem eru a.m.k. jafnstrangir og þeir sem settir eru fyrir skilflötinn sem notendur greiðsluþjónustu þeirra nota, bæði hvað varðar aðgengileika og gögn sem látin eru í té eru í samræmi við 36. gr. Lögbær yfirvöld skulu vakta þessa skilfleti, vísa og markmið og þau álagsprófuð.

3. Greiðsluþjónustuveitendur sem veita reikningsþjónustu og hafa tekið í notkun sérhæfðan skilflöt skulu tryggja að þessi skilflötur hamli ekki greiðsluvirkjun og veitingu reikningsupplýsingaþjónustu. Slíkar hömlur geta m.a. komið í veg fyrir að greiðsluþjónustuveitendur sem um getur í 1. mgr. 30. gr., noti öryggisskilríki sem greiðsluþjónustuveitandi sem veitir reikningsþjónustu gefur út til viðskiptavina sinna, þvingað sendingu til sannvottunar greiðsluþjónustuveitanda sem veitir reikningsþjónustu eða annarra þátta hans inn á aðra braut, að krafist sé sannvottunar og skráningar til viðbótar við það sem um getur í 11., 14. og 15. gr. tilskipunar (ESB) 2015/2366, eða að krafist sé viðbótarskoðunar á samþykki sem notendur greiðsluþjónustu hafa veitt greiðsluvirkjendum og veitendum reikningsupplýsingaþjónustu.

4. Að því er varðar 1. og 2. mgr. skulu greiðsluþjónustuveitendur sem veita reikningsþjónustu vakta aðgengileika og afköst sérhæfða skilflatarins. Greiðsluþjónustuveitendur sem veita reikningsþjónustu skulu birta ársfjórðungslega tölfræðilegar upplýsingar á vefsetri sínu um aðgengileika og afköst sérhæfða skilflatarins og viðmótsins sem notendur greiðsluþjónustu þess nota.

33. gr.

Viðbragðsaðgerðir vegna sérhæfðs skilflatar

1. Greiðsluþjónustuveitendur sem veita reikningsþjónustu skulu, við hönnun á sérhæfðum skilfleti, koma á skipulagi og áætlun vegna viðbragðsaðgerða ef skilflöturinn virkar ekki í samræmi við 32. gr., ef hann er óvænt ekki tiltækur eða ef kerfið bilar. Ef fimm beiðnum um aðgang í röð að upplýsingum um greiðsluvirkjun eða veitingu reikningsupplýsingaþjónustu er ekki svarað innan 30 sekúnda má gera ráð fyrr að um óvæntan ótiltækileika eða bilun á kerfum sé að ræða.

2. Viðbragðsaðgerðir skulu taka til samskiptaáætlana til að upplýsa greiðsluþjónustuveitendur sem nota sérhæfðan skilflöt um aðgerðir til að endurvirkja kerfið og jafnframt lýsingar á öðrum valkostum sem greiðsluþjónustuveitendum bjóðast meðan á þessu stendur.

3. Greiðsluþjónustuveitandi sem veitir reikningsþjónustu og greiðsluþjónustuveitandi sem um getur í 1. mgr. 30 gr. skulu báðir tilkynna vandamál sem tengjast sérhæfðu skilflötunum sem lýst er í 1. mgr. til lögbærra landsyfirvalda sinna án tafar.

4. Innan ramma viðbragðsaðgerðar skal greiðsluþjónustuveitendum sem um getur í 1. mgr. 30. gr. vera heimilt að nota skilfleti sem gerðir eru tiltækir notendum greiðsluþjónustu vegna sannvottunar og samskipta við greiðsluþjónustuveitanda sem veitir þeim reikningsþjónustu þar til sérhæfði skilflöturinn er aftur tiltækur og nær þeim afköstum sem um getur í 32. gr.

5. Í þessu skyni skulu greiðsluþjónustuveitendur sem veita reikningsþjónustu tryggja að hægt sé að auðkenna greiðsluþjónustuveitendur sem um getur í 1. mgr. 30. gr. og að þeir geti treyst á sannvottunarferlið sem greiðsluþjónustuveitendur sem veita reikningsþjónustu veita notanda greiðsluþjónustu. Þegar greiðsluþjónustuveitendur sem um getur í 1. mgr. 30. gr. nota skilflötinn sem um getur í 4. mgr. skulu þeir:

a) grípa til nauðsynlegra aðgerða til að tryggja að þeir hafi ekki aðgang að, geymi né vinni úr gögnum í öðrum tilgangi en að veita þjónustu sem notandi greiðsluþjónustunnar óskaði eftir,

b) halda áfram að fara að skuldbindingunum sem leiðir af 3. mgr. 66 gr. annars vegar og hins vegar 2. mgr. 67. gr. tilskipunar (ESB) 2015/2366,

c) skrá gögnin sem aðgangur er veittur að gegnum skilflötinn, sem starfræktur er af greiðsluþjónustuveitandanum sem veitir reikningsþjónustu, í aðgerðaskrá og láta landsyfirvöldum sínum í té aðgerðaskrá, þegar um er beðið og án ótilhlýðilegra tafa,

d) útskýra á viðeigandi hátt fyrir lögbærum landsyfirvöldum, að beiðni þeirra og án ótilhlýðilegra tafa, notkunina á skilfletinum sem notendunum greiðsluþjónustunnar er gerður tiltækur svo þeir hafi beinan aðgang að greiðslureikningi sínum á Netinu,

e) upplýsa greiðsluþjónustuveitandann sem veitir reikningsþjónustu til samræmis við það.

6. Lögbær yfirvöld skulu, að höfðu samráði við Evrópsku bankaeftirlitsstofnuna til að tryggja samræmda beitingu eftirfarandi skilyrða, veita greiðsluþjónustuveitendum sem veita reikningsþjónustu sem hafa valið sérhæfðan skilflöt, undanþágu frá skuldbindingunni um að grípa til viðbragðsaðgerðanna sem lýst er í 4. mgr., þegar sérhæfði skilflöturinn uppfyllir öll eftirfarandi skilyrði:

a) hann uppfyllir öll skilyrði fyrir sérhæfða skilfleti sem um getur í 32. gr.,

b) hann er hannaður og prófaður í samræmi við 5. mgr. 30. gr. og greiðsluþjónustuveitendurnir sem þar um getur gera sig ánægða með það,

c) greiðsluþjónustuveitendur hafi almennt notað hann að lágmarki í 3 mánuði til að bjóða upp á reikningsupplýsingaþjónustu, greiðsluvirkjun og til að veita staðfestingu á aðgengileika fjármuna fyrir kortatengdar greiðslur,

d) öll vandkvæði tengd sérhæfða skilfletinum hafa verið leyst án ástæðulausrar tafar.

7. Lögbær yfirvöld skulu afturkalla undanþáguna sem um getur í 6. mgr. ef greiðsluþjónustuveitendur sem veita reikningsþjónustu uppfylla ekki skilyrðin í a- og d-lið, lengur en 2 samfelldar almanaksvikur. Lögbær yfirvöld skulu upplýsa evrópsku bankaeftirlitsstofnunina um þessa afturköllun og tryggja að greiðsluþjónustuveitendur sem veita reikningsþjónustu komi á, eins fljótt og unnt er og eigi síðar en innan 2 mánaða, viðbragðsaðgerðunum sem um getur í 4. mgr.

34. gr.

Vottorð

1. Að því er varðar auðkenningu, eins og um getur í a-lið 1. mgr. 30. gr., skulu greiðsluþjónustuveitendur treysta á fullgilda vottun fyrir rafræn innsigli sbr. 3. mgr. 30. gr. reglugerðar (ESB) 910/2014 eða fyrir sannvottun vefseturs eins og um getur í 39. mgr. 3. gr. þeirrar reglugerðar

2. Að því er varðar þessa reglugerð skal skráningarnúmerið eins og um getur í opinberum skrám í samræmi við c-lið III. viðauka eða c-lið IV. viðauka við reglugerð (ESB) nr. 910/2014 vera leyfisnúmer greiðsluþjónustuveitanda sem gefur út kortatengda greiðslumiðla, reikningsupplýsingaþjónustuveitanda og greiðsluvirkjenda, þ.m.t. greiðsluþjónustuveitenda sem veita reikningsþjónustu sem veita slíka þjónustu, aðgengilegt í opinberri skrá heimaaðildarríkis skv. 14. gr. tilskipunar (ESB) 2015/2366 eða vegna tilkynninga fyrir hverja sannvottun sem heimiluð er skv. 8. gr. tilskipunar Evrópuþingsins og ráðsins 2013/36/ESB ([1]), í samræmi við 20. gr. þeirrar tilskipunar.

3. Að því er varðar þessa reglugerð skulu fullgild vottorð fyrir rafræn innsigli eða fyrir sannvottun vefsetra sem um getur í 1. mgr., fela í sér, á tungumáli sem venja er að nota innan alþjóðafjármálageirans, sérstakar viðbótareigindir með tilliti til alls eftirfarandi:

a) hlutverks greiðsluþjónustuveitanda, sem getur verið eitt eða fleiri eftirfarandi:

   i. veiting reikningsþjónustu

   ii. greiðsluvirkjun,

   iii. reikningsupplýsingar,

   iv. útgáfa kortatengdra greiðslumiðla,

b) heitis lögbærra yfirvalda þar sem greiðsluþjónustuveitandi er skráður.

4. Eiginleikarnir sem um getur í 3. mgr. skulu ekki hafa áhrif á samvirkni og viðurkenningu á viðurkenndum vottorðum fyrir rafræn innsigli eða sannvottun vefsetra.

([1]) Tilskipun Evrópuþingsins og ráðsins 2013/36/ESB frá 26. júní 2013 um aðgang að starfsemi lánastofnana og varfærniseftirlit með lánastofnunum og verðbréfafyrirtækjum, um breytingu á tilskipun 2002/87/EB og um niðurfellingu á tilskipunum 2006/48/EB og 2006/49/EB (Stjtíð. ESB L 176, 27.6.2013, bls. 338).

35. gr.

Öruggar samskiptalotur

1. Greiðsluþjónustuveitendur sem veita reikningsþjónustu, greiðsluþjónustuveitendur sem gefa út kortatengda greiðslumiðla, reikningsupplýsingaþjónustuveitendur og greiðsluvirkjendur skulu tryggja að í gagnaskiptum um Netið noti aðilar örugga dulkóðun í samskiptum sínum á meðan viðkomandi samskiptalota varir til að vernda trúnað og gagnavernd, með því að nota skilvirka og almennt viðurkennda dulkóðunartækni.

2. Greiðsluþjónustuveitendur sem gefa út kortatengda greiðslumiðla, reikningsupplýsingaþjónustuveitendur og greiðsluvirkjendur skulu halda aðgengislotunum sem greiðsluþjónustuveitendur sem veita reikningsþjónustu bjóða eins stuttum og mögulegt er og enda slíkar lotur með virkum hætti um leið og umbeðinni aðgerð er lokið.

3. Reikningsupplýsingaþjónustuveitendur og greiðsluvirkjendur skulu sjá til þess þegar samhliða netlotum við greiðsluþjónustuveitanda sem veitir reikningsþjónustu er viðhaldið, að þessar lotur séu tengdar á öruggan hátt við viðkomandi lotur sem komið er á við notanda eða notendur greiðsluþjónustu til að hindra að skilaboðum eða upplýsingum sem fara á milli þeirra séu mögulega beint annað.

4. Reikningsupplýsingaþjónustuveitendur, greiðsluvirkjendur og greiðsluþjónustuveitendur sem gefa út kortatengda greiðslumiðla með greiðsluþjónustuveitanda sem veitir reikningsþjónustu skulu hafa skýrar tilvísanir í alla eftirfarandi þætti:

a) notanda eða notendur greiðsluþjónustu og samsvarandi samskiptalotu til að greina á milli fjölda beiðna frá sama notanda eða notendum greiðsluþjónustu,

b) fyrir greiðsluvirkjun, sérstaklega auðkenndar greiðslur sem virkjaðar eru,

c) fyrir staðfestingu á aðgengileika fjármuna, sérstaklega auðkenndar beiðnir í tengslum við fjárhæðina sem nauðsynleg er til að framkvæma kortatengda greiðslu.

5. Greiðsluþjónustuveitendur sem veita reikningsþjónustu, reikningsupplýsingaþjónustuveitendur, greiðsluvirkjendur og greiðsluþjónustuveitendur sem gefa út kortatengda greiðslumiðla skulu tryggja að þegar þeir senda persónubundin öryggisskilríki og sannvottunarkóða geti starfsfólk ekki lesið þau, beint eða óbeint.

Ef persónubundin öryggisskilríki tapa leynd sinni meðan þau eru á ábyrgð þessara veitenda skulu þeir upplýsa notanda greiðsluþjónustunnar sem tengist þeim og útgefanda persónubundnu öryggisskilríkjanna um það, án ástæðulausrar tafar

36. gr.

Gagnaskipti

1. Greiðsluþjónustuveitendur sem veita reikningsþjónustu skulu uppfylla allar eftirfarandi kröfur:

a) þeir skulu veita reikningsupplýsingaþjónustuveitendum sömu upplýsingar úr tilteknum greiðslureikningum og tengdum greiðslum sem gerðar eru tiltækar notanda greiðsluþjónustu þegar hann biður beint um aðgang að reikningsupplýsingum, að því tilskildu að þessar upplýsingar feli ekki í sér viðkvæm greiðslugögn,

b) þeir skulu, strax við viðtöku greiðslufyrirmæla, veita greiðsluvirkjendum sömu upplýsingar um virkjun og framkvæmd greiðslu og sem veittar eru eða gerðar aðgengilegar notanda greiðsluþjónustu þegar sá síðarnefndi virkjar greiðsluna beint,

c) þeir skulu, sé þess óskað, veita greiðsluþjónustuveitendum umsvifalaust staðfestingu á einföldu „já“ eða „nei“ sniði, hvort fjárhæðin sem nauðsynleg er til að framkvæma greiðslu sé tiltæk á greiðslureikningi greiðandans.

2. Ef óvæntur atburður eða villa verður á meðan auðkenning, sannvottun eða skipti á gagnastökum á sér stað, skal greiðsluþjónustuveitandi sem veitir reikningsþjónustu senda tilkynningu til greiðsluvirkjanda eða reikningsupplýsingaþjónustuveitanda og greiðsluþjónustuveitanda sem gefur út kortatengda greiðslumiðla, sem útskýrir ástæðurnar fyrir óvænta atburðinum eða villunni.

Þegar greiðsluþjónustuveitandinn sem veitir reikningsþjónustu býður upp á sérhæfðan skilflöt í samræmi við 32. gr. skal skilflöturinn tryggja að tilkynningarskilaboð sem varða óvænta atburði eða villur séu send til annarra greiðsluþjónustuveitenda sem taka þátt í samskiptalotunni frá öllum greiðsluþjónustuveitendum sem verða varir við atburðinn eða villuna.

3. Reikningsupplýsingaþjónustuveitendur skulu hafa til staðar viðeigandi og skilvirk kerfi sem koma í veg fyrir aðgengi að upplýsingum öðrum en frá tilteknum greiðslureikningum og tengdum greiðslum, í samræmi við skýlaust samþykki notandans.

4. Greiðsluvirkjendur skulu veita greiðsluþjónustuveitendum sem veita reikningsþjónustu sömu upplýsingar og notandi greiðsluþjónustu óskar eftir þegar hann virkjar greiðsluna beint.

5. Reikningsupplýsingaþjónustuveitendur skulu geta nálgast upplýsingar frá tilteknum greiðslureikningum og tengdum greiðslum í vörslu greiðsluþjónustuveitenda sem veita reikningsþjónustu í þeim tilgangi að framkvæma reiknings-upplýsingaþjónustu við aðrar hvorar eftirfarandi aðstæður:

a) þegar notandi greiðsluþjónustu óskar eftir slíkum upplýsingum með virkum hætti,

b) þegar notandi greiðsluþjónustu óskar ekki eftir slíkum upplýsingum með virkum hætti, að hámarki fjórum sinnum á sólarhring, nema ef reikningsupplýsingaþjónustuveitandi og greiðsluþjónustuveitandi sem veitir reikningsþjónustu koma sér saman um fleiri skipti, með samþykki notanda greiðsluþjónustu.

VI. KAFLI

LOKAÁKVÆÐI

37. gr.

Endurskoðun

Með fyrirvara um 5. mgr. 98. gr. í tilskipun (ESB) 2015/2366 skal Evrópska bankaeftirlitsstofnunin fyrir 14. mars 2021 endurskoða svikahlutföllin sem um getur í viðaukanum við þessa reglugerð ásamt undanþágunum sem veittar eru skv. 6. mgr. 33. gr. í tengslum við sérhæfða skilfleti og ef við á, leggja fram drög að uppfærslu til framkvæmdastjórnarinnar í samræmi við 10. gr. reglugerðar (ESB) nr. 1093/2010.

38. gr.

Gildistaka

1. Reglugerð þessi öðlast gildi daginn eftir að hún birtist í *Stjórnartíðindum Evrópusambandsins*.

2. Reglugerð þessi kemur til framkvæmda frá og með 14. september 2019.

3. Þó skulu 3. og 5. mgr. 30. gr. gilda frá 14. mars 2019.

Reglugerð þessi er bindandi í heild sinni og gildir í öllum aðildarríkjunum án frekari lögfestingar.

Gjört í Brussel 27. nóvember 2017.

Fyrir hönd framkvæmdastjórnarinnar,

Jean-Claude JUNCKER

forseti.

VIÐAUKI

	Viðmiðunarhlutfall svika (%) fyrir:	
Fjárhæðarmörk undanþágu	Rafrænar kortatengdar fjargreiðslur	Rafrænar fjarmillifærslur fjármuna
500 evrur	0,01	0,005
250 evrur	0,06	0,01
100 evrur	0,13	0,015