DELEGIRANA UREDBA KOMISIJE (EU) 2018/389

od 27. studenoga 2017.

o dopuni Direktive (EU) 2015/2366 Europskog parlamenta i Vijeća u pogledu regulatornih tehničkih standarda za pouzdanu autentifikaciju klijenta i zajedničke i sigurne otvorene standarde komunikacije

(Tekst značajan za EGP)

EUROPSKA KOMISIJA,

uzimajući u obzir Ugovor o funkcioniranju Europske unije,

uzimajući u obzir Direktivu (EU) 2015/2366 Europskog parlamenta i Vijeća od 25. studenoga 2015. o platnim uslugama na unutarnjem tržištu, o izmjeni direktiva 2002/65/EZ, 2009/110/EZ i 2013/36/EU te Uredbe (EU) br. 1093/2010 i o stavljanju izvan snage Direktive 2007/64/EZ [1], a posebno njezin članak 98. stavak 4. drugi podstavak,

budući da:

(1) Platne usluge koje se nude elektroničkim putem trebale bi se izvoditi na siguran način uz usvajanje tehnologija kojima se može jamčiti sigurna autentifikacija korisnika i u najvećoj mogućoj mjeri smanjiti rizik od prijevare. Postupak autentifikacije općenito bi trebao uključivati mehanizme za praćenje transakcija kako bi se otkrili pokušaji upotrebe personaliziranih sigurnosnih podataka korisnika platnih usluga koji su izgubljeni, ukradeni ili zloupotrijebljeni te bi trebao osiguravati da je korisnik platnih usluga zakoniti korisnik i da stoga daje suglasnost za prijenos novčanih sredstava i pristup svojim informacijama o računu kroz uobičajenu upotrebu personaliziranih sigurnosnih podataka. Nadalje, nužno je utvrditi zahtjeve pouzdane autentifikacije klijenta koje bi trebalo primijeniti svaki put kad platitelj pristupi svojem računu za plaćanje putem interneta, inicira elektroničku platnu transakciju ili izvrši bilo koju radnju s udaljenosti u vezi s kojom može postojati rizik od prijevare povezane s plaćanjem ili drugih oblika zlouporabe na način da se zahtijeva generiranje kôda za autentifikaciju koji bi trebao biti otporan na rizik od krivotvorenja cijelog kôda ili otkrivanja bilo kojeg elementa na temelju kojeg je kôd generiran.

(2) Budući da se metode prijevare stalno mijenjaju, zahtjevi u pogledu pouzdane autentifikacije klijenta trebali bi omogućiti razvoj inovacija u području tehničkih rješenja kao odgovora na pojavu novih prijetnji sigurnosti elektroničkih plaćanja. Kako bi se zahtjevi koji će se utvrditi provodili učinkovito i kontinuirano, primjereno je i zahtijevati da sigurnosne mjere za primjenu pouzdane autentifikacije klijenta i izuzeća od nje, mjere zaštite povjerljivosti i cjelovitosti personaliziranih sigurnosnih podataka i mjere kojima se uspostavljaju zajednički i sigurni otvoreni standardi komunikacije dokumentiraju, periodično testiraju, ocjenjuju i revidiraju neovisni revizori s iskustvom u području IT sigurnosti i platnog prometa. Kako bi nadležna tijela mogla pratiti kvalitetu revizija tih mjera, te bi im revizije trebale biti dostupne na zahtjev.

(3) Budući da elektroničke platne transakcije s udaljenosti podliježu većem riziku od prijevare, za te je transakcije nužno uvesti dodatne zahtjeve za pouzdanu autentifikaciju klijenta kojima se osigurava da elementi dinamično povezuju transakciju s iznosom i primateljem plaćanja koje je odredio platitelj pri iniciranju transakcije.

(4) Dinamično povezivanje moguće je na temelju generiranja kôdova za autentifikaciju koje podliježe strogim sigurnosnim zahtjevima. Kako bi se zadržala tehnološka neutralnost, ne bi trebalo zahtijevati posebnu tehnologiju za primjenu kôdova za autentifikaciju. Stoga bi se kôdovi za autentifikaciju trebali temeljiti na rješenjima kao što je generiranje i potvrđivanje jednokratnih lozinki, digitalnih potpisa ili drugih kriptografski utemeljenih potvrda valjanosti korištenjem ključeva ili kriptografskog materijala pohranjenih u elementima za autentifikaciju, pod uvjetom da su ispunjeni sigurnosni zahtjevi.

[1] SL L 337, 23.12.2015., str. 35.

(5) Nužno je utvrditi posebne zahtjeve za slučaj u kojemu konačni iznos nije poznat u trenutku kada platitelj inicira elektroničku platnu transakciju s udaljenosti kako bi se osiguralo da pouzdana autentifikacija klijenta odgovara maksimalnom iznosu za koji je platitelj dao suglasnost kako je navedeno u Direktivi (EU) 2015/2366.

(6) Kako bi se osigurala primjena pouzdane autentifikacije klijenta, nužno je i zahtijevati odgovarajuće sigurnosne značajke primjenjive na elemente pouzdane autentifikacije klijenta koji pripadaju kategoriji znanja (nešto što samo korisnik zna), kao što su duljina ili složenost, na elemente koji pripadaju kategoriji posjedovanja (nešto što samo korisnik posjeduje), kao što su specifikacije algoritma, duljina ključa i informacijska entropija, te na uređaje i softver koji čitaju elemente koji pripadaju kategoriji svojstvenosti (nešto što korisnik jest), kao što su specifikacije algoritma, biometrijski senzor i elementi za zaštitu predloška, osobito kako bi se smanjio rizik da neovlaštene osobe otkriju, doznaju ili upotrebljavaju te elemente. Potrebno je i utvrditi zahtjeve kojima se osigurava neovisnost tih elemenata kako kršenje jednog od njih ne bi umanjilo pouzdanost drugih, osobito kada se koji od elemenata upotrebljava s pomoću višenamjenskog uređaja, točnije uređaja kao što su tablet ili mobilni telefon koji se mogu upotrebljavati i za davanje upute za izvršenje plaćanja i u postupku autentifikacije.

(7) Zahtjevi za pouzdanu autentifikaciju klijenta primjenjuju se na plaćanja koja inicira platitelj neovisno o tome radi li se o fizičkoj ili pravnoj osobi.

(8) Plaćanja izvršena uporabom anonimnih platnih instrumenata zbog svoje prirode ne podliježu obvezi pouzdane autentifikacije klijenta. Kada se anonimnost tih instrumenata ukine na ugovornoj ili zakonodavnoj osnovi, plaćanja podliježu sigurnosnim zahtjevima iz Direktive (EU) 2015/2366 i ovog regulatornog tehničkog standarda.

(9) U skladu s Direktivom (EU) 2015/2366 izuzeća od načela pouzdane autentifikacije klijenta utvrđena su na temelju razine rizika, iznosa, ponavljanja i kanala plaćanja koji se upotrebljava za izvršenje platne transakcije.

(10) Radnje koje podrazumijevaju pristup stanju i nedavnim transakcijama po računu za plaćanje bez objave osjetljivih podataka o plaćanju, ponavljajuća plaćanja istim primateljima plaćanja koja je platitelj prethodno spremio ili potvrdio upotrebom pouzdane autentifikacije klijenta i plaćanja istoj fizičkoj ili pravnoj osobi ili doznake od iste fizičke ili pravne osobe kada su oba računa kod istog pružatelja platnih usluga niske su razine rizika te pružatelji platnih usluga nisu obvezni primjenjivati pouzdanu autentifikaciju klijenta. Time se ne uzima u obzir da bi u skladu s člancima 65., 66. i 67. Direktive (EU) 2015/2366 pružatelji usluga iniciranja plaćanja, pružatelji platnih usluga koji izdaju kartične platne instrumente i pružatelji usluga pružanja informacija o računu trebali od pružatelja platnih usluga koji vodi račun tražiti i dobiti samo potrebne i ključne informacije za pružanje određene platne usluge uz suglasnost korisnika platnih usluga. Suglasnost se može dati pojedinačno za svaki zahtjev za informacije ili za svako plaćanje koje će se inicirati ili, u slučaju pružatelja usluga pružanja informacija o računu, kao ovlaštenje za određene račune za plaćanje i s njima povezane platne transakcije kako je utvrđeno u ugovoru s korisnikom platnih usluga.

(11) Izuzeća za beskontaktna plaćanja male vrijednosti na prodajnom mjestu, kojima se u obzir uzima i najveći broj uzastopnih transakcija ili određena fiksna najveća vrijednost uzastopnih transakcija bez primjene pouzdane autentifikacije klijenta, omogućuju razvoj niskorizičnih platnih usluga prilagođenih korisnicima te bi ih stoga trebalo predvidjeti. Trebalo bi i utvrditi iznimku u slučaju elektroničkih platnih transakcija iniciranih na samoposlužnim terminalima na kojima nije uvijek jednostavno primijeniti pouzdanu autentifikaciju klijenta iz operativnih razloga (npr. kako bi se izbjegla čekanja i moguće nezgode na naplatnim rampama ili zbog drugih sigurnosnih rizika).

(12) Slično izuzeću za beskontaktna plaćanja niske vrijednosti na prodajnom mjestu, trebalo bi postići odgovarajuću ravnotežu između interesa za većom sigurnosti plaćanja s udaljenosti i potrebe za korisniku prilagođenim i pristupačnim plaćanjima u području e-trgovine. U skladu s tim načelima trebalo bi razborito postaviti pragove ispod kojih nije potrebno primjenjivati pouzdanu autentifikaciju klijenta kako bi se obuhvatila samo kupnja na internetu niske vrijednosti. Trebalo bi razboritije postaviti pragove za kupnju na internetu jer je u tom slučaju sigurnosni rizik nešto viši zbog činjenice da osoba nije fizički prisutna u trenutku kupnje.

(13) Zahtjevi za pouzdanu autentifikaciju klijenta primjenjuju se na plaćanja koja inicira platitelj neovisno o tome radi li se o fizičkoj ili pravnoj osobi. Mnoga korporativna plaćanja iniciraju se posebnim postupcima i protokolima koji jamče visoke razine sigurnosti plaćanja, što se u skladu s Direktivom (EU) 2015/2366 želi postići uporabom pouzdane autentifikacije klijenta. Kada nadležna tijela utvrde da ti postupci i protokoli plaćanja koji su stavljeni na raspolaganje isključivo platiteljima koji nisu potrošači ispunjavaju ciljeve Direktive (EU) 2015/2366 u pogledu sigurnosti, pružatelji platnih usluga mogu u pogledu navedenih postupaka i protokola biti izuzeti od primjene zahtjeva za pouzdanu autentifikaciju klijenta.

(14) Ako se analizom rizika transakcije u stvarnom vremenu platna transakcija svrsta u kategoriju niskog rizika, primjereno je također uvesti izuzeće za pružatelja platnih usluga koji ne namjerava primijeniti pouzdanu autentifikaciju klijenta uvođenjem učinkovitih zahtjeva koji se temelje na riziku i kojima se jamči sigurnost sredstava i osobnih podataka korisnika platnih usluga. U okviru tih zahtjeva utemeljenih na riziku trebali bi se kombinirati rezultati analize rizika, koji potvrđuju da nije utvrđen neuobičajen obrazac potrošnje ili ponašanja platitelja, uzimajući u obzir druge čimbenike rizika, uključujući informacije o lokaciji platitelja i primatelja plaćanja, s novčanim pragovima koji se temelje na stopama prijevare izračunanima za plaćanja s udaljenosti. Ako se na temelju analize rizika transakcije u stvarnom vremenu plaćanje ne može odrediti kao niskorizično, pružatelj platnih usluga trebao bi primijeniti pouzdanu autentifikaciju klijenta. Najveću vrijednost tog izuzeća utemeljenog na riziku trebalo bi utvrditi tako da se osigura vrlo niska odgovarajuća stopa prijevare, među ostalim i usporedbom sa stopama prijevare svih platnih transakcija pružatelja platnih usluga u određenom razdoblju i na kontinuiranoj osnovi, uključujući one koje su autentificirane primjenom pouzdane autentifikacije klijenta.

(15) Kako bi se osigurala učinkovita provedba, pružatelji platnih usluga koji žele iskoristiti mogućnost izuzećâ od pouzdane autentifikacije klijenta trebali bi redovito pratiti i za svaku vrstu platne transakcije nadležnim tijelima i Europskom nadzornom tijelu za bankarstvo (EBA) na zahtjev staviti na raspolaganje vrijednost prijevarnih ili neovlaštenih platnih transakcija i uočene stope prijevare za sve svoje platne transakcije, neovisno o tome jesu li autentificirane primjenom pouzdane autentifikacije klijenta ili izvršene u skladu s relevantnim izuzećem.

(16) Prikupljanje tih novih podataka o prethodnim stopama prijevare pri elektroničkim platnim transakcijama pridonijet će EBA-inom učinkovitom revidiranju pragova za izuzeće od pouzdane autentifikacije klijenta na temelju analize rizika transakcije u stvarnom vremenu. U skladu s člankom 98. stavkom 5. Direktive (EU) 2015/2366 i člankom 10. Uredbe (EU) br. 1093/2010 Europskog parlamenta i Vijeća ([1]) EBA bi trebala preispitati i prema potrebi dostaviti Komisiji nacrt ažuriranih regulatornih tehničkih standarda s novim pragovima i odgovarajućim stopama prijevare u cilju povećanja sigurnosti elektroničkih plaćanja s udaljenosti.

(17) Pružateljima platnih usluga koji primjenjuju bilo koje izuzeće koje treba predvidjeti trebalo bi omogućiti da u bilo kojem trenutku mogu primijeniti pouzdanu autentifikaciju klijenta za radnje i platne transakcije iz tih odredaba.

(18) Mjere za zaštitu povjerljivosti i cjelovitosti personaliziranih sigurnosnih podataka, kao i uređaji i softver za autentifikaciju, trebali bi ograničiti rizike povezane s prijevarom u obliku neovlaštene ili prijevarne uporabe platnog instrumenta i neovlaštenog pristupa računima za plaćanje. U tu svrhu treba uvesti zahtjeve za sigurno stvaranje i isporuku personaliziranih sigurnosnih podataka i njihovo povezivanje s korisnikom platnih usluga te osigurati uvjete za obnovu i deaktivaciju tih sigurnosnih podataka.

(19) Kako bi se osigurala učinkovita i sigurna komunikacija između relevantnih aktera u kontekstu usluga pružanja informacija o računu, usluga iniciranja plaćanja i potvrde raspoloživosti sredstava, treba utvrditi zahtjeve za zajedničke i sigurne otvorene standarde komunikacije koje moraju ispuniti svi relevantni pružatelji platnih usluga. Direktivom (EU) 2015/2366 predviđa se način na koji pružatelji usluga pružanja informacija o računu pristupaju informacijama o računu za plaćanje i način na koji ih upotrebljavaju. Stoga se ovom Uredbom ne mijenjaju pravila za pristup računima koji nisu računi za plaćanje.

([1]) Uredba (EU) br. 1093/2010 Europskog parlamenta i Vijeća od 24. studenoga 2010. o osnivanju europskog nadzornog tijela (Europskog nadzornog tijela za bankarstvo), kojom se izmjenjuje Odluka br. 716/2009/EZ i stavlja izvan snage Odluka Komisije 2009/78/EZ (SL L 331, 15.12.2010., str. 12.).

(20) Svaki pružatelj platnih usluga koji vodi račune za plaćanje dostupne putem interneta trebao bi nuditi barem jedno sučelje za pristup koje omogućava sigurnu komunikaciju s pružateljima usluga pružanja informacija o računu, pružateljima usluga iniciranja plaćanja i pružateljima platnih usluga koji izdaju kartične platne instrumente. Sučelje bi pružateljima usluga pružanja informacija o računu, pružateljima usluga iniciranja plaćanja i pružateljima platnih usluga koji izdaju kartične platne instrumente trebalo omogućiti da se identificiraju pružatelju platnih usluga koji vodi račun. Osim toga, sučelje bi i pružateljima usluga pružanja informacija o računu i pružateljima usluga iniciranja plaćanja trebalo omogućiti da se mogu pouzdati u postupke autentifikacije koje pružatelj platnih usluga koji vodi račun pruža korisniku platnih usluga. Kako bi se osigurala tehnološka neutralnost i neutralnost poslovnog modela, pružatelji platnih usluga koji vode račune trebali bi moći odlučiti žele li ponuditi sučelje namijenjeno komunikaciji s pružateljima usluga pružanja informacija o računu, pružateljima usluga iniciranja plaćanja i pružateljima platnih usluga koji izdaju kartične platne instrumente ili žele li za tu komunikaciju omogućiti upotrebu sučelja za identifikaciju i komunikaciju s korisnicima platnih usluga koje pruža pružatelj platnih usluga koji vodi račun.

(21) Tehničke specifikacije sučelja trebale bi biti primjereno dokumentirane i javno dostupne kako bi se pružateljima usluga pružanja informacija o računu, pružateljima usluga iniciranja plaćanja i pružateljima platnih usluga koji izdaju kartične platne instrumente omogućio razvoj vlastitih tehničkih rješenja. Osim toga, pružatelj platnih usluga koji vodi račun trebao bi ponuditi alat koji će pružateljima platnih usluga omogućiti testiranje tehnoloških rješenja tijekom barem šest mjeseci prije datuma primjene ovih regulatornih standarda ili prije datuma stavljanja sučelja na tržište ako je to nakon datuma primjene ovih standarda. Kako bi se osigurala interoperabilnost različitih tehnoloških komunikacijskih rješenja, sučelje bi trebalo primjenjivati standarde komunikacije koje su razvila međunarodna ili europska tijela za normizaciju.

(22) Kvaliteta usluga koje pružaju pružatelji usluga pružanja informacija o računu i pružatelji usluga iniciranja plaćanja ovisit će o pravilnom funkcioniranju sučelja koja uspostavljaju ili prilagođavaju pružatelji platnih usluga koji vode račune. Stoga je važno da se u slučaju neusklađenosti takvih sučelja s odredbama ovih standarda poduzmu mjere kojima se osigurava kontinuitet poslovanja u korist korisnika tih usluga. Odgovornost je nacionalnih nadležnih tijela osigurati da se pružatelje usluga pružanja informacija o računu i pružatelje usluga iniciranja plaćanja ne blokira ili ometa u pružanju njihovih usluga.

(23) Ako se pristup računima za plaćanje nudi putem namjenskog sučelja, kako bi se korisnicima platnih usluga osiguralo pravo da upotrebljavaju usluge pružatelja usluga iniciranja plaćanja i usluge koje omogućuju pristup informacijama o računu u skladu s Direktivom (EU) 2015/2366, namjenska sučelja trebaju imati istu razinu dostupnosti i učinkovitosti kao i sučelje dostupno korisniku platnih usluga. Pružatelji platnih usluga koji vode račune trebali bi definirati i transparentne ključne pokazatelje uspješnosti i ciljnu razinu usluga u pogledu dostupnosti i učinkovitosti namjenskih sučelja koji su barem jednako strogi kao oni za sučelje koje se koristi za njihove korisnike platnih usluga. Ta bi namjenska sučelja trebali testirati pružatelji platnih usluga koji će ih upotrebljavati, a nadležna tijela trebala bi ispitivati njihovu otpornost na stres i pratiti ih.

(24) Kako bi pružatelji platnih usluga koji se oslanjaju na namjensko sučelje mogli nastaviti pružati svoje usluge u slučaju poteškoća s dostupnošću ili nepravilnog funkcioniranja, nužno je pružiti pomoćni mehanizam koji će u skladu sa strogim uvjetima tim pružateljima omogućiti korištenje sučelja koje pružatelj platnih usluga koji vodi račun održava za identifikaciju svojih korisnika platnih usluga i komunikaciju s njima. Određeni pružatelji platnih usluga koji vode račune bit će izuzeti iz obveze osiguravanja takvog pomoćnog mehanizma putem svojih sučelja za klijente u slučaju da njihova nadležna tijela utvrde da su namjenska sučelja u skladu s posebnim uvjetima kojima se osigurava neometano tržišno natjecanje. Ako izuzeta namjenska sučelja ne ispune potrebne uvjete, relevantna nadležna tijela ukidaju odobrena izuzeća.

(25) Kako bi se nadležnim tijelima omogućio učinkovit nadzor i praćenje provedbe komunikacijskih sučelja i upravljanja njima, pružatelji platnih usluga koji vode račune trebali bi na svojim internetskim stranicama objaviti sažetak relevantne dokumentacije i na zahtjev dostaviti nadležnim tijelima dokumentaciju o rješenjima u izvanrednim situacijama. Pružatelji platnih usluga koji vode račune trebali bi i javno objaviti statističke podatke o dostupnosti i učinkovitosti tog sučelja.

(26) Kako bi se zaštitila povjerljivost i cjelovitost podataka, potrebno je osigurati sigurnost komunikacijskih sesija između pružatelja platnih usluga koji vode račune, pružatelja usluga pružanja informacija o računu, pružatelja usluga iniciranja plaćanja i pružatelja platnih usluga koji izdaju kartične platne instrumente. Osobito je važno

zahtijevati primjenu sigurnog kodiranja pri razmjeni podataka između pružatelja usluga pružanja informacija o računu, pružatelja usluga iniciranja plaćanja, pružatelja platnih usluga koji izdaju kartične platne instrumente i pružatelja platnih usluga koji vode račune.

(27) Kako bi se povećalo povjerenje korisnika i osigurala pouzdana autentifikacija klijenta, trebalo bi uzeti u obzir upotrebu sredstava elektroničke identifikacije i usluga povjerenja kako je utvrđeno u Uredbi (EU) br. 910/2014 Europskog parlamenta i Vijeća ([1]), osobito u pogledu prijavljenih sustava elektroničke identifikacije.

(28) Kako bi se osigurala usklađenost datuma primjene, ova bi se Uredba trebala primjenjivati od istog datuma od kojeg države članice moraju osigurati primjenu sigurnosnih mjera navedenih u člancima 65., 66., 67. i 97. Direktive (EU) 2015/2366.

(29) Ova se Uredba temelji na nacrtima regulatornih tehničkih standarda koje je Europsko nadzorno tijelo za bankarstvo (EBA) dostavilo Komisiji.

(30) EBA je provela otvorena i transparentna javna savjetovanja o nacrtima regulatornih tehničkih standarda na kojima se temelji ova Uredba, analizirala potencijalne povezane troškove i koristi te zatražila mišljenje Interesne skupine za bankarstvo osnovane u skladu s člankom 37. Uredbe (EU) br. 1093/2010,

DONIJELA JE OVU UREDBU:

POGLAVLJE I.

OPĆE ODREDBE

Članak 1.

Predmet

Ovom Uredbom utvrđuju se zahtjevi koje trebaju ispunjavati pružatelji platnih usluga za potrebe provedbe sigurnosnih mjera koje im omogućuju sljedeće:

(a) primjenu pouzdane autentifikacije klijenta u skladu s člankom 97. Direktive (EU) 2015/2366;

(b) izuzeće od primjene sigurnosnih zahtjeva za pouzdanu autentifikaciju klijenta, koje podliježe određenim i ograničenim uvjetima koji se temelje na razini rizika, iznosu i ponavljanju platne transakcije te kanalu plaćanja koji se koristi za izvršenje transakcije;

(c) zaštitu povjerljivosti i cjelovitosti personaliziranih sigurnosnih podataka korisnika platnih usluga;

(d) uspostavu zajedničkih i sigurnih otvorenih standarda komunikacije među pružateljima platnih usluga koji vode račune, pružateljima usluga iniciranja plaćanja, pružateljima usluga pružanja informacija o računu, platiteljima, primateljima plaćanja i drugim pružateljima platnih usluga u vezi s pružanjem i uporabom platnih usluga u svrhu primjene glave IV. Direktive (EU) 2015/2366.

Članak 2.

Opći zahtjevi za autentifikaciju

1. Pružatelji platnih usluga uspostavljaju mehanizme za praćenje transakcija koji im omogućuju otkrivanje neovlaštenih ili prijevarnih platnih transakcija za potrebe provedbe sigurnosnih mjera iz članka 1. točaka (a) i (b).

([1]) Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ (SL L 257, 28.8.2014., str. 53.).

Ti se mehanizmi temelje na analizi platnih transakcija kojom se uzimaju u obzir elementi tipični za korisnika platnih usluga u okviru uobičajene upotrebe personaliziranih sigurnosnih podataka.

2. Pružatelji platnih usluga osiguravaju da se mehanizmima za praćenje transakcija nužno uzimaju u obzir barem svi sljedeći čimbenici rizika:

(a) popis ugroženih ili ukradenih elemenata za autentifikaciju;

(b) iznos svake platne transakcije;

(c) poznati scenariji prijevare pri pružanju platnih usluga;

(d) znakovi infekcije zlonamjernim programima u bilo kojoj sesiji postupka autentifikacije;

(e) ako pružatelj platnih usluga osigurava uređaj ili softver za pristup, zapisnik upotrebe uređaja ili softvera za pristup koji su dostavljeni korisniku platnih usluga i neuobičajena upotreba uređaja ili softvera za pristup.

Članak 3.

Preispitivanje sigurnosnih mjera

1. Provedbu sigurnosnih mjera iz članka 1. dokumentiraju, periodično testiraju, ocjenjuju i revidiraju revizori s iskustvom u području IT sigurnosti i platnog prometa koji djeluju neovisno unutar pružatelja platnih usluga ili neovisno o njemu, u skladu s pravnim okvirom koji je primjenjiv na pružatelja platnih usluga.

2. Razdoblje između revizija iz stavka 1. određuje se u skladu s odgovarajućim okvirom za računovodstvo i zakonsku reviziju koji se primjenjuju na pružatelja platnih usluga.

Međutim, pružatelji platnih usluga koji se koriste izuzećem iz članka 18. podliježu reviziji metodologije, modela i prijavljene stope prijevara najmanje jednom godišnje. Revizor koji provodi predmetnu reviziju ima iskustvo u području IT sigurnosti i platnog prometa i djeluje neovisno unutar pružatelja platnih usluga ili neovisno o njemu. Tijekom prve godine primjene izuzeća na temelju članka 18. i najmanje tri godine nakon toga ili češće, na zahtjev nadležnog tijela, tu reviziju provodi neovisni i kvalificirani vanjski revizor.

3. Ta revizija sadržava ocjenu i izvješće o usklađenosti sigurnosnih mjera pružatelja platnih usluga sa zahtjevima iz ove Uredbe.

Cjelovito izvješće stavlja se na raspolaganje nadležnim tijelima na njihov zahtjev.

POGLAVLJE II.

SIGURNOSNE MJERE ZA PRIMJENU POUZDANE AUTENTIFIKACIJE KLIJENTA

Članak 4.

Kôd za autentifikaciju

1. Ako pružatelji platnih usluga primjenjuju pouzdanu autentifikaciju klijenta u skladu s člankom 97. stavkom 1. Direktive (EU) 2015/2366, autentifikacija se temelji na dva ili više elemenata koji pripadaju kategoriji znanja, posjedovanja i svojstvenosti i rezultira generiranjem kôda za autentifikaciju.

Pružatelj platnih usluga prihvaća kôd za autentifikaciju samo jednom kada platitelj koristi kôd za autentifikaciju kako bi svojem računu za plaćanje pristupio preko interneta, inicirao elektroničku platnu transakciju ili izvršio bilo koju radnju s udaljenosti koja može podrazumijevati rizik u smislu prijevara povezanih s plaćanjem ili drugih oblika zlouporabe.

2. Za potrebe stavka 1. pružatelji platnih usluga uspostavljaju sigurnosne mjere kojima se osigurava ispunjavanje svih sljedećih zahtjeva:

(a) otkrivanjem kôda za autentifikaciju nije moguće utvrditi informacije o bilo kojem elementu iz stavka 1.;

(b) novi kôd za autentifikaciju ne može se generirati na temelju saznanja o bilo kojem prethodno generiranom kôdu za autentifikaciju;

(c) kôd za autentifikaciju ne može se krivotvoriti.

3. Pružatelji platnih usluga osiguravaju da autentifikacija na temelju generiranja kôda za autentifikaciju obuhvaća sve sljedeće mjere:

(a) ako se kod za autentifikaciju za potrebe stavka 1. nije generirao autentifikacijom za potrebe pristupa s udaljenosti, elektroničkog plaćanja s udaljenosti i svih drugih radnji koje se izvršavaju s udaljenosti i koje mogu podrazumijevati rizik u pogledu prijevara povezanih s plaćanjem ili drugih oblika zlouporabe, nije moguće utvrditi koji je element iz tog stavka bio pogrešan;

(b) broj uzastopnih neuspješnih pokušaja autentifikacije, nakon kojih se radnje iz članka 97. stavka 1. Direktive (EU) 2015/2366 privremeno ili trajno blokiraju, ne smije biti veći od pet tijekom određenog razdoblja;

(c) komunikacijske sesije zaštićene su od bilježenja podataka o autentifikaciji koji se prenose tijekom autentifikacije i od manipulacije neovlaštenih osoba u skladu sa zahtjevima iz poglavlja V.;

(d) najdulje razdoblje bez aktivnosti platitelja nakon što je autentificiran za internetski pristup svojem računu za plaćanje ne smije biti dulje od pet minuta.

4. Ako je blokada iz stavka 3. točke (b) privremena, njezino trajanje i broj ponovnih pokušaja određuje se na temelju karakteristika usluga koje se pružaju platitelju i svih relevantnih povezanih rizika, uzimajući u obzir barem čimbenike iz članka 2. stavka 2.

Platitelja se obavješćuje prije nego što blokada postane trajna.

Ako blokada postane trajna, uspostavlja se sigurnosni postupak kojim se platitelju omogućuje ponovna upotreba blokiranih elektroničkih platnih instrumenata.

Članak 5.

Dinamično povezivanje

1. Ako pružatelji platnih usluga primjenjuju pouzdanu autentifikaciju klijenta u skladu s člankom 97. stavkom 2. Direktive (EU) 2015/2366, oni uz zahtjeve iz članka 4. ove Uredbe uvode i sigurnosne mjere koje ispunjavaju sve sljedeće zahtjeve:

(a) platitelj je obaviješten o iznosu platne transakcije i o primatelju plaćanja;

(b) generirani kôd za autentifikaciju određen je za iznos platne transakcije i primatelja plaćanja koje je platitelj naznačio pri iniciranju transakcije;

(c) kôd za autentifikaciju koji je pružatelj platnih usluga prihvatio odgovara izvorno navedenom iznosu platne transakcije i identitetu primatelja plaćanja koje je platitelj naznačio;

(d) svaka promjena iznosa ili primatelja plaćanja dovodi do poništenja generiranog kôda za autentifikaciju.

2. Za potrebe stavka 1. pružatelji platnih usluga uspostavljaju sigurnosne mjere kojima se osigurava povjerljivost, autentičnost i cjelovitost svih podataka u nastavku:

(a) iznosa transakcije i primatelja plaćanja tijekom svih faza autentifikacije;

(b) informacija koje se platitelju prikazuju tijekom svih faza autentifikacije, uključujući generiranje, prijenos i upotrebu kôda za autentifikaciju.

3. Za potrebe stavka 1. točke (b) i ako pružatelji platnih usluga primjenjuju pouzdanu autentifikaciju klijenta u skladu s člankom 97. stavkom 2. Direktive (EU) 2015/2366, primjenjuju se sljedeći zahtjevi za kôd za autentifikaciju:

(a) u pogledu platne transakcije na temelju kartica za koju je platitelj dao suglasnost za točan iznos novčanih sredstava koja će se blokirati u skladu s člankom 75. stavkom 1. te Direktive, kôd za autentifikaciju specifičan je za iznos za čije je blokiranje platitelj dao suglasnost i koji je pri iniciranju transakcije naznačio;

(b) u pogledu platnih transakcija za koje je platitelj dao suglasnost za izvršenje skupine elektroničkih platnih transakcija s udaljenosti upućenih jednom ili više primatelja plaćanja, kôd za autentifikaciju specifičan je za ukupni iznos skupine platnih transakcija i za naznačene primatelje plaćanja.

Članak 6.

Zahtjevi za elemente koji pripadaju kategoriji znanja

1. Pružatelji platnih usluga uspostavljaju mjere za smanjenje rizika da neovlaštene osobe otkriju ili da im se otkriju elementi pouzdane autentifikacije klijenta koji pripadaju kategoriji znanja.

2. Upotreba tih elemenata od strane platitelja podliježe primjeni mjera smanjenja rizika kako bi se spriječilo otkrivanje neovlaštenim osobama.

Članak 7.

Zahtjevi za elemente koji pripadaju kategoriji posjedovanja

1. Pružatelji platnih usluga uspostavljaju mjere za smanjenje rizika upotrebe elemenata pouzdane autentifikacije klijenta koji pripadaju kategoriji posjedovanja od strane neovlaštenih osoba.

2. Upotreba tih elemenata od strane platitelja podliježe primjeni mjera kojima je svrha spriječiti replikaciju tih elemenata.

Članak 8.

Zahtjevi za uređaje i softver koji su povezani s elementima koji pripadaju kategoriji svojstvenosti

1. Pružatelji platnih usluga uspostavljaju mjere za smanjenje rizika da neovlaštene osobe otkriju elemente autentifikacije koji pripadaju kategoriji svojstvenosti i koje učitavaju uređaji i softver za pristup koji su dostavljeni platitelju. Pružatelji platnih usluga kao minimum osiguravaju da ti uređaji i softver za pristup imaju vrlo nisku vjerojatnost da se neovlaštena osoba autentificira kao platitelj.

2. Pri upotrebi tih elemenata od strane platitelja primjenjuju se mjere kojima se jamči otpornost tih uređaja i softvera na neovlaštenu upotrebu tih elemenata u slučaju pristupa tim uređajima i softveru.

Članak 9.

Neovisnost elemenata

1. Pružatelji platnih usluga osiguravaju da upotreba elemenata pouzdane autentifikacije klijenta iz članaka 6., 7. i 8. podliježe mjerama kojima se osigurava da proboj jednog od elemenata u pogledu tehnologije, algoritama i parametara ne umanjuje pouzdanost ostalih elemenata.

2. Pružatelji platnih usluga u slučaju upotrebe bilo kojeg elementa pouzdane autentifikacije klijenta ili samog kôda za autentifikaciju putem višenamjenskog uređaja uspostavljaju sigurnosne mjere radi smanjenja rizika koji bi mogao nastati zloupotrebom višenamjenskog uređaja.

3. Za potrebe stavka 2. mjere smanjenja rizika uključuju sve mjere navedene u nastavku:

(a) upotreba odvojenih sigurnih okruženja za izvršavanje s pomoću softvera instaliranog na višenamjenskom uređaju;

(b) mehanizmi kojima se osigurava da platitelj ili treća strana ne mogu preinačiti softver ili uređaj;

(c) u slučaju njihove preinake, mehanizmi kojima se ublažavaju posljedice preinake.

POGLAVLJE III.

IZUZEĆA OD POUZDANE AUTENTIFIKACIJE KLIJENTA

Članak 10.

Informacije o računu za plaćanje

1. Pružateljima platnih usluga dopušteno je ne primjenjivati pouzdanu autentifikaciju klijenta uz uvjet da poštuju zahtjeve iz članka 2. i stavka 2. ovog članka ako je korisnik platnih usluga ograničen na internetski pristup jednoj ili objema stavkama u nastavku bez objave osjetljivih podataka o plaćanju:

(a) stanje na jednom ili više utvrđenih računa za plaćanje;

(b) platne transakcije izvršene u posljednjih 90 dana preko jednog ili više utvrđenih računa za plaćanje.

2. Za potrebe stavka 1. pružatelji platnih usluga nisu izuzeti od primjene pouzdane autentifikacije klijenta ako je ispunjen bilo koji od sljedeća dva uvjeta:

(a) korisnik platnih usluga putem interneta prvi put pristupa informacijama iz stavka 1.;

(b) prošlo je više od 90 dana od kada je korisnik platnih usluga posljednji put putem interneta pristupio informacijama iz stavka 1. točke (b) uz primjenu pouzdane autentifikacije klijenta.

Članak 11.

Beskontaktna plaćanja na prodajnom mjestu

Pružateljima platnih usluga dopušteno je ne primjenjivati pouzdanu autentifikaciju klijenta uz uvjet da poštuju zahtjeve iz članka 2. ako platitelj inicira beskontaktnu elektroničku platnu transakciju i ispunjeni su sljedeći uvjeti:

(a) pojedinačni iznos beskontaktne elektroničke platne transakcije ne prelazi 50 EUR; i

(b) ukupna vrijednost prethodnih beskontaktnih elektroničkih platnih transakcija koje su inicirane platnim instrumentom s beskontaktnom funkcijom u razdoblju od datuma posljednje primjene pouzdane autentifikacije klijenta ne prelazi 150 EUR; ili

(c) broj uzastopnih beskontaktnih elektroničkih platnih transakcija iniciranih platnim instrumentom opremljenim beskontaktnom funkcijom u razdoblju od posljednje primjene pouzdane autentifikacije klijenta nije veći od pet.

Članak 12.

Samoposlužni terminali za plaćanje prijevoza i naknada za parkiranje

Pružateljima platnih usluga dopušteno je ne primjenjivati pouzdanu autentifikaciju klijenta uz uvjet da poštuju zahtjeve iz članka 2. ako platitelj inicira elektroničku platnu transakciju na samoposlužnom terminalu za potrebe plaćanje prijevoza i naknada za parkiranje.

Članak 13.

Provjereni korisnici

1. Pružatelji platnih usluga primjenjuju pouzdanu autentifikaciju klijenta u slučajevima kada platitelj stvara ili mijenja popis provjerenih korisnika preko pružatelja platnih usluga koji vodi račun.

2. Pružateljima platnih usluga dopušteno je ne primjenjivati pouzdanu autentifikaciju klijenta uz uvjet da poštuju opće zahtjeve za autentifikaciju ako platitelj inicira platnu transakciju, a primatelj plaćanja nalazi se na popisu provjerenih korisnika koji je prethodno izradio platitelj.

Članak 14.

Ponavljajuće transakcije

1. Pružatelji platnih usluga primjenjuju pouzdanu autentifikaciju klijenta ako platitelj stvara, mijenja ili prvi put inicira niz ponavljajućih transakcija s istim iznosom i istim primateljem plaćanja.

2. Pružateljima platnih usluga dopušteno je ne primjenjivati pouzdanu autentifikaciju klijenta, uz uvjet da poštuju opće zahtjeve za autentifikaciju, pri iniciranju svih naknadnih platnih transakcija uvrštenih u niz platnih transakcija iz stavka 1.

Članak 15.

Kreditni transferi između računa koje posjeduje ista fizička ili pravna osoba

Pružateljima platnih usluga dopušteno je ne primjenjivati pouzdanu autentifikaciju klijenta uz uvjet da poštuju zahtjeve iz članka 2. ako platitelj inicira kreditni transfer u okolnostima gdje su platitelj i primatelj plaćanja ista fizička ili pravna osoba i oba računa za plaćanje drži isti pružatelj platnih usluga koji vodi račun.

Članak 16.

Transakcije male vrijednosti

Pružateljima platnih usluga dopušteno je ne primjenjivati pouzdanu autentifikaciju klijenta ako platitelj inicira elektroničku platnu transakciju s udaljenosti i ispunjeni su sljedeći uvjeti:

(a) iznos elektroničke platne transakcije s udaljenosti ne prelazi 30 EUR; i

(b) ukupna vrijednost prethodnih elektroničkih platnih transakcija s udaljenosti koje je platitelj inicirao od posljednje primjene pouzdane autentifikacije klijenta ne prelazi 100 EUR; ili

(c) broj prethodnih elektroničkih platnih transakcija s udaljenosti koje je platitelj inicirao od posljednje primjene pouzdane autentifikacije klijenta nije veći od 5 uzastopnih pojedinačnih elektroničkih platnih transakcija s udaljenosti.

Članak 17.

Sigurni korporativni postupci i protokoli plaćanja

Pružateljima platnih usluga dopušteno je ne primjenjivati pouzdanu autentifikaciju klijenta u pogledu pravnih osoba koje iniciraju elektroničke platne transakcije s pomoću namjenskih postupaka i protokola plaćanja koji su stavljeni na raspolaganja isključivo platiteljima koji nisu potrošači, a nadležna tijela utvrdila su da se tim postupcima ili protokolima jamče razine sigurnosti koje su barem jednakovrijedne onima iz Direktive (EU) 2015/2366.

Članak 18.

Analiza rizika transakcije

1. Pružateljima platnih usluga dopušteno je ne primjenjivati pouzdanu autentifikaciju klijenta ako platitelj inicira elektroničku platnu transakciju s udaljenosti za koju je pružatelj platnih usluga utvrdio da predstavlja niski rizik u skladu s mehanizmima za praćenje transakcija iz članka 2. i stavka 2. točke (c) ovog članka.

2. Smatra se da elektronička platna transakcija iz stavka 1. predstavlja niski rizik ako su ispunjeni svi sljedeći uvjeti:

(a) stopa prijevare za tu vrstu transakcije, prema izvješćima pružatelja platnih usluga i izračunana u skladu s člankom 19., jednaka je ili niža od referentnih stopa prijevare iz tablice u Prilogu za stavke „elektronička plaćanja na temelju kartica s daljine" odnosno „elektronički kreditni transferi s udaljenosti";

(b) iznos transakcije ne prelazi relevantnu vrijednost praga za izuzeće navedenu u tablici iz Priloga;

(c) pružatelji platnih usluga nakon provedbe analize rizika u realnom vremenu nisu utvrdili nijedno od sljedećeg:

   i. neuobičajeni obrazac potrošnje ili ponašanja platitelja;

   ii. neuobičajene informacije o pristupu uređaju/softveru od strane platitelja;

   iii. infekciju zlonamjernim programima u bilo kojoj sesiji postupka autentifikacije;

   iv. poznati scenarij prijevare pri pružanju platnih usluga;

   v. neuobičajenu lokaciju platitelja;

   vi. visokorizičnu lokaciju primatelja plaćanja.

3. Pružatelji platnih usluga koji namjeravaju ne primjenjivati pouzdanu autentifikaciju klijenta za elektroničke platne transakcije s udaljenosti na temelju toga što predstavljaju niski rizik uzimaju u obzir najmanje sljedeće čimbenike rizika:

(a) prethodne obrasce potrošnje pojedinačnog korisnika platnih usluga;

(b) povijest platnih transakcija svakog od korisnika platnih usluga pružatelja platnih usluga;

(c) lokaciju platitelja i primatelja plaćanja u vrijeme platne transakcije u slučajevima kad pružatelj platnih usluga osigurava uređaj ili softver za pristup;

(d) identifikaciju neuobičajenih obrazaca plaćanja korisnika platnih usluga s obzirom na korisnikovu povijest platnih transakcija.

Pružatelj platnih usluga sve navedene čimbenike rizika u svojoj procjeni objedinjuje u ocjenu rizika za svaku pojedinačnu transakciju kako bi utvrdio treba li konkretno plaćanje odobriti bez pouzdane autentifikacije klijenta.

Članak 19.

Izračun stope prijevara

1. Pružatelj platnih usluga za svaku vrstu transakcije iz tablice u Prilogu osigurava da su ukupne stope prijevare za platne transakcije koje su autentificirane primjenom pouzdane autentifikacije klijenta i za transakcije izvršene u skladu s izuzećem iz članaka od 13. do 18. jednake ili niže od referentne stope prijevare za istu vrstu platne transakcije navedene u tablici iz Priloga.

Ukupna stopa prijevare za svaku vrstu transakcije izračunava se kao ukupna vrijednost neovlaštenih ili prijevarnih transakcija s udaljenosti, bez obzira na to jesu li sredstva vraćena ili ne, podijeljena s ukupnom vrijednošću svih transakcija s udaljenosti za istu vrstu transakcije, bez obzira na to jesu li autentificirane primjenom pouzdane autentifikacije klijenta ili su izvršene u skladu s izuzećem iz članaka od 13. do 18. na pomičnoj tromjesečnoj osnovi (90 dana).

2. Izračun stope prijevara i dobiveni rezultati procjenjuju se revizijskim pregledom iz članka 3. stavka 2., kojim se osigurava njihova potpunost i točnost.

3. Metodologija i svi modeli kojima se pružatelj platnih usluga koristi za izračun stopa prijevare i same stope prijevare primjereno se dokumentiraju i na zahtjev u cijelosti stavljaju na raspolaganje nadležnim tijelima i EBA-i, uz prethodnu obavijest relevantnom nadležnom tijelu ili tijelima.

Članak 20.

Prestanak primjene izuzeća na temelju analize rizika transakcije

1. Pružatelji platnih usluga koji se koriste izuzećem iz članka 18. nadležnim tijelima odmah prijavljuju slučajeve kada jedna od praćenih stopa prijevare, za bilo koju vrstu platne transakcije navedene u tablici iz Priloga, premaši primjenjivu referentnu stopu prijevare te im dostavljaju opis mjera koje namjeravaju poduzeti kako bi ponovno osigurali usklađenost svoje praćene stope prijevare s primjenjivim referentnim stopama prijevare.

2. Pružatelji platnih usluga odmah prestaju primjenjivati izuzeće iz članka 18. na sve platne transakcije navedene u tablici iz Priloga u određenom rasponu praga za izuzeće ako njihova praćena stopa prijevare tijekom dva uzastopna tromjesečja premašuje referentnu stopu prijevare koja se primjenjuje za taj platni instrument ili za tu vrstu platne transakcije u tom rasponu praga za izuzeće.

3. Nakon prestanka primjene izuzeća iz članka 18. u skladu sa stavkom 2. ovog članka pružatelji platnih usluga ne koriste se tim izuzećem sve dok njihova izračunana stopa prijevare ne bude jednaka ili niža od referentnih stopa prijevare za tu vrstu platne transakcije u tom rasponu praga za izuzeće tijekom jednog tromjesečja.

4. Ako se pružatelji platnih usluga namjeravaju ponovo koristiti izuzećem iz članka 18., oni u razumnom roku obavješćuju nadležna tijela, a prije ponovne primjene izuzeća pružaju dokaze o ponovnoj usklađenosti svoje praćene stope prijevare s primjenjivom referentnom stopom prijevare za taj raspon praga za izuzeće u skladu sa stavkom 3. ovog članka.

Članak 21.

Praćenje

1. Kako bi se koristili izuzećima iz članaka od 10. do 18., pružatelji platnih usluga bilježe i prate sljedeće podatke za svaku vrstu platne transakcije, uz raščlambu na platne transakcije s udaljenosti i platne transakcije koje se ne izvršavaju s udaljenosti, najmanje svaka tri mjeseca:

(a) ukupna vrijednost neovlaštenih ili prijevarnih platnih transakcija u skladu s člankom 64. stavkom 2. Direktive (EU) 2015/2366, ukupna vrijednost svih platnih transakcija i dobivene stope prijevare, uključujući raščlambu platnih transakcija koje su inicirane uz pouzdanu autentifikaciju klijenta i u okviru svakog izuzeća;

(b) prosječna vrijednost transakcije, uključujući raščlambu platnih transakcija koje su inicirane uz pouzdanu autentifikaciju klijenta i u okviru svakog izuzeća;

(c) broj platnih transakcija u kojima su primijenjena izuzeća i njihov postotak u odnosu na ukupan broj platnih transakcija.

2. Pružatelji platnih usluga rezultate praćenja u skladu sa stavkom 1. na zahtjev stavljaju na raspolaganje nadležnim tijelima i EBA-i, uz prethodnu obavijest relevantnom nadležnom tijelu ili tijelima.

POGLAVLJE IV.

POVJERLJIVOST I CJELOVITOST PERSONALIZIRANIH SIGURNOSNIH PODATAKA KORISNIKA PLATNIH USLUGA

Članak 22.

Opći zahtjevi

1. Pružatelji platnih usluga osiguravaju povjerljivost i cjelovitost personaliziranih sigurnosnih podataka korisnika platnih usluga, među ostalim i kôdova za autentifikaciju, tijekom svih faza autentifikacije.

2. Za potrebe stavka 1. pružatelji platnih usluga osiguravaju da su ispunjeni svi sljedeći zahtjevi:

(a) personalizirani sigurnosni podaci prikriveni su tijekom prikaza i nisu u potpunosti čitljivi kad ih korisnik platnih usluga unosi tijekom autentifikacije;

(b) personalizirani sigurnosni podaci u formatu podataka i kriptografski materijali povezani sa šifriranjem personaliziranih sigurnosnih podataka ne spremaju se kao nešifrirani podaci;

(c) tajni kriptografski materijal zaštićen je od neovlaštenog otkrivanja.

3. Pružatelji platnih usluga u cijelosti dokumentiraju postupak povezan s upravljanjem kriptografskim materijalom kojim se personalizirani sigurnosni podaci šifriraju ili na drugi način čine nečitljivima.

4. Pružatelji platnih usluga osiguravaju da se obrada i preusmjeravanje personaliziranih sigurnosnih podataka i kôdova za autentifikaciju koji su generirani u skladu s poglavljem II. odvija u sigurnim okruženjima u skladu s pouzdanim i općepriznatim industrijskim standardima.

Članak 23.

Nastanak i prijenos sigurnosnih podataka

Pružatelji platnih usluga osiguravaju da se personalizirani sigurnosni podaci stvaraju u sigurnom okruženju.

Oni smanjuju rizik od neovlaštene upotrebe personaliziranih sigurnosnih podataka te uređaja i softvera za autentifikaciju nakon njihova gubitka, krađe ili kopiranja prije isporuke platitelju.

Članak 24.

Povezivanje s pružateljem platnih usluga

1. Pružatelji platnih usluga osiguravaju da je samo korisnik platnih usluga povezan, na siguran način, s personaliziranim sigurnosnim podacima te uređajima i softverom za autentifikaciju.

2. Za potrebe stavka 1. pružatelji platnih usluga osiguravaju da su ispunjeni svi sljedeći zahtjevi:

(a) povezivanje identiteta korisnika platnih usluga s personaliziranim sigurnosnim podacima te uređajima i softverom za autentifikaciju obavlja se u sigurnim okruženjima za koje je odgovoran pružatelj platnih usluga, što obuhvaća barem poslovne prostore pružatelja platnih usluga, internetsko okruženje koje osigurava pružatelj platnih usluga ili slična sigurna *web*-mjesta kojima se koristi pružatelj platnih usluga i njegove usluge bankomata, uzimajući u obzir rizike povezane s uređajima i povezanim komponentama koji se upotrebljavaju tijekom postupka povezivanja za koje nije odgovoran pružatelj platnih usluga;

(b) povezivanje s udaljenosti identiteta korisnika platnih usluga s personaliziranim sigurnosnim podacima te uređajima i softverom za autentifikaciju obavlja se uz primjenu pouzdane autentifikacije klijenta.

Članak 25.

Isporuka sigurnosnih podataka i uređajâ i softvera za autentifikaciju

1. Pružatelji platnih usluga osiguravaju da se isporuka personaliziranih sigurnosnih podataka te uređajâ i softvera za autentifikaciju korisniku platnih usluga obavlja na siguran način osmišljen tako da se vodi računa o riziku povezanom s neovlaštenom upotrebom u slučaju njihova gubitka, krađe ili kopiranja.

2. Pružatelji platnih usluga za potrebe stavka 1. nužno primjenjuju sve sljedeće mjere:

(a) učinkovite i sigurne mehanizme isporuke kojima se osigurava isporuka personaliziranih sigurnosnih podataka te uređajâ i softvera za autentifikaciju zakonitom korisniku platnih usluga;

(b) mehanizme koji pružatelju platnih usluga omogućuju provjeru autentičnosti softvera za autentifikaciju koji je korisniku platnih usluga isporučen putem interneta;

(c) aranžmane kojima se u slučaju isporuke personaliziranih sigurnosnih podataka izvan prostorija pružatelja platnih usluga ili s udaljenosti osigurava sljedeće:

i. neovlaštena osoba ne može dobiti više od jednog obilježja personaliziranih sigurnosnih podataka i uređajâ ili softvera za autentifikaciju kada se isporučuju istim kanalom;

ii. isporučeni personalizirani sigurnosni podaci te uređaji i softver za autentifikaciju prije upotrebe zahtijevaju aktivaciju;

(d) aranžmane kojima se u slučaju obvezne aktivacije personaliziranih sigurnosnih podataka i uređajâ ili softvera za autentifikaciju prije njihove prve upotrebe osigurava da se aktivacija odvija u sigurnom okruženju u skladu s postupcima povezivanja iz članka 24.

Članak 26.

Obnavljanje personaliziranih sigurnosnih podataka

Pružatelji platnih usluga osiguravaju da se obnavljanje ili ponovna aktivacija personaliziranih sigurnosnih podataka provodi u skladu s postupcima za stvaranje, povezivanje i isporuku sigurnosnih podataka i uređajâ za autentifikaciju u skladu s člancima 23., 24. i 25.

Članak 27.

Uništenje, deaktivacija i opoziv

Pružatelji platnih usluga osiguravaju uspostavu učinkovitih postupaka za primjenu svih sigurnosnih mjera navedenih u nastavku:

(a) sigurno uništenje, deaktivacija ili opoziv personaliziranih sigurnosnih podataka te uređajâ i softvera za autentifikaciju;

(b) ako pružatelj platnih usluga distribuira uređaje i softver za autentifikaciju za višekratnu uporabu, prije ponovnog stavljanja na raspolaganje drugom korisniku platnih usluga uspostavlja se, dokumentira i provodi sigurna ponovna upotreba uređaja ili softvera;

(c) deaktivacija ili opoziv informacija povezanih s personaliziranim sigurnosnim podacima pohranjenima u sustavima i bazama podataka pružatelja platnih usluga i, ovisno o slučaju, javnim repozitorijima.

POGLAVLJE V.

ZAJEDNIČKI I SIGURNI OTVORENI STANDARDI KOMUNIKACIJE

Odjeljak 1.

Opći zahtjevi za komunikaciju

Članak 28.

Zahtjevi za identifikaciju

1. Pružatelji platnih usluga osiguravaju sigurnu identifikaciju tijekom komunikacije između platiteljeva uređaja i uređajâ primatelja plaćanja za primanje elektroničkih plaćanja, uključujući među ostalim terminale za plaćanje.

2. Pružatelji platnih usluga osiguravaju učinkovito smanjenje rizika od pogrešnog usmjeravanja komunikacije prema neovlaštenim osobama u mobilnim aplikacijama i drugim sučeljima koja korisniku platnih usluga nude elektroničke platne usluge.

Članak 29.

Sljedivost

1. Pružatelji platnih usluga imaju uspostavljene postupke kojima se osigurava sljedivost svih platnih transakcija i drugih interakcija s korisnikom platnih usluga, drugim pružateljima platnih usluga i subjektima, uključujući trgovce, u kontekstu pružanja platne usluge i osigurava *ex post* informacije o svim događajima bitnima za elektroničku transakciju u svim fazama.

2. Za potrebe stavka 1. pružatelji platnih usluga osiguravaju da se svaka komunikacijska sesija koja je uspostavljena prema korisniku platnih usluga, drugim pružateljima platnih usluga i subjektima, uključujući trgovce, oslanja na svaku od sljedećih stavki:

(a) jedinstvenu identifikacijsku oznaku sesije;

(b) sigurnosne mehanizme za podrobno evidentiranje transakcije, uključujući broj transakcije, vremenske žigove i sve relevantne podatke o transakciji;

(c) vremenske žigove koji se temelje na jedinstvenom vremenskom referentnom sustavu i koji se sinkroniziraju sa službenim vremenskim signalom.

Odjeljak 2.

Posebni zahtjevi za zajedničke i sigurne otvorene standarde komunikacije

Članak 30.

Opće obveze u pogledu sučelja za pristup

1. Pružatelji platnih usluga koji vode račune koji platitelju nude račun za plaćanje s internetskim pristupom uspostavljaju najmanje jedno sučelje koje ispunjava sve sljedeće zahtjeve:

(a) pružatelji usluga pružanja informacija o računu, pružatelji usluga iniciranja plaćanja i pružatelji platnih usluga koji izdaju kartične platne instrumente mogu se identificirati prema pružatelju platnih usluga koji vodi račun;

(b) pružatelji usluga pružanja informacija o računu mogu sigurno komunicirati kad zahtijevaju i primaju informacije o jednom ili više utvrđenih računa za plaćanje i s njima povezanim platnim transakcijama;

(c) pružatelji usluga iniciranja plaćanja mogu sigurno komunicirati kad iniciraju nalog za plaćanje s platiteljeva računa za plaćanje i primaju sve informacije o iniciranju platne transakcije i sve informacije o izvršenju platne transakcije koje su dostupne pružateljima platnih usluga koji vode račune.

2. Za potrebe autentifikacije korisnika platnih usluga sučelje iz stavka 1. pružateljima usluga pružanja informacija o računu i pružateljima usluga iniciranja plaćanja omogućuje da se mogu oslanjati na sve postupke autentifikacije koje pružatelj platnih usluga koji vodi račun pruža korisniku platnih usluga.

Sučelje kao minimum ispunjava sve sljedeće zahtjeve:

(a) pružatelj usluga iniciranja plaćanja ili pružatelj usluga pružanja informacija o računu mogu dati uputu pružatelju platnih usluga koji vodi račun da pokrene autentifikaciju na temelju suglasnosti korisnika platnih usluga;

(b) komunikacijske sesije između pružatelja platnih usluga koji vodi račun, pružatelja usluga pružanja informacija o računu, pružatelja usluga iniciranja plaćanja i bilo kojeg predmetnog korisnika platnih usluga uspostavljaju se i održavaju tijekom cjelokupne autentifikacije;

(c) osigurana je cjelovitost i povjerljivost personaliziranih sigurnosnih podataka i kodova za autentifikaciju koje pružatelj usluga iniciranja plaćanja ili pružatelj usluga pružanja informacija o računu prenose ili koji se preko njih prenose.

3. Pružatelji platnih usluga koji vode račune osiguravaju usklađenost svojih sučelja sa standardima komunikacije koje izdaju međunarodne ili europske organizacije za normizaciju.

Pružatelji platnih usluga koji vode račune osiguravaju i dokumentiranje tehničkih specifikacija svih svojih sučelja uz navođenje skupa rutina, protokola i alata koji su pružateljima usluga iniciranja plaćanja, pružateljima usluga pružanja informacija o računu i pružateljima platnih usluga koji izdaju kartične platne instrumente potrebni kako bi mogli uspostaviti interoperabilnost između svojeg softvera i aplikacija i sustavâ pružatelja platnih usluga koji vode račune.

Kao minimalan zahtjev, pružatelji platnih usluga koji vode račune na zahtjev ovlaštenih pružatelja usluga iniciranja plaćanja, pružatelja usluga pružanja informacija o računu i pružatelja platnih usluga koji izdaju kartične platne instrumente ili pružatelja platnih usluga koji su svojim nadležnim tijelima podnijeli zahtjev za izdavanje relevantnog odobrenja bez naknade stavljaju na raspolaganje dokumentaciju i na svojem *web*-mjestu objavljuju javno dostupan sažetak dokumentacije najkasnije šest mjeseci prije datuma primjene iz članka 38. stavka 2. ili prije ciljnog datuma stavljanja na tržište sučelja za pristup ako je datum stavljanja na tržište kasniji od datuma iz članka 38. stavka 2.

4. Uz uvjete iz stavka 3., pružatelji platnih usluga koji vode račune osiguravaju, osim u izvanrednim situacijama, dostupnost svih izmjena tehničkih specifikacija svojih sučelja ovlaštenim pružateljima usluga iniciranja plaćanja, pružateljima usluga pružanja informacija o računu i pružateljima platnih usluga koji izdaju kartične platne instrumente ili pružateljima platnih usluga koji su svojim nadležnim tijelima podnijeli zahtjev za izdavanje relevantnog odobrenja, što je ranije moguće unaprijed, a najkasnije tri mjeseca prije implementacije izmjene.

Pružatelji platnih usluga u slučaju izmjena dokumentiraju izvanredne situacije i tu dokumentaciju na zahtjev stavljaju na raspolaganje nadležnim tijelima.

5. Pružatelji platnih usluga koji vode račune omogućuju platformu, uključujući potporu, za testiranje povezivanja i funkcioniranja koje ovlaštenim pružateljima usluga iniciranja plaćanja, pružateljima usluga pružanja informacija o računu i pružateljima platnih usluga koji izdaju kartične platne instrumente ili pružateljima platnih usluga koji su svojim nadležnim tijelima podnijeli zahtjev za izdavanje relevantnog odobrenja omogućuje testiranje njihova softvera i aplikacija koji se upotrebljavaju za pružanje platnih usluga korisnicima. Platforma za testiranje treba biti dostupna najkasnije šest mjeseci prije datuma primjene iz članka 38. stavka 2. ili prije ciljnog datuma stavljanja na tržište sučelja za pristup ako je datum stavljanja na tržište kasniji od datuma iz članka 38. stavka 2.

Na toj se platformi ne smiju dijeliti osjetljive informacije.

6. Nadležna tijela osiguravaju da pružatelji platnih usluga koji vode račune u svakom trenutku ispunjavaju sve obveze navedene u ovim standardima u pogledu sučeljâ koja su uspostavili. Ako pružatelji platnih usluga koji vode račune ne ispunjavaju zahtjeve u pogledu sučeljâ utvrđene u ovim standardima, nadležna tijela osiguravaju da ne dođe do sprječavanja ili prekida pružanja usluga iniciranja plaćanja i usluga pružanja informacija o računu u mjeri u kojoj pružatelji tih usluga ispunjavaju zahtjeve definirane u članku 33. stavku 5.

Članak 31.

Mogućnosti u pogledu sučelja za pristup

Pružatelji platnih usluga koji vode račune uspostavljaju sučelje (ili sučelja) iz članka 30. na način da osiguraju namjensko sučelje ili da pružateljima platnih usluga iz članka 30. stavka 1. omoguće uporabu sučelja koja se koriste za autentifikaciju i komunikaciju s korisnicima platnih usluga koje pruža pružatelj platnih usluga koji vodi račun.

Članak 32.

Obveze u pogledu namjenskog sučelja

1. Pod uvjetom primjene članaka 30. i 31., pružatelji platnih usluga koji vode račune koji su uspostavili namjensko sučelje osiguravaju da to namjensko sučelje u svakom trenutku nudi istu razinu dostupnosti i učinkovitosti, među ostalim i potporu, kao i sučelja koja su korisniku platnih usluga stavljena na raspolaganje za izravan internetski pristup svojem računu za plaćanje.

2. Pružatelji platnih usluga koji vode račune koji su uspostavili namjensko sučelje definiraju transparentne ključne pokazatelje učinkovitosti i ciljnu razinu usluga koji će i u pogledu dostupnosti i u pogledu pruženih podataka u skladu s člankom 36. biti barem jednako strogi kao oni za sučelje kojim se koriste korisnici njihovih platnih usluga. Nadležna tijela prate ta sučelja, pokazatelje i ciljeve te ispituju njihovu otpornost na stres.

3. Pružatelji platnih usluga koji vode račune koji su uspostavili namjensko sučelje osiguravaju da to sučelje ne stvara prepreke pružanju usluga iniciranja plaćanja i usluga pružanja informacija o računu. Te prepreke među ostalim mogu uključivati sprječavanje da pružatelji platnih usluga iz članka 30. stavka 1. upotrebljavaju podatke koje su pružatelji platnih usluga koji vode račune izdali svojim klijentima, nametanje preusmjeravanja na funkciju autentifikacije ili na druge funkcije pružatelja platnih usluga koji vode račune, zahtijevanje dodatnih odobrenja i registracija uz one koji su predviđeni člancima 11., 14. i 15. Direktive (EU) 2015/2366 ili zahtijevanje dodatnih provjera suglasnosti koje su korisnici platnih usluga dali pružateljima usluga iniciranja plaćanja i usluga pružanja informacija o računu.

4. Za potrebe stavaka 1. i 2. pružatelji platnih usluga koji vode račune prate dostupnost i učinkovitost namjenskog sučelja. Pružatelji platnih usluga koji vode račune objavljuju na svojem *web*-mjestu tromjesečne statističke podatke o dostupnosti i uspješnosti namjenskog sučelja i sučelja kojim se koriste korisnici njegovih platnih usluga.

Članak 33.

Izvanredne mjere povezane s namjenskim sučeljem

1. Pružatelji platnih usluga koji vode račune pri koncipiranju namjenskog sučelja uključuju strategiju i planove za izvanredne mjere u slučaju da sučelje ne funkcionira u skladu s člankom 32., da je sučelje neplanirano nedostupno ili u slučaju pada sustava. Može se smatrati da je sučelje neplanirano nedostupno ili da je došlo do pada sustava ako se na pet uzastopnih zahtjeva za pristup informacijama za pružanje usluga iniciranja plaćanja ili usluga pružanja informacija o računu ne odgovori u roku od 30 sekundi.

2. Izvanredne mjere uključuju komunikacijske planove za informiranje pružatelja platnih usluga putem namjenskog sučelja o mjerama za ponovnu uspostavu sustava i opis neposredno dostupnih alternativnih mogućnosti koje su pružateljima platnih usluga u međuvremenu na raspolaganju.

3. I pružatelji platnih usluga koji vode račune i pružatelji platnih usluga iz članka 30. stavka 1. svojim nadležnim nacionalnim tijelima bez odgađanja prijavljuju probleme povezane s namjenskim sučeljima kako je opisano u stavku 1.

4. U okviru mehanizma za izvanredne situacije pružateljima platnih usluga iz članka 30. stavka 1. dopušteno je koristiti se sučeljima koja su korisnicima platnih usluga stavljena na raspolaganje za autentifikaciju i komunikaciju s njihovim pružateljem platnih usluga koji vodi račun sve dok se ne osigura razina dostupnosti i učinkovitosti namjenskog sučelja propisana člankom 32.

5. U tu svrhu pružatelji platnih usluga koji vode račune osiguravaju da se pružatelji platnih usluga iz članka 30. stavka 1. mogu identificirati te da se mogu oslanjati na postupke autentifikacije koje pružatelj platnih usluga koji vodi račun pruža korisniku platnih usluga. Ako se pružatelji platnih usluga iz članka 30. stavka 1. koriste sučeljem iz stavka 4., dužni su sljedeće:

(a) poduzeti potrebne mjere kako bi osigurali da ne pristupaju podacima, ne pohranjuju podatke i ne obrađuju podatke za druge svrhe osim pružanja usluge koju je zatražio korisnik platne usluge;

(b) nastaviti ispunjavati obveze iz članka 66. stavka 3. i članka 67. stavka 2. Direktive (EU) 2015/2366;

(c) evidentirati podatke kojima se pristupa putem sučelja kojim pružatelj platnih usluga koji vodi račun upravlja za potrebe korisnika svojih platnih usluga te na zahtjev i bez odgađanja svojim nadležnim nacionalnim tijelima dostaviti datoteke zapisnika;

(d) nadležnim nacionalnim tijelima na zahtjev i bez neopravdanog odgađanja propisno obrazložiti uporabu sučelja koje je korisnicima platnih usluga stavljeno na raspolaganje za direktan internetski pristup svojem računu za plaćanje;

(e) na odgovarajući način obavijestiti pružatelja platnih usluga koji vodi račun.

6. Nadležna tijela, nakon savjetovanja s EBA-om radi osiguravanja dosljedne primjene sljedećih uvjeta, pružatelje platnih usluga koji vode račune koji su se odlučili za namjensko sučelje izuzimaju od obveze uspostave mehanizma za izvanredne situacije iz stavka 4. ako namjensko sučelje ispunjava sve sljedeće uvjete:

(a) ispunjuje sve obveze koje se odnose na namjenska sučelja iz članka 32.;

(b) koncipirano je i ispitano u skladu s člankom 30. stavkom 5. na zadovoljstvo pružatelja platnih usluga iz tog članka i stavka;

(c) pružatelji platnih usluga njime su se tijekom najmanje tri mjeseca u velikoj mjeri koristili za pružanje usluga pružanja informacija o računu, usluga iniciranja plaćanja i potvrđivanje raspoloživosti sredstava za kartična plaćanja;

(d) svi problemi povezani s namjenskim sučeljem riješeni su bez neopravdanog odgađanja.

7. Nadležna tijela opozivaju izuzeće iz stavka 6. ako pružatelji platnih usluga koji vode račune ne ispunjavaju uvjete iz točaka (a) i (d) dulje od dva uzastopna kalendarska tjedna. Nadležna tijela o tom opozivu obavješćuju EBA-u i osiguravaju da pružatelj platnih usluga koji vodi račun u najkraćem mogućem roku, a najkasnije u roku od dva mjeseca, uspostavi mehanizam za izvanredne situacije iz stavka 4.

Članak 34.

Certifikati

1. Za potrebe identifikacije iz članka 30. stavka 1. točke (a) pružatelji platnih usluga oslanjaju se na kvalificirane certifikate za elektroničke pečate iz članka 3. stavka 30. Uredbe (EU) br. 910/2014 ili za autentikaciju mrežnih stranica iz članka 3. stavka 39. te Uredbe.

2. Za potrebe ove Uredbe registracijski broj kako je navedeno u službenoj evidenciji u skladu s točkom (c) Priloga III. ili točkom (c) Priloga IV. Uredbi (EU) br. 910/2014 znači broj odobrenja pružatelja platnih usluga koji izdaje kartične platne instrumente, pružatelja usluga pružanja informacija o računu i pružatelja usluga iniciranja plaćanja, uključujući pružatelje platnih usluga koji vode račune koji pružaju takve usluge, dostupan u javnom registru države članice domaćina u skladu s člankom 14. Direktive (EU) 2015/2366 ili koji proizlazi iz obavijesti o svakom odobrenju izdanom na temelju članka 8. Direktive 2013/36/EU Europskog parlamenta i Vijeća ([1]) u skladu s člankom 20. te Direktive.

3. Za potrebe ove Uredbe kvalificirani certifikati za elektroničke pečate ili za autentifikaciju mrežnih stranica iz stavka 1. uključuju, na jeziku uobičajenom u području međunarodnih financija, dodatna posebna obilježja za svaku od sljedećih stavki:

(a) ulogu pružatelja platnih usluga, koji može imati jednu ili više od sljedećih uloga:

i. vođenje računa;

ii. iniciranje plaćanja;

iii. pružanje informacija o računu;

iv. izdavanje kartičnih platnih instrumenata;

(b) ime nadležnih tijela kod kojih je pružatelj platnih usluga registriran.

4. Obilježja iz stavka 3. ne utječu na interoperabilnost i priznavanje kvalificiranih certifikata za elektroničke pečate ili autentifikaciju mrežnih stranica.

([1]) Direktiva 2013/36/EU Europskog parlamenta i Vijeća od 26. lipnja 2013. o pristupanju djelatnosti kreditnih institucija i bonitetnom nadzoru nad kreditnim institucijama i investicijskim društvima, izmjeni Direktive 2002/87/EZ te stavljanju izvan snage direktiva 2006/48/EZ i 2006/49/EZ (SL L 176, 27.6.2013., str. 338.).

Članak 35.

Sigurnost komunikacijske sesije

1. Pružatelji platnih usluga koji vode račune, pružatelji platnih usluga koji izdaju kartične platne instrumente, pružatelji usluga pružanja informacija o računu i usluga iniciranja plaćanja osiguravaju da se pri internetskoj razmjeni podataka među stranama koje su uključene u komunikaciju tijekom cijele komunikacijske sesije primjenjuje sigurno šifriranje upotrebom općepriznatih tehnika šifriranja kako bi se zaštitila povjerljivost i cjelovitost podataka.

2. Pružatelji platnih usluga koji izdaju kartične platne instrumente, pružatelji usluga pružanja informacija o računu i pružatelji usluga iniciranja plaćanja u najvećoj mogućoj mjeri ograničavaju trajanje sesija pristupa koje nude pružatelji platnih usluga koji vode račune i aktivno prekidaju svaku takvu sesiju čim se tražena radnja dovrši.

3. U slučaju paralelnih mrežnih sesija s pružateljem platnih usluga koji vodi račun, pružatelji usluga pružanja informacija o računu i pružatelji usluga iniciranja plaćanja osiguravaju da su te sesije sigurno povezane s relevantnim sesijama uspostavljenima s korisnikom odnosno korisnicima platnih usluga kako bi se spriječila mogućnost pogrešnog usmjeravanja poruka ili informacija koje su razmijenjene tijekom komunikacije.

4. Pružatelji usluga pružanja informacija o računu, pružatelji usluga iniciranja plaćanja i pružatelji platnih usluga koji izdaju kartične platne instrumente s pružateljem platnih usluga koji vodi račun sadržavaju jedinstvena upućivanja na svaku od sljedećih stavki:

(a) korisnika ili korisnike platnih usluga i odgovarajuću komunikacijsku sesiju kako bi se razlikovali različiti zahtjevi istog korisnika platnih usluga odnosno istih korisnika platnih usluga;

(b) za usluge iniciranja plaćanja, jedinstveno identificiranu iniciranu platnu transakciju;

(c) za potvrdu raspoloživosti sredstava, jedinstveno identificirani zahtjev koji se odnosi na iznos potreban za izvršenje kartične platne transakcije.

5. Pružatelji platnih usluga koji vode račune, pružatelji usluga pružanja informacija o računu, pružatelji usluga iniciranja plaćanja i pružatelji platnih usluga koji izdaju kartične platne instrumente osiguravaju da u slučaju komuniciranja personaliziranih sigurnosnih podataka i autentifikacijskih kodova ti podaci i kodovi ne budu izravno ili neizravno čitljivi ijednom članu osoblja u ijednom trenutku.

U slučaju gubitka povjerljivosti personaliziranih sigurnosnih podataka koji su pod njihovom nadležnošću, ti pružatelji bez nepotrebnog odgađanja informiraju dotičnog korisnika platnih usluga i izdavatelja personaliziranih sigurnosnih podataka.

Članak 36.

Razmjene podataka

1. Pružatelji platnih usluga koji vode račune ispunjavaju svaki od sljedećih zahtjeva:

(a) pružateljima usluga pružanja informacija o računu pružaju iste informacije s utvrđenih računa za plaćanje i s njima povezanih platnih transakcija koje su stavljene na raspolaganje korisniku platnih usluga pri izravnom zahtjevu za pristup informacijama o računu, pod uvjetom da te informacije ne uključuju osjetljive podatke o plaćanju;

(b) odmah nakon primitka naloga za plaćanje pružateljima usluga iniciranja plaćanja pružaju iste informacije o iniciranju i izvršenju platne transakcije pružene ili stavljene na raspolaganje korisniku platnih usluga kada transakciju izravno inicira korisnik platnih usluga;

(c) na zahtjev pružatelja platnih usluga odmah u jednostavnom „da” ili „ne” formatu potvrđuju je li iznos potreban za izvršenje platne transakcije raspoloživ na platiteljevu računu za plaćanje.

2. U slučaju neočekivanog događaja ili pogreške nastalih tijekom postupka identifikacije, autentifikacije ili razmjene podatkovnih elemenata, pružatelj platnih usluga koji vodi račun šalje obavijest pružatelju usluga iniciranja plaćanja ili pružatelju usluga pružanja informacija o računu i pružatelju platnih usluga koji izdaje kartične platne instrumente s objašnjenjem uzroka neočekivanog događaja ili pogreške.

Ako pružatelj platnih usluga koji vodi račun osigurava namjensko sučelje u skladu s člankom 32., sučelje omogućuje generiranje obavijesti o neočekivanim događajima ili pogreškama koju pružatelj platnih usluga koji otkrije taj događaj ili pogrešku treba dostaviti drugim pružateljima platnih usluga koji sudjeluju u komunikacijskoj sesiji.

3. Pružatelji usluga pružanja informacija o računu raspolažu odgovarajućim i učinkovitim mehanizmima kojima se sprječava pristup informacijama osim informacijama s utvrđenih računa za plaćanje i s njima povezanih platnih transakcija, uz izričitu suglasnost korisnika.

4. Pružatelji usluga iniciranja plaćanja pružateljima platnih usluga koji vode račune pružaju iste informacije koje korisnik platnih usluga zatraži pri izravnom iniciranju platne transakcije.

5. Pružatelji usluga pružanja informacija o računu mogu za potrebe pružanja usluge pružanja informacija o računu u bilo kojoj od sljedećih situacija pristupiti informacijama s utvrđenih računa za plaćanje i s njima povezanih platnih transakcija koje drže pružatelji platnih usluga koji vode račune:

(a) kad god korisnik platnih usluga aktivno zahtijeva te informacije;

(b) ako korisnik platnih usluga ne zahtijeva aktivno te informacije, ne više od četiri puta tijekom 24 sata, osim ako veću učestalost ne dogovore pružatelj usluga pružanja informacija o računu i pružatelj platnih usluga koji vodi račun, uz izričitu suglasnost korisnika platnih usluga.

POGLAVLJE VI.

ZAVRŠNE ODREDBE

Članak 37.

Preispitivanje

Ne dovodeći u pitanje članak 98. stavak 5. Uredbe (EU) 2015/2366, EBA do 14. ožujka 2021. preispituje stope prijevare iz Priloga ovoj Uredbi i izuzeća odobrena na temelju članka 33. stavka 6. u vezi s namjenskim sučeljima i, prema potrebi, Komisiji podnosi nacrt njihova ažuriranja u skladu s člankom 10. Uredbe (EU) br. 1093/2010.

Članak 38.

Stupanje na snagu

1. Ova Uredba stupa na snagu sljedećeg dana od dana objave u *Službenom listu Europske unije*.

2. Ova Uredba primjenjuje se od 14. rujna 2019.

3. Međutim, članak 30. stavci 3. i 5. primjenjuju se 14. ožujka 2019.

Ova je Uredba u cijelosti obvezujuća i izravno se primjenjuje u svim državama članicama.

Sastavljeno u Bruxellesu 27. studenoga 2017.

Za Komisiju

Predsjednik

Jean-Claude JUNCKER

PRILOG

	Referentna stopa prijevara (%) za:	
Vrijednost praga izuzeća (ETV)	Elektronička plaćanja na temelju kartica s daljine	Elektronički kreditni transferi s udaljenosti
500 EUR	0,01	0,005
250 EUR	0,06	0,01
100 EUR	0,13	0,015