EBA/GL/2014/12

19. prosinca 2014.

Konačne smjernice

o sigurnosti internetskih plaćanja

Sadržaj

Smjernice o sigurnosti internetskih plaćanja

Status ovih Smjernica

Ovaj dokument sadrži smjernice objavljene u skladu s člankom 16. Uredbe (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 (Uredba o EBA-i). U skladu s člankom 16. stavkom 3. Uredbe o EBA-i nadležna tijela i financijske institucije moraju ulagati napore da se usklade s tim smjernicama.

Smjernice navode EBA-ino stajalište o odgovarajućim nadzornim praksama unutar Europskog sustava financijskog nadzora ili o tome kako bi se pravo Unije trebalo primjenjivati u određenom području. EBA stoga od svih nadležnih tijela i financijskih institucija kojima su smjernice upućene očekuje usklađenost s tim smjernicama. Nadležna tijela na koja se primjenjuju ove smjernice trebala bi se uskladiti uvodeći ih, kada je to moguće, u svoje nadzorne prakse (npr. izmjenom svojeg pravnog okvira ili postupaka nadzora), uključujući u slučaju kada su smjernice namijenjene prvenstveno institucijama.

Zahtjevi u pogledu izvješćivanja

U skladu s člankom 16. stavkom 3. Uredbe o EBA-i nadležna tijela moraju do 5. svibnja 2015. obavijestiti EBA-u o tome jesu li usklađena ili se namjeravaju uskladiti s ovim smjernicama ili, ako to nije slučaj, navesti razloge neusklađenosti. U slučaju neprimitka obavijesti unutar ovog roka EBA će smatrati da nadležna tijela nisu usklađena. Obavijesti se dostavljaju slanjem ispunjenog obrasca koji se nalazi u odjeljku 5. na adresu compliance@eba.europa.eu s naznakom „EBA/GL/2014/12”. Obavijesti šalju osobe nadležne za izvješćivanje o usklađenosti u ime svojih nadležnih tijela.

Obavijesti će biti objavljene na EBA-inoj internetskoj stranici u skladu s člankom 16. stavkom 3. Uredbe o EBA-i.

Glava I. – Područje primjene i definicije

Područje primjene

1. Ovim smjernicama utvrđuje se niz minimalnih zahtjeva u području sigurnosti internetskih plaćanja. Ove smjernice nadograđuju se na odredbe Direktive 2007/64/EZ[1] („Direktiva o platnim uslugama") o obvezama informiranja u vezi s platnim uslugama i obvezama pružatelja platnih usluga u vezi s pružanjem platnih usluga. Nadalje, u članku 10. stavku 4. Direktive od institucija za platni promet zahtijeva se uspostava robusnog sustava upravljanja i odgovarajući mehanizmi unutarnje kontrole.

2. Smjernice se primjenjuju na pružanje platnih usluga putem interneta od strane pružatelja platnih usluga koji su definirani u članku 1. Direktive.

3. Ove su smjernice upućene financijskim institucijama koje su definirane u članku 4. stavku 1. Uredbe (EU) br. 1093/2010 i nadležnim tijelima koja su definirana u članku 4. stavku 2. Uredbe (EU) br. 1093/2010. Nadležna tijela u 28 država članica Europske unije trebala bi osigurati primjenu ovih smjernica od strane pružatelja platnih usluga koji su definirani u članku 1. Direktive o platnim uslugama, pod njihovim nadzorom.

4. Osim toga, nadležna tijela mogu odlučiti zatražiti od pružatelja platnih usluga podnošenje izvještaja o usklađenosti s ovim smjernicama.

5. Ove smjernice ne utječu na valjanost „Preporuka za sigurnost internetskih plaćanja" („Izvještaj") Europske središnje banke.[2] Taj Izvještaj i dalje predstavlja dokument temeljem kojega bi središnje banke u svojoj funkciji nadzora platnih sustava i platnih instrumenata trebale procjenjivati usklađenost u pogledu sigurnosti internetskih plaćanja.

6. Smjernice predstavljaju minimalna očekivanja. One ne dovode u pitanje odgovornost pružatelja platnih usluga za praćenje i procjenu rizika prisutnih u njihovim platnim operacijama, za razvoj vlastitih detaljno razrađenih politika sigurnosti i provedbu odgovarajućih sigurnosnih mjera, postupanja u izvanrednim situacijama, upravljanja incidentima i mjera za održavanje kontinuiteta poslovanja koje su razmjerne rizicima prisutnima u platnim uslugama koje pružaju.

7. Svrha je ovih smjernica odrediti zajedničke minimalne zahtjeve za usluge internetskih plaćanja koje su navedene u nastavku, neovisno o upotrijebljenom uređaju za pristup:

[1] Direktiva 2007/64/EZ Europskog parlamenta i Vijeća od 13. studenoga 2007. o platnim uslugama na unutarnjem tržištu i o izmjeni direktiva 97/7/EZ, 2002/65/EZ, 2005/60/EZ i 2006/48/EZ te stavljanju izvan snage Direktive 97/5/EZ, SL L 319, 05.12.2007.

[2] http://www.ecb.europa.eu/press/pr/date/2013/html/pr130131_1.en.html

- [kartice] izvršenje kartičnih plaćanja na internetu, uključujući virtualna kartična plaćanja, kao i evidentiranje podataka kartičnog plaćanja za uporabu u „rješenjima novčanika" (engl. wallet solutions);

- [kreditni transferi] izvršenje kreditnih transfera na internetu;

- [e-ovlaštenje] izdavanje i izmjena elektroničkih ovlaštenja za izravno terećenje;

- [e-novac] transferi elektroničkog novca između dva računa elektroničkog novca putem interneta.

8. Ukoliko smjernice navode ishod, njega je moguće postići različitim načinima. Uz zahtjeve utvrđene u nastavku, ove smjernice daju i primjere najbolje prakse (u Prilogu 1.), za koje se pružateljima platnih usluga preporuča da ih slijede, iako ih se na to ne obvezuje.

9. Kada se platne usluge i platni instrumenti nude putem platne sheme (npr. sheme kartičnog plaćanja, sheme kreditnih transfera, sheme izravnih terećenja, itd.), nadležna tijela i relevantna središnja banka s nadzornom funkcijom za platne instrumente trebali bi se povezati kako bi osigurali da sudionici koji su odgovorni za funkcioniranje shema dosljedno primjenjuju smjernice.

10. Integratori plaćanja[3] koji nude usluge iniciranja plaćanja smatraju se ili prihvatiteljima usluga internetskog plaćanja (i slijedom toga pružateljima platnih usluga) ili vanjskim pružateljima tehničkih usluga relevantnim shemama ili pružateljima platnih usluga. U slučaju potonjih, integratore plaćanja potrebno je ugovorno obvezati da poštuju ove smjernice.

11. Područje primjene smjernica ne obuhvaća sljedeće:

- ostale internetske usluge koje pružaju pružatelji platnih usluga putem svoje internetske stranice za plaćanje (npr. e-brokerstvo, sklapanje ugovora elektroničkim putem);

- plaćanja za koje se instrukcija daje poštom, telefonskim nalogom, govornom poštom ili uporabom SMS tehnologije;

- mobilna plaćanja osim plaćanja putem *web* preglednika;

- kreditne transfere u slučajevima kada treća strana pristupa računu za plaćanje klijenta;

- platne transakcije koje poduzeća provode putem namjenskih mreža;

[3] Integratori plaćanja osiguravaju primatelju plaćanja (npr. e-trgovcu) stavljaju na raspolaganje standardizirano sučelje za iniciranje plaćanja pružatelja platnih usluga.

- kartična plaćanja uporabom anonimnih i nenadoplativih fizičkih ili virtualnih *prepaid* kartica kada ne postoji trajni odnos između izdavatelja i imatelja kartice;

- obračun i namira platnih transakcija.

Definicije

12. Za potrebe ovih smjernica, uz definicije navedene u Direktivi o platnim uslugama, primjenjuju se sljedeće definicije:

- *Autentifikacija* znači postupak kojim se pružatelju platnih usluga omogućava da provjeri identitet klijenta.

- *Pouzdana (stroga) autentifikacija klijenta* je, za potrebe ovih smjernica, postupak koji se temelji na uporabi dvaju ili više sljedećih elemenata koji ulaze u kategorije znanja, vlasništva i svojstvenosti: i) nešto što je poznato samo korisniku, npr. statična zaporka, šifra, PIN; ii) nešto što posjeduje samo korisnik, npr. token, pametna kartica, mobilni telefon; iii) nešto što korisnik jest, npr. biometrijska značajka, poput otiska prsta. Dodatno, odabrani elementi moraju biti međusobno neovisni u smislu da narušavanje jednog elementa ne umanjuje pouzdanost drugog odnosno drugih elemenata. Barem jedan od tih elementa ne bi smjelo biti moguće ponovno upotrijebiti ili reproducirati (osim u slučaju elemenata koji ulaze u kategoriju svojstvenosti) te ga ne bi smjelo biti moguće potajno ukrasti putem interneta. Postupak pouzdane autentifikacije trebao bi biti osmišljen na takav način da zaštiti povjerljivost autentifikacijskih podataka.

- *Autorizacija* znači postupak kojim se provjerava ima li klijent ili pružatelj platnih usluga pravo izvršiti određenu radnju, npr. pravo na prijenos sredstava, ili ima li pravo pristupa osjetljivim podacima.

- *Vjerodajnice* znače informacije – u pravilu povjerljive – koje daje klijent ili pružatelj platnih usluga za potrebe autentifikacije. Vjerodajnice mogu također označavati i posjed fizičkog alata koji sadrži informacije (npr. jednokratni generator zaporke, pametnu karticu) ili nešto što korisnik pamti ili posjeduje (poput biometrijske značajke).

- *Značajan incident vezan uz sigurnost plaćanja* znači incident koji ima ili može imati značajan učinak na sigurnost, cjelovitost ili kontinuitet rada platnih sustava pružatelja platnih usluga i/ili na sigurnost osjetljivih podataka o plaćanjima ili na novčana sredstava. Procjena materijalnosti trebala bi u obzir uzeti broj potencijalno pogođenih klijenata, rizični iznos i učinak na druge pružatelje platnih usluga ili na druge infrastrukture platnog prometa.

- *Analiza rizika transakcije* znači ocjena rizika povezanih uz određenu transakciju koja u obzir uzima kriterije poput, na primjer, karakteristike plaćanja klijenta odnosno obrasce ponašanja, vrijednost povezane transakcije, vrstu proizvoda i profil primatelja plaćanja.

- *Virtualne kartice* znači rješenje kartičnog plaćanja kod kojeg se generira alternativan, privremeni broj kartice sa skraćenim razdobljem valjanosti, ograničenom uporabom i unaprijed određenim limitom potrošnje koji se može upotrebljavati za kupnje putem interneta.

- *Rješenja novčanika* znači rješenja koja klijentu omogućuju da registrira podatke vezane uz jedan ili više platnih instrumenata u svrhu izvršenja plaćanja s nekoliko e-trgovaca.

Glava II. - Smjernice o sigurnosti internetskih plaćanja

Opća kontrola i sigurnosno okruženje

Upravljanje

1. Pružatelji platnih usluga trebali bi implementirati i redovito revidirati politiku sigurnosti za usluge internetskog plaćanja.

   1.1 Politiku sigurnosti potrebno je primjereno dokumentirati i redovito revidirati (u skladu sa smjernicom 2.4.) te bi je trebalo odobriti više rukovodstvo. Politika sigurnosti trebala bi odrediti sigurnosne ciljeve i sklonost preuzimanju rizika.

   1.2 Politika sigurnosti trebala bi odrediti uloge i odgovornosti, uključujući funkciju upravljanja rizicima s izravnom linijom izvješćivanja uprave, te linije izvješćivanja za pružene usluge internetskih plaćanja, uključujući upravljanje osjetljivim podacima o plaćanjima u vezi s procjenom, kontrolom i ovladavanjem rizikom.

Procjena rizika

2. Pružatelji platnih usluga trebali bi provoditi i dokumentirati temeljite procjene rizika u pogledu sigurnosti internetskih plaćanja i povezanih usluga, kako prije uvođenja usluge odnosno usluga tako i redovito nakon toga.

   2.1 Kroz svoju funkciju upravljanja rizicima, pružatelji platnih usluga trebali bi provoditi i dokumentirati detaljne procjene rizika u pogledu internetskih plaćanja i povezanih usluga. Pružatelji platnih usluga trebali bi razmotriti rezultate kontinuiranog praćenja sigurnosnih prijetnji vezanih uz usluge internetskog plaćanja koje nude ili planiraju nuditi, pritom uzimajući u obzir: i) tehnološka rješenja koja upotrebljavaju, ii) usluge koje su eksternalizirane vanjskim pružateljima usluga te iii) tehničko okruženje klijenata. Pružatelji platnih usluga trebali bi razmotriti rizike povezane s odabranim tehnološkim platformama, aplikacijskom arhitekturom, tehnikama programiranja i praksama kako na svojoj strani[4] tako i na strani svojih klijenata,[5] kao i rezultate procesa praćenja sigurnosnih incidenata (vidi smjernicu 3.).

   2.2 Na temelju navedenog, pružatelji platnih usluga trebali bi odrediti jesu li, i u kojoj mjeri, potrebne izmjene postojećih sigurnosnih mjera, upotrijebljenih tehnologija i postupaka ili ponuđenih usluga. Pružatelji platnih usluga trebali bi u obzir uzeti vrijeme koje je potrebno za provedbu izmjena (uključujući vrijeme potrebno da klijent provede promjenu) i poduzeti primjerene privremene mjere kako bi minimizirali sigurnosne incidente i prijevare, kao i moguće remeteće učinke.

[4] Poput podložnosti sustava otimanju platnih sesija, SQL injektiranju, XSS napadima, *buffer overflow* napadima itd.

[5] Poput rizika povezanih s uporabom multimedijalnih aplikacija, dodataka preglednicima, okvira, vanjskih poveznica itd.

2.3 Procjena rizika trebala bi adresirati potrebu zaštite osjetljivih podataka o plaćanjima.

2.4 Pružatelji platnih usluga trebali bi preispitati scenarije rizika i postojeće sigurnosne mjere nakon značajnih incidenata koji utječu na njihove usluge, prije značajnih izmjena infrastrukture ili postupaka te nakon utvrđivanja novih prijetnji putem aktivnosti praćenja rizika. Dodatno, općenito preispitivanje procjene rizika trebalo bi se provoditi barem jednom godišnje. Rezultate procjena rizika i kontrole procjene rizika trebalo bi podnijeti višem rukovodstvu na odobrenje.

Nadziranje i izvješćivanje o incidentima

3. Pružatelji platnih usluga trebali bi osigurati dosljedno i cjelovito nadziranje, rješavanje i naknadno praćenje (engl. *follow-up*) sigurnosnih incidenata, uključujući prigovore klijenata vezane uz sigurnost. Pružatelji platnih usluga trebali bi uspostaviti postupak za izvješćivanje rukovodstva o takvim incidentima i, u slučaju značajnih sigurnosnih incidenata vezanih uz plaćanje, nadležnih tijela.

3.1 Pružatelji platnih usluga trebali bi uspostaviti proces za nadziranje, rješavanje i naknadno praćenje sigurnosnih incidenata i pritužbi klijenata vezanih uz sigurnost te za izvješćivanje rukovodstva o takvim incidentima.

3.2 Pružatelji platnih usluga trebaju uspostaviti postupak za trenutno obavješćivanje nadležnih tijela (tj. nadzornih tijela i tijela za zaštitu podataka), ukoliko takva postoje, u slučaju značajnih sigurnosnih incidenata vezanih uz pružene platne usluge.

3.3 Pružatelji platnih usluga trebali bi uspostaviti postupak za suradnju s nadležnim tijelima odgovornim za provođenje zakona na značajnim sigurnosnim incidentima vezanim uz plaćanja, uključujući povredu sigurnosti podataka.

3.4 Pružatelji platnih usluga - prihvatitelji trebali bi od e-trgovaca koji pohranjuju, obrađuju ili prenose osjetljive podatke o plaćanju ugovorom zahtijevati suradnju na značajnim sigurnosnim incidentima vezanim uz plaćanja, uključujući povrede podataka, i s njima i s nadležnim tijelima odgovornim za provođenje zakona. Ako pružatelj platnih usluga sazna da određeni e-trgovac ne surađuje sukladno ugovoru, pružatelj platnih usluga trebao bi poduzeti mjere za provedbu ove ugovorne obveze ili raskinuti ugovor.

Kontrola i ovladavanje rizikom

4. Kako bi ovladali utvrđenim rizicima, pružatelji platnih usluga trebali bi implementirati sigurnosne mjere u skladu s politikama sigurnosti. Ove bi mjere trebale obuhvaćati više slojeva (razina) sigurnosnih zaštita, gdje neučinkovitost jedne razine zaštite nadoknađuje sljedeća razina (višeslojna zaštita, odnosno „dubinska obrana").

4.1 U osmišljavanju, razvoju i održavanju usluga internetskih plaćanja, pružatelji platnih usluga trebali bi obratiti posebnu pozornost na primjereno razdvajanje dužnosti u

okruženjima informacijske tehnologije (npr. razvojnom, testnom i produkcijskom okruženju) i na odgovarajuću provedbu načela najmanjih ovlasti kao osnove za pouzdano upravljanje identitetom i pristupom.[6]

4.2 Pružatelji platnih usluga trebali bi postaviti primjerena sigurnosna rješenja u svrhu zaštite mreža, internetskih stranica, poslužitelja i komunikacijskih veza od zlouporabe ili napada. Pružatelji platnih usluga trebali bi sa svih poslužitelja ukloniti sve suvišne funkcije kako bi zaštitili (učvrstili) i uklonili ili smanjili ranjivosti rizičnih aplikacija. Pristup raznih aplikacija potrebnim podacima ili resursima trebao bi se ograničiti na strogi minimum uz primjenu načela najmanjih ovlasti. Kako bi se ograničila uporaba „lažnih" internetskih stranica (koje oponašaju legitimne internetske stranice pružatelja platnih usluga), transakcijske internetske stranice koje nude usluge internetskih plaćanja trebalo bi identificirati certifikatima proširene provjere valjanosti izrađenih u ime pružatelja platnih usluga ili drugim sličnim metodama autentifikacije.

4.3 Pružatelji platnih usluga trebali bi uspostaviti primjerene procese za nadziranje, bilježenje i ograničenje pristupa: i) osjetljivim podacima o plaćanjima te ii) logičkim i fizičkim kritičnim resursima, poput mreža, sustava, baza podataka, sigurnosnih modula, itd. Pružatelji platnih usluga trebali bi izraditi, pohraniti i analizirati odgovarajuće zapise i revizijske tragove.

4.4 U osmišljavanju[7], razvoju i održavanju usluga internetskih plaćanja, pružatelji platnih usluga trebali bi osigurati da minimizacija podataka[8] predstavlja ključni element osnovne funkcionalnosti: sakupljanja, usmjeravanja, obrade, pohrane i/ili arhiviranja; vizualizacija osjetljivih podataka o plaćanju bi također trebala biti na apsolutno minimalnoj razini.

4.5 Sigurnosne mjere za usluge internetskih plaćanja trebalo bi testirati pod nadzorom funkcije upravljanja rizicima kako bi se osigurala njihova robusnost i učinkovitost. Sve bi promjene trebalo podvrgnuti formalnom procesu upravljanja promjenama kojim se osigurava primjereno planiranje, testiranje, dokumentiranje i odobrenje promjena. Na temelju provedenih promjena i zapaženih sigurnosnih prijetnji, testove je potrebno redovito ponavljati i uključiti scenarije relevantnih i poznatih potencijalnih napada.

4.6 Sigurnosne mjere pružatelja platnih usluga za usluge internetskih plaćanja trebalo bi periodično revidirati kako bi se osigurala njihova robusnost i učinkovitost. Trebalo bi također revidirati implementaciju i funkcioniranje usluga internetskih plaćanja. Pri utvrđivanju dinamike i fokusa takvih revizija trebalo bi uzeti u obzir prisutne

[6] „Svaki program i svaki povlašteni korisnik sustava trebali bi raditi uz najmanju razinu ovlasti koja je potrebna kako bi se posao obavio." Vidi Saltzer, J. H. (1974.), „Protection and the Control of Information Sharing in Multics", Communications of the ACM, sv. 17, br. 7, str. 388.

[7] Privatnost kroz kreiranje.

[8] Minimizacija podataka odnosi se na politiku prikupljanja što je moguće manje osobnih podataka koji su nužni za provedbu određene funkcije.

sigurnosne rizike, s kojima trebaju biti razmjerni. Revizije bi trebali provoditi pouzdani i neovisni (unutarnji ili vanjski) stručnjaci. Oni ne bi trebali biti uključeni na bilo koji način u razvoj, provedbu ili operativno upravljanje pruženim uslugama internetskog plaćanja.

4.7 Kada god pružatelji platnih usluga eksternaliziraju funkcije vezane uz sigurnost usluga internetskog plaćanja, ugovor bi trebao uključivati odredbe koje zahtijevaju usklađenost s načelima i smjernicama koje su utvrđene ovim smjernicama.

4.8 Pružatelji platnih usluga koji nude usluge prihvata trebali bi e-trgovce koji rukuju s osjetljivim podacima o plaćanjima (tj. pohranjuju ih, obrađuju ili prenose) ugovorom obvezati na primjenu sigurnosnih mjera u svojim IT infrastrukturama, u skladu sa smjernicama 4.1. do 4.7., kako bi se izbjegla krađa tih osjetljivih podataka kroz njihove sustave. Ako pružatelj platnih usluga sazna da određeni e-trgovac nije uspostavio potrebne sigurnosne mjere, pružatelj platnih usluga trebao bi poduzeti korake za provedbu ove ugovorne obveze ili raskinuti ugovor.

Sljedivost

5. Pružatelji platnih usluga trebali bi uspostaviti procese kojima se osigurava sljedivost svih transakcija, kao i tijek procesa zadavanja e-ovlaštenja.

5.1 Pružatelji platnih usluga trebali bi osigurati da njihova usluga obuhvaća sigurnosne mehanizme za detaljno bilježenje transakcija i podataka o e-ovlaštenjima, uključujući redni broj transakcije, vremensku oznaku nastanka transakcijskih podataka, promjene parametara, kao i pristup podacima o transakcijama i e-ovlaštenjima.

5.2 Pružatelji platnih usluga trebali bi osigurati izradu datoteka sa zapisima koje omogućavaju praćenje bilo kakvog dodavanja, izmjene ili brisanja podataka o transakcijama i e-ovlaštenjima.

5.3 Pružatelji platnih usluga trebali bi pretraživati i analizirati podatke o transakcijama i e-ovlaštenjima i osigurati da imaju alate za procjenu datoteka sa zapisima. Te bi aplikacije trebale biti dostupne jedino ovlaštenom osoblju.

Posebna kontrola i sigurnosne mjere za internetska plaćanja

Početna identifikacija klijenta, informacija

6. Klijenti se trebaju ispravno identificirati, u skladu s europskim zakonodavstvom o sprečavanju pranja novca[9] te trebaju potvrditi spremnost za korištenje internetskih plaćanja uporabom

[9] Primjerice, Direktiva 2005/60/EZ Europskog parlamenta i Vijeća od 26. listopada 2005. o sprečavanju korištenja financijskog sustava u svrhu pranja novca i financiranja terorizma. SL L 309, 25.11.2005., str. 15.-36. Vidi također Direktivu Komisije 2006/70/EZ od 1. kolovoza 2006. o utvrđivanju provedbenih mjera za Direktivu 2005/60/EZ Europskog parlamenta i Vijeća u vezi s definicijom „politički izložene osobe" i tehničkim kriterijima za postupke

odnosnih usluga prije nego im se dozvoli pristup tim uslugama. Pružatelji platnih usluga trebali bi klijentu pružiti odgovarajuće „prethodne", „redovne" ili, po potrebi, „*ad hoc*" informacije o potrebnim zahtjevima (npr. opremi, postupcima) za provedbu sigurnih transakcija internetskog plaćanja i pripadajućim rizicima.

6.1 Pružatelji platnih usluga trebali bi osigurati da je klijent podvrgnut postupcima dubinskog ispitivanja i da je dostavio odgovarajuće identifikacijske isprave[10] kao i povezane informacije prije omogućavanja pristupa uslugama internetskog plaćanja.[11]

6.2 Pružatelji platnih usluga trebali bi osigurati da prethodne informacije [12] koje se pružaju klijentu sadrže detalje o uslugama internetskog plaćanja. One bi trebale obuhvaćati, po potrebi:

- jasne informacije o svim zahtjevima u pogledu opreme klijenta, softvera ili drugih potrebnih alata (npr. antivirusni softver, vatrozid);
- smjernice za ispravnu i sigurnu uporabu personaliziranih sigurnosnih vjerodajnica;
- detaljan (korak po korak) opis postupka kojeg klijent treba slijediti za podnošenje naloga za plaćanje i autoriziranje platne transakcije i/ili dobivanje informacija, uključujući posljedice svake radnje;
- smjernice za primjerenu i sigurnu uporabu svog hardvera i softvera koji je dana klijentu dana na korištenje;
- postupke koje je potrebno slijediti u slučaju gubitka ili krađe personaliziranih sigurnosnih vjerodajnica ili hardvera i softvera klijenta za prijavu na sustav ili provođenje transakcija;
- postupke koje je potrebno slijediti u slučaju otkrivene zlouporabe ili sumnje na zlouporabu;
- opis pojedinačnih odgovornosti i obveza pružatelja platnih usluga i klijenta u pogledu korištenja usluge internetskog plaćanja.

pojednostavljene temeljite identifikacije stranaka i za oslobođenje na temelju financijske djelatnosti koja se provodila povremeno ili u vrlo ograničenom opsegu. SL L 214, 4.8.2006., str. 29.-34.

[10] Primjerice putovnicu, osobnu iskaznicu ili napredni elektronički potpis.

[11] Postupak utvrđivanja identiteta korisnika ne dovodi u pitanje nijednu iznimku predviđenu zakonodavstvom o sprječavanju pranja novca. Pružatelji platnih usluga ne trebaju provesti zaseban postupak utvrđivanja identiteta korisnika za usluge internetskog plaćanja, pod uvjetom da je takvo utvrđivanja identiteta korisnika već provedeno, primjerice za druge postojeće usluge vezane uz plaćanje ili za otvaranje računa.

[12] Te informacije upotpunjuju članak 42. Direktive o platnim uslugama u kojem su navode informacije koje pružatelj platnih usluga mora pružiti korisniku platne usluge prije sklapanja ugovora o pružanju platnih usluga.

6.3 Pružatelji platnih usluga trebali bi osigurati da u okvirnom ugovoru sklopljenom s klijentom stoji da pružatelj platnih usluga može blokirati određenu transakciju ili platni instrument[13] na temelju sigurnosnih razloga. U ugovoru bi trebala biti navedena metoda i uvjeti obavješćivanja klijenta te način stupanja u kontakt s pružateljem platnih usluga u svrhu deblokiranja transakcije internetskog plaćanja ili usluge, u skladu s Direktivom o platnim uslugama.

Pouzdana (stroga) autentifikacija klijenta

7. Iniciranje internetskih plaćanja, kao i pristup osjetljivim podacima o plaćanju, trebalo bi biti zaštićeno pouzdanom autentifikacijom klijenta. Pružatelji platnih usluga trebali bi imati postupak pouzdane autentifikacije klijenta u skladu s definicijom iz ovih smjernica.

7.1 [kreditni transfer/e-ovlaštenje/elektronički novac] Pružatelji platnih usluga trebali bi provesti pouzdanu autentifikaciju klijenta u svrhu provjere autorizacije transakcija internetskog plaćanja (uključujući skupne kreditne transfere) i izdavanje ili izmjenu elektroničkih ovlaštenja za izravno terećenje. Ipak, pružatelji platnih usluga trebaju razmotriti usvajanje alternativnih mjera autentifikacije klijenta u slučaju:

- isplata pouzdanim korisnicima koji su uključeni u prethodno formirane bijele liste za tog klijenta;
- transakcija između dva računa istog klijenta kod istog pružatelja platnih usluga;
- prijenosa unutar istog pružatelja platnih usluga opravdanih analizom rizika transakcije;
- plaćanja malih vrijednosti, kako je navedeno u Direktivi o platnim uslugama.[14]

7.2 Dobivanje pristupa ili izmjena osjetljivih podataka o plaćanjima (uključujući izradu i izmjenu bijelih lista) zahtijeva pouzdanu autentifikaciju klijenta. Kada pružatelj platnih usluga nudi isključivo usluge savjetovanja, bez prikaza osjetljivih podataka o klijentu ili plaćanjima, poput podataka o platnim karticama koje je moguće lako zlouporabiti kako bi se počinila prijevara, pružatelj platnih usluga može prilagoditi svoje zahtjeve uvjete za autentifikaciju na temelju svoje procjene rizika.

7.3 [kartice] U pogledu kartičnih transakcija, svi pružatelji platnih usluga koji izdaju kartice trebali bi podržavati pouzdanu autentifikaciju imatelja kartice. Sve izdane kartice moraju biti tehnički spremne (registrirane) za uporabu uz pouzdanu autentifikaciju.

[13] Vidi članak 55. Direktive o platnim uslugama o ograničenjima korištenja platnih instrumenta.

[14] Vidi definiciju platnih instrumenata male vrijednosti u članku 34. stavku 1. i članku 53. stavku 1. Direktive o platnim uslugama.

7.4 [kartice] Pružatelji platnih usluga koji nude usluge prihvata trebali bi podržavati tehnologije koje izdavatelju omogućuju provođenje pouzdane autentifikacije imatelja kartice za sheme kartičnog plaćanja u kojima prihvatitelj sudjeluje.

7.5 [kartice] Pružatelji platnih usluga koji nude usluge prihvata trebali bi od svog e-trgovca zahtijevati da podržava tehnologije koje izdavatelju omogućuju provođenje pouzdane autentifikacije imatelja kartice za kartične transakcije putem interneta. Upotreba alternativnih mjera autentifikacije može se razmotriti za unaprijed definirane kategorije transakcija niskog rizika, npr. na temelju analize rizika transakcije, ili za plaćanja malih vrijednosti, kako je navedeno u Direktivi o platnim uslugama.

7.6 [kartice] Za sheme kartičnih plaćanja koje usluga prihvaća, pružatelji rješenja novčanika trebali bi zahtijevati pouzdanu autentifikaciju od strane izdavatelja prilikom prve registracije podataka o kartici od strane legitimnog imatelja.

7.7 Pružatelji rješenja novčanika trebali bi podržavati pouzdanu autentifikaciju klijenta pri prijavi klijenata u platne usluge ili izvršenju kartičnih transakcija putem interneta. Upotreba alternativnih mjera autentifikacije može se razmotriti za unaprijed definirane kategorije transakcija niskog rizika, npr. na temelju analize rizika transakcije, ili za plaćanja malih vrijednosti, kako je navedeno u Direktivi o platnim uslugama.

7.8 [kartice] Početna registracija za virtualne kartice trebala bi se odvijati u sigurnom i pouzdanom okruženju.[15] Pouzdanu autentifikaciju klijenta trebalo bi zahtijevati u slučaju procesa generiranja podataka o virtualnim karticama ako se kartica izdaje u internetskom okruženju.

7.9 Pri komunikaciji s e-trgovcima pružatelji platnih usluga trebali bi osigurati odgovarajuću uzajamnu autentifikaciju u svrhu iniciranja internetskih plaćanja i pristupa osjetljivim podacima o plaćanjima.

Prijava za i osiguravanje alata za autentifikaciju i/ili softvera koji se dostavlja klijentu

8. Pružatelji platnih usluga trebali bi osigurati da se prijava klijenta te početno stavljanje na raspolaganje alata za autentifikaciju koji su potrebni za uporabu usluge internetskog plaćanja i/ili dostava softvera za plaćanje odvijaju na siguran način.

8.1 Prijava za i stavljanje na raspolaganje alata za autentifikaciju i/ili softvera za plaćanje koja se dostavlja klijentu trebali bi zadovoljiti sljedeće zahtjeve.

[15] Okruženja koja su odgovornost pružatelja platnih usluga, u kojima je osigurana primjerena autentifikacija korisnika i pružatelja platnih usluga koji nudi uslugu, kao i zaštita povjerljivih/osjetljivih podataka uključuju: i) prostorije pružatelja platnih usluga; ii) internetsko bankarstvo ili drugu sigurnu internetsku stranicu, npr. gdje GA nudi slične sigurnosne značajke, između ostalog, kako je definirano u smjernici 4.; ili iii) usluge bankomata. (U slučaju bankomata, zahtijeva se pouzdana autentifikacija. Takva autentifikacija najčešće uključuje čip i PIN ili čip i biometrijske značajke).

- Povezane postupke trebalo bi provesti u sigurnom i pouzdanom okruženju pritom uzimajući u obzir moguće rizike koji proizlaze iz uređaja koje ne kontrolira pružatelj platnih usluga.

- Trebalo bi uspostaviti učinkovite i sigurne postupke za dostavu personaliziranih sigurnosnih vjerodajnica, softvera za plaćanje i svih personaliziranih uređaja vezanih za internetska plaćanja. Softver koji se dostavlja putem interneta trebao bi biti digitalno potpisan od pružatelja platnih usluga kako bi se klijentu omogućilo da provjeri njegovu autentičnost te je li došlo do neovlaštene izmjene.

- [kartice] Vezano uz kartične transakcije, klijent bi trebao imati mogućnost prijave za pouzdanu autentifikaciju, neovisno o određenoj kupnji putem interneta. U slučaju kada se nudi aktivacija tijekom *on-line* kupnje, ovo bi se trebalo učiniti na način da se klijenta preusmjeri u sigurno i pouzdano okruženje.

8.2 [kartice] Izdavatelji bi trebali aktivno poticati imatelje kartica na prijavu za pouzdanu autentifikaciju i dopustiti svojim imateljima kartica izbjegavanje navedene prijave samo iznimno i u ograničenom broju slučajeva kada to opravdava rizik vezan uz određenu kartičnu transakciju.

Pokušaji prijave na sustav, vremensko ograničenje sesije, valjanost autentifikacije

9. Pružatelji platnih usluga trebali bi ograničiti broj pokušaja prijave na sustav ili autentifikacije, za usluge internetskog plaćanja utvrditi pravila „vremenskog ograničenja" sesije i odrediti vremenska ograničenja za valjanost autentifikacije.

9.1 Kada se za potrebe autentifikacije upotrebljava jednokratna zaporka (OTP), pružatelji platnih usluga trebali bi osigurati da razdoblje valjanosti takvih zaporka bude ograničeno na strogo nužan minimum.

9.2 Pružatelji platnih usluga trebali bi utvrditi maksimalan broj neuspjelih pokušaja prijave ili autentifikacije nakon kojeg se pristup usluzi internetskog plaćanja (privremeno ili trajno) blokira. Pružatelji platnih usluga trebali bi uspostaviti siguran postupak za reaktivaciju blokiranih usluga internetskog plaćanja.

9.3 Pružatelji platnih usluga trebali bi odrediti maksimalno razdoblje nakon kojeg neaktivne usluge internetskog plaćanja automatski završavaju.

Praćenje transakcija

10. Mehanizmi praćenja transakcija koji su osmišljeni za sprječavanje, otkrivanje i blokiranje prijevarnih platnih transakcija trebali bi biti aktivirani prije konačne autorizacije od pružatelja platnih usluga; sumnjive ili visokorizične transakcije trebale bi biti podvrgnute posebnom postupku ispitivanja i procjene. Usporedivi mehanizmi za praćenje sigurnosti i autorizaciju bi se trebali uspostaviti i za izdavanje e-ovlaštenja.

10.1 Prije nego što konačno autoriziraju transakcije ili e-ovlaštenje, pružatelji platnih usluga trebali bi se koristiti sustavima za otkrivanje i sprječavanje prijevara u svrhu utvrđivanja sumnjivih transakcija. Takvi bi se sustavi trebali zasnivati, na primjer, na parametriziranim pravilima (poput crnih lista zlouporabljenih ili ukradenih kartičnih podataka) i trebali bi pratiti neuobičajene obrasce ponašanja klijenta ili njegovog uređaja za pristup (poput izmjene IP adrese[16] ili IP raspona tijekom sesije usluga internetskog plaćanja, ponekad utvrđenom provjerama IP geolokacije,[17] atipičnim kategorijama e-trgovaca za određenog klijenta ili neuobičajenim podacima o transakcijama itd.). Takvi bi sustavi također trebali moći otkriti znakove zaraze zlonamjernim softverom u sesiji (npr. skriptna naspram ljudske validacije) i poznate scenarije prijevare. Opseg, složenost i prilagodljivost rješenja za praćenje, uz poštivanje relevantnog zakonodavstva o zaštiti podataka, trebali bi biti razmjerni ishodu procjene rizika.

10.2 Pružatelji platnih usluga - prihvatitelji trebali bi imati sustave otkrivanja i sprječavanja prijevara kako bi pratili aktivnosti e-trgovaca.

10.3 Pružatelji platnih usluga trebali bi provoditi postupke kontrole i procjene transakcija unutar primjerenog razdoblja kako ne bi neopravdano odgodili iniciranje i/ili izvršenje dotične platne usluge.

10.4 Ukoliko pružatelj platnih usluga, u skladu sa svojom politikom rizika, odluči blokirati platnu transakciju koja je bila identificirana kao potencijalno prijevarna, pružatelj platnih usluga trebao bi blokadu ostaviti što je kraće moguće dok se ne razriješe sigurnosna pitanja.

Zaštita osjetljivih podataka o plaćanjima

11. Osjetljive podatke o plaćanjima trebalo bi zaštititi prilikom pohrane, obrade ili prijenosa.

11.1 Sve podatke koji se upotrebljavaju za utvrđivanje identiteta i autentifikaciju klijenata (npr. pri prijavi, iniciranju internetskih plaćanja te pri zadavanju, izmjeni ili otkazivanju e-ovlaštenja), kao i na sučelju klijenta (internetske stranice pružatelja platnih usluga ili e-trgovca), potrebno je primjereno osigurati od krađe i neovlaštenog pristupa ili izmjene.

11.2 Pružatelji platnih usluga trebali bi osigurati da se pri razmjeni osjetljivih podataka o plaćanju putem interneta primjenjuje sigurno šifriranje cjelokupnog prijenosnog puta (*end-to-end*)[18] između strana koje komuniciraju, za cijelo vrijeme sesije, u svrhu zaštite

[16] IP adresa je jedinstveni numerički kôd kojim se identificira svako računalo spojeno na internet.

[17] „Geo-IP" provjera utvrđuje je li država izdavanja sukladna IP adresi s koje korisnik inicira transakciju.

[18] *End-to-end* šifriranje odnosi se na šifriranje unutar ili na izvorišnom sustavu, uz odgovarajuće dešifriranje tek unutar ili na odredišnom sustavu. ETSI EN 302 109 V1.1.1. (2003-06).

povjerljivosti i cjelovitosti podataka, koristeći se snažnim i široko poznatim tehnikama šifriranja.

11.3 Pružatelji platnih usluga koji nude usluge prihvata trebali bi poticati svoje e-trgovce da ne pohranjuju osjetljive podatke o plaćanjima. U slučaju da e-trgovci rukuju osjetljivim podacima o plaćanjima, odnosno pohranjuju ih, obrađuju ili prenose, ti pružatelji platnih usluga trebali bi ugovorom zahtijevati od e-trgovaca uspostavu potrebnih mjera za zaštitu ovih podataka. Pružatelji platnih usluga trebali bi provoditi redovite provjere, te ako pružatelj platnih usluga sazna da određeni e-trgovac koji rukuje osjetljivim podacima o plaćanjima nije uspostavio potrebne sigurnosne mjere, pružatelj platnih usluga trebao bi poduzeti mjere za provedbu ove ugovorne obveze ili raskinuti ugovor.

Podizanje svijesti klijenata, edukacija i komunikacija

Edukacija klijenata i komunikacija

12. Po potrebi, pružatelji platnih usluga trebali bi pružiti pomoć i savjete klijentima u pogledu sigurne uporabe internetskih plaćanja i platnih usluga. Pružatelji platnih usluga trebali bi sa svojim klijentima komunicirati na takav način da ih uvjere u autentičnost primljenih poruka.

12.1 Pružatelji platnih usluga trebali bi omogućiti barem jedan siguran kanal [19] za kontinuiranu komunikaciju s klijentima o ispravnom i sigurnom korištenju internetskih plaćanja. Pružatelji platnih usluga trebali bi obavijestiti klijente o tom kanalu i objasniti da bilo koja poruka poslana u ime pružatelja platnih usluga bilo kojim drugim sredstvom, poput elektroničke pošte, a koja se tiče ispravne i sigurne uporabe usluga internetskog plaćanja, nije pouzdana. Pružatelj platnih usluga trebao bi objasniti:

- postupak kojim klijenti pružatelju platnih usluga prijavljuju (sumnju na) prijevarna plaćanja, sumnjive incidente ili anomalije tijekom sesije usluga internetskog plaćanja i/ili moguće pokušaje socijalnog inženjeringa[20];
- sljedeće korake odnosno kako će pružatelj platnih usluga odgovoriti klijentu;
- kako će pružatelj platnih usluga obavijestiti klijenta o (potencijalnim) prijevarnim transakcijama ili njihovom neiniciranju ili upozoriti klijenta o napadima (npr. prijevarnim *phishing* porukama elektroničke pošte).

12.2 Putem sigurnog kanala, pružatelji platnih usluga trebali bi klijente obavještavati o ažuriranjima sigurnosnih postupaka u vezi s uslugama internetskog plaćanja. Sva upozorenja o značajnim nadolazećim rizicima (npr. upozorenja o socijalnom inženjeringu) također bi trebalo dostavljati putem sigurnog kanala.

12.3 Pružatelji platnih usluga trebali bi osigurati pomoć klijentima u vezi svih pitanja, prigovora, zahtjeva za podrškom i prijavama anomalija ili incidenata koji se odnose na internetska plaćanja i povezane usluge te bi klijenti trebali biti primjereno obaviješteni kako takvu pomoć mogu dobiti.

12.4 Pružatelji platnih usluga trebali bi inicirati programe edukacije i podizanja svijesti klijenata čija je svrha osigurati razumijevanje klijenata barem o potrebi:

- zaštite svojih zaporka, sigurnosnih tokena, osobnih podataka i drugih povjerljivih podataka;

[19] Poput namjenskog poštanskog pretinca na internetskoj stranici pružatelja platnih usluga ili sigurnoj internetskoj stranici.

[20] Socijalni inženjering u ovom kontekstu znači tehnike manipuliranja ljudima u svrhu dobivanja informacija (npr. putem elektroničke pošte ili telefonskih razgovora), ili prikupljanje podataka s društvenih mreža, u svrhu stjecanja neovlaštenog pristupa računalu ili mreži.

- primjerenog upravljanja sigurnošću osobnih uređaja (npr. računala) instaliranjem i ažuriranjem sigurnosnih komponenti (antivirusa, vatrozida, sigurnosnih zakrpi);

- razmatranja značajnih prijetnji i rizika povezanih s preuzimanjem softvera s interneta ako klijent ne može biti dovoljno siguran da se radi o izvornom softveru koji nije neovlašteno mijenjan;

- uporabe izvornih internetskih stranica pružatelja platnih usluga za internetska plaćanja.

12.5 Pružatelji platnih usluga - prihvatitelji trebali bi od e-trgovaca zatražiti da iz e-trgovine jasno izdvoje procese vezane uz plaćanje kako bi olakšali klijentima olakšali utvrđivanje kada komuniciraju s pružateljem platnih usluga, a ne s primateljem plaćanja (npr. preusmjeravanjem klijenta i otvaranjem posebnog prozora tako da proces plaćanja nije vidljiv unutar okvira e-trgovine).

Obavijesti, određivanje limita

13. Pružatelji platnih usluga trebaju odrediti limite za usluge internetskog plaćanja te mogu svojim klijentima dati mogućnosti daljnjeg ograničenja rizika unutar tih limita. Također mogu pružiti usluge upozoravanja i upravljanja profilom klijenta.

13.1 Prije pružanja usluga internetskih plaćanja klijentu, pružatelji platnih usluga trebali bi odrediti limite[21] koji se primjenjuju na te usluge, (npr. maksimalan iznos svakog pojedinačnog plaćanja ili ukupan iznos tijekom određenog razdoblja) i trebali bi o tomu obavijestiti svoje klijente. Pružatelji platnih usluga trebali bi klijentima omogućiti da isključe funkciju internetskog plaćanja.

Pristup klijenta informacijama o statusu iniciranja i izvršenja plaćanja

14. Pružatelji platnih usluga trebali bi svojim klijentima potvrditi iniciranje plaćanja i pravovremeno im dostaviti informacije radi provjere je li platna transakcija ispravno inicirana i/ili izvršena.

14.1 [kreditni transfer/e-ovlaštenje] Pružatelji platnih usluga trebali bi klijentima omogućiti da u gotovo realnom vremenu provjere status izvršenja transakcija kao i stanja računa u svakom trenutku[22] i to u sigurnom i pouzdanom okruženju.

14.2 Sva detaljna elektronička izvješća trebala bi biti dostupna u sigurnom i pouzdanom okruženju. Kada pružatelji platnih usluga obavještavaju klijente o dostupnosti elektroničkih izvješća (npr. redovito prilikom izdavanja periodičkih elektroničkih izvješća, ili na *ad hoc* osnovi nakon provedbe transakcije) putem alternativnog kanala,

[21] Ti limiti mogu se primijeniti na globalnoj razini (tj. na sve platne instrumente kojima se omogućuje internetsko plaćanje) ili na pojedinačnoj razini.

[22] Isključujući izvanrednu neraspoloživost usluge zbog tehničkog održavanja ili kao posljedice značajnih incidenata.

poput SMS-a, elektroničke pošte ili dopisa, osjetljivi podaci o plaćanjima ne bi trebali biti uključeni u takve obavijesti ili, ako su uključeni, trebali bi biti prikriveni.

Prilog 1.: Primjeri najbolje prakse:

Uz prethodno utvrđene zahtjeve, ove smjernice daju i primjere najbolje prakse za koje se pružateljima platnih usluga i relevantnim sudionicima na tržištu preporučuje da ih usvoje, iako ih se na to ne obvezuje. Radi lakšeg snalaženja, poglavlja na koja se najbolje prakse primjenjuju izričito su navedena.

Opća kontrola i okruženje sigurnosti

Upravljanje

NP 1.: Politika sigurnosti može se sastaviti u posebnom dokumentu.

Kontrola i ovladavanje rizikom

NP 2.: Pružatelji platnih usluga mogu ponuditi sigurnosne alate (npr. uređaje i/ili prilagođene *web* preglednike, primjereno osigurane) za zaštitu sučelja klijenta od nezakonite uporabe ili napada (npr. napadi umetanjem malicioznog koda unutar web preglednika - „man in the browser").

Sljedivost

NP 3.: Pružatelji platnih usluga koji nude usluge prihvata mogu ugovorom zahtijevati od e-trgovaca koji pohranjuju informacije o plaćanjima da uspostave primjerene procese koji omogućuju sljedivost.

Posebna kontrola i sigurnosne mjere za internetska plaćanja

Početna identifikacija klijenta, informacije

NP 4.: Klijent bi mogao potpisati poseban ugovor o provođenju transakcija internetskog plaćanja umjesto da se uvjeti uključe u općenitiji opći ugovor o pružanju usluge s pružateljem platnih usluga.

NP 5.: Pružatelji platnih usluga također bi mogli osigurati da se klijentima kontinuirano ili, po potrebi, na *ad hoc* osnovi te putem primjerenih sredstava (npr. letaka, internetskih stranica), daju jasne i razumljive upute kojima se objašnjavaju njihove odgovornosti u pogledu sigurne uporabe usluge.

Pouzdana (stroga) autentifikacija

NP 6.: [kartice] E-trgovci mogu podržavati pouzdanu autentifikaciju imatelja kartice od strane izdavatelja za kartične transakcije putem interneta.

NP 7.: Pružatelji platnih usluga mogli bi razmotriti uporabu jedinstvenog alata za pouzdanu autentifikaciju klijenta za sve usluge internetskog plaćanja, kako bi proces bio što jednostavniji za klijenta. To bi moglo povećati prihvaćenost rješenja među klijentima i olakšati pravilnu uporabu.

NP 8.: Pouzdana autentifikacija klijenta mogla bi uključiti elemente koji povezuju provjeru s točno određenim iznosom i primateljem plaćanja. To bi moglo klijentima dati dodatnu sigurnost pri autorizaciji plaćanja. Tehnološko rješenje koje omogućuje povezivanje pouzdane autentifikacije podataka i podataka o transakciji trebalo bi biti otporno na zlonamjernu izmjenu.

Zaštita osjetljivih podataka o plaćanjima

NP 9.: Poželjno je da e-trgovci koji rukuju osjetljivim podacima o plaćanjima primjereno obuče svoje osoblje za sprječavanje prijevara te da obuku redovito unaprjeđuju kako bi osigurali da sadržaj obuke ostane relevantan u skladu s dinamičnim sigurnosnim okruženjem.

Edukacija klijenata i komunikacija

NP 10.: Poželjno je da pružatelji platnih usluga koji nude usluge prihvata organiziraju programe edukacije o sprečavanju prijevara za svoje e-trgovce.

Obavijesti, određivanje limita

NP 11: Unutar postavljenih limita, pružatelji platnih usluga mogli bi svojim klijentima omogućiti upravljanje limitima za usluge internetskog plaćanja u sigurnom i pouzdanom okruženju.

NP 12: Pružatelji platnih usluga mogli bi upozoravati klijente, putem telefona ili SMS-a, o sumnjivim i visoko rizičnim platnim transakcijama na temelju svojih politika o upravljanju rizicima.

NP 13.: Pružatelji platnih usluga mogli bi klijentima omogućiti određivanje općih, personaliziranih pravila kao parametara za njihovo ponašanje vezano uz internetska plaćanja i povezane usluge, npr. inciranje plaćanja samo iz određenih država i blokiranje plaćanja iniciranih iz drugih država ili uvrštavanje određenih primatelja plaćanja na bijele ili crne liste.