EBA/GL/2014/12_Rev1

19. december 2014

Končne smernice

o varnosti spletnih plačil

Vsebina

Smernice o varnosti spletnih plačil

Vloga teh smernic

Ta dokument vsebuje smernice, izdane v skladu s členom 16 Uredbe (EU) št. 1093/2010 Evropskega parlamenta in Sveta z dne 24. novembra 2010 o ustanovitvi Evropskega nadzornega organa (Evropski bančni organ) in o spremembi Sklepa št. 716/2009/ES ter razveljavitvi Sklepa Komisije 2009/78/ES (v nadaljnjem besedilu: uredba o EBA). V skladu s členom 16(3) uredbe o EBA si morajo pristojni organi in finančne institucije na vsak način prizadevati za upoštevanje smernic.

V smernicah je predstavljeno stališče organa EBA glede ustreznih nadzorniških praks v okviru Evropskega sistema finančnega nadzora ali glede tega, kako bi bilo treba uporabljati zakonodajo Unije na posameznih področjih. Organ EBA zato od vseh pristojnih organov in finančnih institucij, na katere je naslovil smernice, pričakuje, da jih bodo upoštevali. Pristojni organi, za katere smernice veljajo, bi jih morali upoštevati tako, da jih ustrezno vključijo v svoje nadzorne prakse (npr. s spremembo pravnega okvira ali nadzorniških postopkov), tudi če so smernice naslovljene predvsem na institucije.

Zahteve v zvezi s poročanjem

Pristojni organi morajo v skladu s členom 16(3) uredbe o EBA do 5. maja 2015 organ EBA uradno obvestiti, ali ravnajo oziroma ali nameravajo ravnati v skladu s temi smernicami, ali pa mu sporočiti razloge za njihovo neupoštevanje. Uradno obvestilo je treba poslati na obrazcu iz poglavja 5 na e-naslov compliance@eba.europa.eu z navedbo oznake „EBA/GL/2014/12“. Uradna obvestila morajo predložiti osebe, ki so pooblaščene za poročanje o skladnosti v imenu svojih pristojnih organov.

Uradna obvestila bodo v skladu s členom 16(3) uredbe o EBA objavljena na spletni strani organa EBA.

Naslov I – Področje uporabe in opredelitev pojmov

Področje uporabe

1. Te smernice določajo niz minimalnih zahtev na področju varnosti spletnih plačil. Smernice temeljijo na pravilih iz Direktive 2007/64/ES[1] (v nadaljnjem besedilu: direktiva o plačilnih storitvah) v zvezi z zahtevami za informacije o plačilnih storitvah in obveznostmi ponudnikov plačilnih storitev v zvezi z opravljanjem plačilnih storitev. Poleg tega člen 10(4) Direktive določa, da morajo imeti plačilne institucije zanesljive ureditve upravljanja in primerne mehanizme notranjih kontrol.

2. Smernice se nanašajo na opravljanje plačilnih storitev, ki jih ponudniki plačilnih storitev iz člena 1 Direktive zagotavljajo prek spleta.

3. Smernice so naslovljene na finančne institucije, kakor so opredeljene v členu 4(1) Uredbe (EU) št. 1093/2010, in pristojne organe, kakor so opredeljeni v členu 4(2) Uredbe (EU) št. 1093/2010. Pristojni organi v 28 državah članicah Evropske unije bi morali zagotoviti, da ponudniki plačilnih storitev iz člena 1 direktive o plačilnih storitvah pod njihovim nadzorom upoštevajo te smernice.

4. Poleg tega lahko pristojni organi od ponudnikov plačilnih storitev zahtevajo, da jim poročajo o tem, da smernice upoštevajo.

5. Te smernice ne vplivajo na veljavnost „Priporočil za varnost spletnih plačil“ Evropske centralne banke (v nadaljnjem besedilu: Poročilo).[2] Poročilo torej še naprej predstavlja dokument, na podlagi katerega bi morale centralne banke v okviru izvajanja pregleda nad plačilnimi sistemi in instrumenti presojati skladnost na področju varnosti spletnih plačil.

6. Smernice predstavljajo minimalna pričakovanja. Ne posegajo v odgovornost ponudnikov plačilnih storitev, da spremljajo in ocenjujejo tveganja, prisotna pri njihovih plačilnih operacijah, razvijajo svoje lastne podrobne varnostne politike ter zagotavljajo ustrezne varnostne ukrepe, ukrepe ob nepredvidljivih dogodkih, ukrepe za obvladovanje incidentov in ukrepe za neprekinjeno poslovanje, ki so sorazmerni s tveganji pri zagotovljenih plačilnih storitvah.

7. Namen smernic je opredeliti skupne minimalne zahteve za spodaj naštete spletne plačilne storitve ne glede na uporabljeno dostopno napravo:

[1] Direktiva 2007/64/ES Evropskega parlamenta in Sveta z dne 13. novembra 2007 o plačilnih storitvah na notranjem trgu in o spremembah direktiv 97/7/ES, 2002/65/ES, 2005/60/ES in 2006/48/ES ter o razveljavitvi Direktive 97/5/ES, UL L 319, 5.12.2007.

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

- [kartice] izvrševanje spletnih plačil s karticami, vključno s plačili z virtualnimi karticami, in registracija podatkov o plačilih s karticami za uporabo v „storitvah elektronske denarnice“;

- [kreditna plačila] izvrševanje spletnih kreditnih plačil;

- [e-pooblastilo] izdajanje in spreminjanje elektronskih pooblastil za direktne obremenitve;

- [e-denar] prenosi elektronskega denarja med dvema računoma elektronskega denarja prek spleta.

8. Kadar smernice navajajo rezultate, se ti lahko dosežejo z različnimi sredstvi. Poleg zahtev, določenih v nadaljevanju, te smernice vsebujejo tudi primere najboljših praks (v Prilogi 1), h katerim se ponudnike plačilnih storitev sicer spodbuja, ne zahteva pa se, da jih upoštevajo.

9. Kadar se opravljanje plačilnih storitev in instrumentov izvaja prek plačilne sheme (npr. sheme plačil s kartico, sheme za kreditna plačila, sheme za direktne obremenitve itd.), bi se morali pristojni organi in ustrezna centralna banka, ki izvaja nadzor nad plačilnimi instrumenti, povezati za namene zagotavljanja, da subjekti, ki so odgovorni za delovanje sheme, smernice dosledno uporabljajo.

10. Integratorji plačil[3], ki ponujajo storitve odrejanja plačil, se obravnavajo kot pridobitelji spletnih plačilnih storitev (in s tem ponudniki plačilnih storitev) ali zunanji ponudniki tehničnih storitev za zadevne sheme ali ponudnike plačilnih storitev. V slednjem primeru bi morali biti integratorji plačil pogodbeno zavezani, da upoštevajo smernice.

11. S področja uporabe smernic so izključeni:

- druge spletne storitve, ki jih zagotavlja ponudnik plačilnih storitev prek svoje spletne strani za plačevanje (npr. e-borzno posredovanje, pogodbe, sklenjene prek spleta);

- plačila, pri katerih se navodila pošljejo po pošti, s telefonskim nalogom, glasovno pošto ali z uporabo tehnologije kratkih sporočil;

- mobilna plačila, ki ne temeljijo na brskalnikih;

- kreditna plačila, pri katerih tretja stranka dostopa do plačilnega računa stranke;

- plačilne transakcije, izvedene s strani podjetij prek namenskih omrežij;

[3] Integratorji plačil zagotavljajo prejemniku plačila (tj. spletnemu trgovcu) standardiziran vmesnik do storitev odrejanja plačil, ki jih ponujajo ponudniki plačilnih storitev.

- plačila s karticami z uporabo anonimnih fizičnih ali virtualnih predplačniških kartic, ki jih ni mogoče ponovno polniti, kadar ni trajnega sodelovanja med izdajateljem in imetnikom kartice;

- kliring in poravnava plačilnih transakcij.

Opredelitev pojmov

12. V teh smernicah se, poleg opredelitev pojmov iz direktive o plačilnih storitvah, uporabljajo naslednje opredelitve pojmov:

- *Avtentikacija* pomeni postopek, ki ponudniku plačilnih storitev omogoča preverjanje strankine identitete.

- *Močna avtentikacija stranke* je za namene teh smernic postopek, ki temelji na uporabi dveh ali več naslednjih elementov – označeni so kot poznavanje, lastništvo in neločljiva povezava: i) nekaj, kar ve samo uporabnik, npr. statično geslo, koda, osebna identifikacijska številka; ii) nekaj, kar je v izključni lasti uporabnika, npr. žeton, pametna kartica, mobilni telefon; iii) nekaj, kar uporabnik je, npr. biometrična značilnost, kot je prstni odtis. Poleg tega morajo biti izbrani elementi vzajemno neodvisni, tj. kršitev enega ne vpliva na drugega oziroma druge. Najmanj en element bi moral biti tak, da ga ni mogoče ponovno uporabiti in reproducirati (z izjemo neločljive povezave) ter neopazno ukrasti prek spleta. Postopek močne avtentikacije bi moral biti zasnovan tako, da varuje zaupnost podatkov za avtentikacijo.

- *Odobritev* pomeni postopek, s katerim se preverja, ali ima stranka ali ponudnik plačilnih storitev pravico izvesti določeno dejanje, npr. pravico do prenosa sredstev ali dostopa do občutljivih podatkov.

- *Pooblastila* pomenijo informacije – običajno zaupne – ki jih zagotovi stranka ali ponudnik plačilnih storitev za avtentikacijo. Pooblastila lahko pomenijo tudi fizične orodje, ki vsebuje informacije (npr. generator enkratnega gesla, pametna kartica), ali nekaj, kar si uporabnik zapomni ali ga predstavlja (kot so biometrične značilnosti).

- *Večji varnostni incident iz naslova plačil* pomeni incident, ki pomembno vpliva ali lahko vpliva na varnost, celovitost ali kontinuiteto sistemov ponudnikov plačilnih storitev, povezanih s plačevanjem, in/ali varnost občutljivih podatkov o plačilih ali sredstev. Ocena pomembnosti bi morala upoštevati število potencialno oškodovanih strank, tvegani znesek in vpliv na druge ponudnike plačilnih storitev ali druge plačilne infrastrukture.

- *Analiza tveganosti transakcije* pomeni oceno tveganja, povezanega z določeno transakcijo, ki upošteva merila, kot so na primer strankini vzorci plačevanja (vedenje), vrednost zadevne transakcije, vrsta proizvoda in profil prejemnika.

- *Virtualne kartice* pomenijo možnost plačevanja s kartico, za katero se ustvari alternativna, začasna številka kartice s krajšim obdobjem veljavnosti, omejeno uporabo in vnaprej določenim limitom porabe, ki se lahko uporablja za spletne nakupe.

- *Storitve elektronske denarnice* pomenijo rešitve, s katerimi stranka lahko prijavi podatke, ki se nanašajo na enega ali več plačilnih instrumentov, za izvrševanje plačil z več spletnimi trgovci.

Naslov II – Smernice o varnosti spletnih plačil

Splošno kontrolno in varnostno okolje

Upravljanje

1. Ponudniki plačilnih storitev bi morali izvajati in redno preverjati formalno varnostno politiko za spletne plačilne storitve.

   1.1 Varnostna politika bi morala biti ustrezno dokumentirana, višje vodstvo pa bi jo moralo redno preverjati (v skladu s smernico 2.4) in odobriti. V njej bi morali biti opredeljeni cilji v zvezi z varnostjo in nagnjenost k prevzemanju tveganja.

   1.2 Varnostna politika bi morala opredeliti vloge in odgovornosti, vključno s funkcijo upravljanja tveganj, ki poroča neposredno ravni uprave, in linije poročanja za zadevne spletne plačilne storitve, vključno z upravljanjem občutljivih podatkov o plačilih, kar zadeva oceno, nadzor in zmanjševanje tveganj.

Ocena tveganja

2. Ponudniki plačilnih storitev bi morali izvajati in dokumentirati temeljita ocenjevanja tveganj v zvezi z varnostjo spletnih plačil in s tem povezanih storitev, in sicer pred samo uvedbo storitve oziroma storitev in naknadno na redni podlagi.

   2.1 Ponudniki plačilnih storitev bi morali prek svoje funkcije za upravljanje tveganj izvajati in dokumentirati podrobna ocenjevanja tveganj za spletna plačila in s tem povezane storitve. Ponudniki plačilnih storitev bi morali proučiti rezultate stalnega spremljanja groženj za varnost v zvezi s spletnimi plačilnimi storitvami, ki jih ponujajo ali nameravajo ponujati, ob upoštevanju: i) tehnoloških rešitev, ki jih uporabljajo, ii) storitev, ki jih zanje opravljajo zunanji izvajalci, in iii) tehničnega okolja strank. Ponudniki plačilnih storitev bi morali proučiti tveganja, ki so povezana z izbranimi tehnološkimi platformami, arhitekturo aplikacij, programskimi tehnikami in rednimi postopki, ki jih uporabljajo sami[4] in njihove stranke,[5] ter rezultate procesa spremljanja varnostnih incidentov (glej smernico 3).

   2.2 Na podlagi tega bi morali ponudniki plačilnih storitev določiti, ali in v kolikšni meri so morda potrebne spremembe obstoječih varnostnih ukrepov, tehnologij, ki se uporabljajo, ter razpoložljivih postopkov ali storitev. Ponudniki plačilnih storitev bi morali upoštevati čas, ki je potreben za izvajanje sprememb (vključno z uvajanjem

[4] Na primer občutljivost sistema na vdor v postopek izvajanja plačila, injekcija SQL, skriptno izvajanje na več mestih, prekoračitve medpomnilnika itd.

[5] Na primer tveganja, ki so povezana z uporabo večpredstavnostnih aplikacij, vtičnikov v brskalnikih, okvirov, zunanjih povezav itd.

strank), in sprejeti ustrezne vmesne ukrepe za čim večje zmanjšanje varnostnih incidentov ter goljufij in morebitnih motečih učinkov.

2.3 Ocenjevanje tveganj bi moralo obravnavati potrebo po zaščiti in varstvu občutljivih podatkov o plačilih.

2.4 Ponudniki plačilnih storitev bi morali proučiti scenarije tveganja in obstoječe varnostne ukrepe po večjih incidentih, ki vplivajo na njihove storitve, pred večjo spremembo infrastrukture ali postopkov in kadar v okviru spremljanja tveganj odkrijejo nove grožnje. Poleg tega bi bilo treba najmanj enkrat na leto izvesti splošen pregled ocenjevanja tveganj. Rezultate ocenjevanj tveganja in pregledov bi bilo treba predložiti višjemu vodstvu v odobritev.

Spremljanje incidentov in poročanje o njih

3. Ponudniki plačilnih storitev bi morali zagotavljati dosledno in celostno spremljanje in obravnavanje varnostnih incidentov ter nadaljnje ukrepe, vključno s pritožbami strank v zvezi z varnostjo. Ponudniki plačilnih storitev bi morali vzpostaviti postopek za poročanje o tovrstnih incidentih upravi, pri večjih varnostnih incidentih iz naslova plačil pa pristojnim organom.

3.1 Ponudniki plačilnih storitev bi morali zagotoviti postopek za spremljanje in obravnavanje varnostnih incidentov in pritožb strank v zvezi z varnostjo in tudi za nadaljnje ukrepe v teh primerih ter o tovrstnih incidentih poročati upravi.

3.2 Ponudniki plačilnih storitev bi morali zagotoviti postopek za takojšnje obveščanje pristojnih organov (tj. nadzornikov in organov za varstvo podatkov), kjer ti obstajajo, in sicer v primeru večjih varnostnih incidentov iz naslova plačil, ki jih zagotavljajo.

3.3 Ponudniki plačilnih storitev bi morali vzpostaviti postopek za sodelovanje z ustreznimi organi pregona pri večjih varnostnih incidentih iz naslova plačil, vključno s kršitvami varstva podatkov.

3.4 Ponudniki plačilnih storitev pridobitelji bi morali na podlagi pogodbe zahtevati, da spletni trgovci, ki shranjujejo, obdelujejo ali posredujejo občutljive podatke o plačilih, sodelujejo z njimi in tudi z ustreznimi organi pregona v primeru večjih varnostnih incidentov iz naslova plačil, vključno s kršitvami varstva podatkov. Če ponudnik plačilnih storitev odkrije, da spletni trgovec ne sodeluje, kot zahteva pogodba, bi moral ukrepati, da uveljavi to pogodbeno obveznost, ali pogodbo prekiniti.

Nadzor in zmanjševanje tveganj

4. Ponudniki plačilnih storitev bi morali izvajati varnostne ukrepe v skladu s svojimi varnostnimi politikami, da bi zmanjšali ugotovljena tveganja. Ti ukrepi bi morali vključevati večplastno

varnostno zaščito, ki omogoča, da se ob neuspehu ene ravni zaščite aktivira druga raven zaščite („globinska zaščita“).

4.1 Pri oblikovanju, razvijanju in vzdrževanju spletnih plačilnih storitev bi morali ponudniki plačilnih storitev posebej upoštevati ustrezno razdelitev nalog v okoljih informacijske tehnologije (IT) (npr. razvojno, testno in produkcijsko okolje) ter ustrezno izvajanje načela „najmanjšega privilegija“ kot osnovo za zanesljivo upravljanje identitete in dostopa.[6]

4.2 Ponudniki plačilnih storitev bi morali imeti na voljo ustrezne varnostne rešitve za zaščito omrežij, spletnih strani, strežnikov in komunikacijskih povezav pred zlorabo ali napadi. Ponudniki plačilnih storitev bi morali razbremeniti strežnike vseh odvečnih funkcij, da bi jih zaščitili (okrepili), ter odpraviti ali zmanjšati ranljivosti ogroženih aplikacij. Dostop različnih aplikacij do potrebnih podatkov in virov bi moral biti strogo omejen na najnižjo raven po načelu „najmanjšega privilegija“. Za omejitev uporabe „lažnih“ spletnih strani (ki oponašajo legitimne strani ponudnikov plačilnih storitev) bi bilo treba transakcijske spletne strani, ki ponujajo spletne plačilne storitve, označiti z razširjenimi potrdili o veljavnosti, sestavljenimi v imenu ponudnikov plačilnih storitev, ali z drugimi podobnimi načini za avtentikacijo.

4.3 Ponudniki plačilnih storitev bi morali imeti na voljo ustrezne postopke za spremljanje, sledenje in omejevanja dostopa do: i) občutljivih podatkov o plačilih ter ii) logičnih in fizičnih kritičnih virov, kot so omrežja, sistemi, zbirke podatkov, varnostni moduli itd. Ponudniki plačilnih storitev bi morali ustvarjati, shranjevati in analizirati ustrezne dnevnike in revizijske sledi.

4.4 Pri oblikovanju,[7] razvijanju in vzdrževanju spletnih plačilnih storitev bi ponudniki plačilnih storitev morali zagotoviti, da je zmanjšanje količine podatkov[8] nujna sestavina osrednje funkcije: zbiranje, preusmerjanje, obdelava, shranjevanje in/ali arhiviranje ter vizualizacija občutljivih podatkov o plačilih bi morali ostati na absolutno minimalni ravni.

4.5 Varnostne ukrepe za spletne plačilne storitve bi bilo treba preizkusiti pod nadzorom funkcije upravljanja tveganj, da bi tako zagotovili njihovo zanesljivost in učinkovitost. Vse spremembe bi morale biti predmet formalnega postopka uvajanja sprememb, ki zagotavlja, da so spremembe ustrezno načrtovane, preizkušene, dokumentirane in odobrene. Na podlagi uvedenih sprememb in opaženih groženj za varnost bi bilo treba

[6] „Vsak program in vsak privilegirani uporabnik sistema bi moral delovati tako, da bi koristil najmanjšo mogočo mero potrebnih privilegijev za dokončanje dela.“ Glej Saltzer, J.H. (1974), „Zaščita in nadzor izmenjave informacij v sistemu Multics“ (*Protection and the Control of Information Sharing in Multics*), Sporočilo ACM, knjiga 17, št. 7, str. 388.

[7] Zasebnost že pri načrtovanju.

[8] Zmanjšanje količine podatkov se nanaša na politiko zbiranja čim manjše količine osebnih podatkov, potrebnih za izpeljavo dane funkcije.

testiranja redno ponavljati, vključno s scenariji zadevnih in znanih potencialnih napadov.

4.6 Varnostne ukrepe ponudnikov plačilnih storitev za spletne plačilne storitve bi bilo treba redno revidirati, da bi zagotovili njihovo zanesljivost in učinkovitost. Revidirati bi bilo treba tudi izvajanje in delovanje spletnih plačilnih storitev. Pogostost in osredotočenost takih revizij bi morala upoštevati s tem povezana varnostna tveganja ter biti z njimi sorazmerna. Revizije bi morali izvajati zanesljivi in neodvisni (notranji ali zunanji) strokovnjaki. Ti nikakor ne bi smeli biti povezani z razvojem, izvajanjem ali operativnim upravljanjem zagotovljenih spletnih plačilnih storitev.

4.7 Kadar koli ponudniki plačilnih storitev funkcije, ki so povezane z varnostjo spletnih plačilnih storitev, prenesejo na zunanje izvajalce, bi pogodba morala vključevati določbe, ki zahtevajo skladnost z načeli in smernicami iz teh smernic.

4.8 Ponudniki plačilnih storitev, ki ponujajo storitve pridobivanja, bi morali od spletnih trgovcev, ki obravnavajo (tj. shranjujejo, obdelujejo ali posredujejo) občutljive podatke o plačilih, na podlagi pogodbe zahtevati, da izvajajo varnostne ukrepe v svoji infrastrukturi IT, v skladu s smernicami 4.1 do 4.7, da se prepreči kraja teh občutljivih podatkov o plačilih iz njihovih sistemov. Če ponudnik plačilnih storitev odkrije, da spletni trgovec ne zagotavlja zahtevanih varnostnih ukrepov, bi moral ukrepati, da uveljavi to pogodbeno obveznost, ali pogodbo prekiniti.

Sledljivost

5. Ponudniki plačilnih storitev bi morali imeti na voljo postopke, ki zagotavljajo, da se lahko ustrezno sledi vsem transakcijam in tudi poteku postopka e-pooblastila.

5.1 Ponudniki plačilnih storitev bi morali zagotoviti, da njihova storitev vključuje varnostne mehanizme za podrobno beleženje podatkov o transakciji in e-pooblastilu, vključno z zaporedno številko transakcije, časovnim žigom za podatke o transakciji, spremembami parametrizacije ter tudi dostopom do podatkov o transakciji in e-pooblastilu.

5.2 Ponudniki plačilnih storitev bi morali uporabljati dnevniške datoteke, ki omogočajo sledenje morebitnim dodatkom, spremembam ali brisanjem podatkov o transakciji in e-pooblastilu.

5.3 Ponudniki plačilnih storitev bi morali preverjati in analizirati podatke o transakciji in e-pooblastilu ter zagotoviti orodja za presojo dnevniških datotek. Zadevne aplikacije bi morale biti na voljo samo pooblaščenemu osebju.

Posebni kontrolni in varnostni ukrepi za spletna plačila

Začetna identifikacija stranke, podatki

6. Stranke bi bilo treba ustrezno identificirati v skladu z evropsko zakonodajo na področju preprečevanja pranja denarja[9], stranke pa bi morale potrditi, da so pripravljene izvesti spletna plačila z uporabo teh storitev, preden se jim zanje odobri dostop. Ponudniki plačilnih storitev bi morali zagotoviti stranki ustrezne „predhodne“, „redne“ ali, kjer to velja, „ad hoc“ informacije o potrebnih zahtevah (npr. oprema, postopki) za izvajanje varnih spletnih plačilnih transakcij in o tveganjih, ki so neločljivo povezana s tem.

6.1 Ponudniki plačilnih storitev bi morali zagotoviti, da je stranka izvedla postopke v zvezi s skrbnim preverjanjem stranke ter zagotovila ustrezne osebne dokumente[10] in s tem povezane podatke, preden se ji odobri dostop do spletnih plačilnih storitev.[11]

6.2 Ponudniki plačilnih storitev bi morali zagotoviti, da predhodne informacije,[12] ki se zagotovijo stranki, vsebujejo vse podrobnosti v zvezi s spletnimi plačilnimi storitvami. Če je to primerno, bi morale vključevati:

- točne informacije o vseh zahtevah, ki zadevajo opremo, programsko opremo ali druga potrebna orodja stranke (npr. protivirusna programska oprema, požarni zidovi);
- navodila za pravilno in varno uporabo osebnih varnostnih poverilnic;
- postopen opis postopka za stranko, da želi predložiti in odobriti plačilno transakcijo in/ali pridobiti informacije, vključno s posledicami vsakega ukrepa;
- navodila za pravilno in varno uporabo vse strojne in programske opreme, ki se zagotovi stranki;
- postopke, ki jih je treba izvesti ob izgubi ali kraji osebnih varnostnih poverilnic ali strojne ali programske opreme stranke za prijavo v sistem ali izvajanje transakcij;
- postopke, ki jih je treba izvesti ob odkritju ali sumu zlorabe;

[9] Na primer, Direktiva 2005/60/ES Evropskega parlamenta in Sveta z dne 26. oktobra 2005 o preprečevanju uporabe finančnega sistema za pranje denarja in financiranje terorizma. UL L 309, 25.11.2005, str. 15–36. Glej tudi Direktivo Komisije 2006/70/ES z dne 1. avgusta 2006 o določitvi izvedbenih ukrepov za Direktivo 2005/60/ES Evropskega parlamenta in Sveta glede opredelitve „politično izpostavljene osebe“ in tehničnih meril za postopke poenostavljene dolžnosti skrbnosti pri ugotavljanju identitete stranke ter izjeme na podlagi finančne dejavnosti, ki poteka zgolj občasno ali v omejenem obsegu. UL L 214, 4.8.2006, str. 29–34.

[10] Na primer potni list, osebno izkaznico ali napredni elektronski podpis.

[11] Postopek identifikacije stranke ne posega v odstopanja, ki jih zagotavlja veljavna zakonodaja na področju preprečevanja pranja denarja. Ponudnikom plačilnih storitev ni treba izvajati ločenega postopka identifikacije stranke za spletne plačilne storitve, če je bila taka identifikacija stranke že izvedena, na primer za druge obstoječe storitve, povezane s plačili, ali za odprtje računa.

[12] Ti podatki dopolnjujejo člen 42 direktive o plačilnih storitvah, ki določa, katere informacije morajo ponudniki plačilnih storitev zagotoviti uporabniku plačilne storitve, preden sklenejo pogodbo za zagotavljanje plačilnih storitev.

- opis odgovornosti in obveznosti ponudnikov plačilnih storitev oziroma stranke v zvezi z uporabo spletne plačilne storitve.

6.3 Ponudniki plačilnih storitev bi morali zagotoviti, da okvirna pogodba s stranko določa, da lahko ponudnik plačilnih storitev blokira določeno transakcijo ali plačilni instrument[13] zaradi varnostnih zadržkov. Določiti bi moral način in pogoje obveščanja strank ter kako lahko stranka vzpostavi stik s ponudnikom plačilnih storitev, da bi spletno plačilno transakcijo ali storitev „deblokirali“, kar je v skladu z direktivo o plačilnih storitvah.

[13] Glej člen 55 direktive o plačilnih storitvah o omejitvah uporabe plačilnega instrumenta.

Močna avtentikacija strank

7. Začetek odreditve spletnih plačil in tudi dostop do občutljivih podatkov o plačilih bi morala biti zaščitena z močno avtentikacijo strank. Ponudniki plačilnih storitev bi morali imeti vzpostavljen postopek močne avtentikacije strank v skladu z opredelitvijo iz teh smernic.

7.1 [kreditna plačila/e-pooblastilo/e-denar] Ponudniki plačilnih storitev bi morali izvajati močno avtentikacijo strank za odobritev strankinih spletnih plačilnih transakcij (vključno z množičnimi kreditnimi plačili) ter izdajo ali spremembo elektronskih pooblastil za direktno obremenitev. Ob tem bi ponudniki plačilnih storitev lahko proučili sprejetje alternativnih ukrepov za avtentikacijo strank za:

- izplačila zanesljivim upravičencem, ki so že na predhodnih belih seznamih za dano stranko;
- transakcije med dvema računoma iste stranke pri istem ponudniku plačilnih storitev;
- prenose pri istem ponudniku plačilnih storitev, utemeljene na podlagi analize tveganosti transakcije;
- plačila majhnih vrednosti, kot jih opredeljuje direktiva o plačilnih storitvah.[14]

7.2 Za pridobitev dostopa do občutljivih podatkov o plačilih ali za njihovo spremembo (vključno z oblikovanjem in spreminjanjem belih seznamov) je potrebna močna avtentikacija. Kadar ponudnik plačilnih storitev ponuja izključno svetovalne storitve in ne razkriva občutljivih podatkov o strankah ali plačilih, na primer podatkov o plačilnih karticah, ki jih je mogoče zlahka zlorabiti za goljufijo, lahko ponudnik plačilnih storitev prilagodi svoje zahteve v zvezi z avtentikacijo na podlagi ocene tveganja.

7.3 [kartice] Pri kartičnih transakcijah bi morali vsi ponudniki plačilnih storitev, ki izdajajo kartice, podpirati močno avtentikacijo imetnika kartice. Vse izdane kartice morajo biti tehnično pripravljene (registrirane) za uporabo z močno avtentikacijo.

7.4 [kartice] Ponudniki plačilnih storitev, ki ponujajo storitve pridobivanja, bi morali podpirati tehnologije, ki izdajatelju omogočajo močno avtentikacijo imetnika kartice za kartične plačilne sheme, v katerih sodeluje pridobitelj.

7.5 [kartice] Ponudniki plačilnih storitev, ki ponujajo storitve pridobivanja, bi morali od svojega spletnega trgovca zahtevati, da podpira rešitve, ki izdajatelju omogočajo močno avtentikacijo imetnika kartice za spletne kartične transakcije. Uporaba alternativnih ukrepov avtentikacije bi lahko bila primerna za vnaprej določene skupine

[14] Glej opredelitev instrumentov za plačila majhnih vrednosti v členih 34(1) in 53(1) direktive o plačilnih storitvah.

transakcij z nizko stopnjo tveganja, na primer na podlagi analize tveganosti transakcije, ali za plačila majhnih vrednosti, kot jih opredeljuje direktiva o plačilnih storitvah.

7.6 [kartice] Za sheme plačil s karticami, ki jih storitev podpira, bi morali ponudniki storitev elektronske denarnice od izdajatelja zahtevati močno avtentikacijo, ko zakoniti imetnik prvič vnaša podatke o kartici.

7.7 Ponudniki storitev elektronske denarnice bi morali podpirati močno avtentikacijo strank, ko se te prijavijo v plačilne storitve elektronske denarnice ali izvajajo spletne kartične transakcije. Uporaba alternativnih ukrepov avtentikacije bi lahko bila primerna za vnaprej določene skupine transakcij z nizko stopnjo tveganja, na primer na podlagi analize tveganosti transakcije, ali za plačila majhnih vrednosti, kot jih opredeljuje direktiva o plačilnih storitvah.

7.8 [kartice] Pri virtualnih karticah bi morala prva registracija potekati v varnem in zanesljivem okolju.[15] Močno avtentikacija stranke bi morala biti obvezna za postopek ustvarjanja podatkov virtualne kartice, če se kartica izdaja v internetnem okolju.

7.9 Ponudniki plačilnih storitev bi morali zagotoviti ustrezno dvostransko avtentikacijo pri komuniciranju s spletnimi trgovci za namene odreditve spletnih plačil in dostopa do občutljivih podatkov o plačilih.

Registracija in zagotavljanje orodij za avtentikacijo in/ali programske opreme, ki jo dobi stranka

8. Ponudniki plačilnih storitev bi morali zagotoviti, da registracija in začetna zagotovitev orodij za avtentikacijo, potrebnih za uporabo spletne plačilne storitve, in/ali dostava programske opreme, povezane s plačili, strankam potekajo varno.

8.1 Registracija in zagotavljanje orodij za avtentikacijo in/ali programske opreme, povezane s plačilom, ki jo dobi stranka, bi morali izpolnjevati naslednje zahteve.

- Postopke, povezane s tem, bi bilo treba izvajati v varnem in zanesljivem okolju ob upoštevanju morebitnih tveganj, ki izhajajo iz naprav, nad katerimi ponudnik plačilnih storitev nima nadzora.

- Vzpostavljeni bi morali biti učinkoviti in varni postopki za dostavo osebnih varnostnih poverilnic, programske opreme za izvajanje plačil in vseh osebnih naprav, povezanih s spletnimi plačili. Programska oprema, dostavljena prek

[15] Okolja v okviru odgovornosti ponudnika plačilnih storitev, ki zagotavljajo ustrezno avtentikacijo stranke in ponudnika plačilnih storitev, ki ponuja storitev, ter tudi zaščito zaupnih/občutljivih informacij, so: i) prostori ponudnika plačilnih storitev; ii) spletna stran internetnega bančništva ali druga varna spletna stran, npr. kadar upravljavec plačilne sheme ponuja primerljive varnostne funkcije med drugim, kot je opredeljeno v smernici 4; ali iii) storitve bankomatov. (Pri bankomatih je obvezna močna avtentikacija stranke. Tako avtentikacijo navadno zagotavljata čip in PIN ali čip in biometrični podatki.)

spleta, bi morala imeti tudi digitalni podpis ponudnika plačilnih storitev, da stranka lahko preveri njeno pristnost in da ni bila nedovoljeno spremenjena.

- [kartice] Pri kartičnih transakcijah bi stranka morala imeti možnost, da se prijavi v močno avtentikacijo neodvisno od določenega spletnega nakupa. Kadar obstaja možnost aktivacije med spletnim nakupovanjem, bi bilo treba stranko preusmeriti v varno in zanesljivo okolje.

8.2 [kartice] Izdajatelji bi morali aktivno spodbujati imetnike kartic k prijavi v močno avtentikacijo ter svojim imetnikom kartic omogočiti, da prijavo obidejo samo izjemoma in v omejenem številu primerov, kadar to upravičuje tveganje, povezano z določeno kartično transakcijo.

Poskusi prijave, iztek postopka, veljavnost avtentikacije

9. Ponudniki plačilnih storitev bi morali omejiti število poskusov prijave ali avtentikacije, opredeliti pravila za „iztek“ postopka spletne plačilne storitve in nastaviti omejitev časa za veljavnost avtentikacije.

9.1 Kadar se za avtentikacijo uporablja enkratno geslo, bi morali ponudniki plačilnih storitev zagotoviti, da je obdobje veljavnosti takih gesel omejeno na najkrajši potrebni čas.

9.2 Ponudniki plačilnih storitev bi morali določiti največje število neuspelih poskusov prijave ali avtentikacije, po katerih se dostop do spletne plačilne storitve (začasno ali trajno) blokira. Zagotoviti bi morali varen postopek za ponovno aktivacijo blokiranih spletnih plačilnih storitev.

9.3 Ponudniki plačilnih storitev bi morali določiti najdaljše obdobje, po katerem se neaktivni postopki spletnih plačilnih storitev samodejno prekinejo.

Spremljanje transakcije

10. Mehanizme za spremljanje transakcije, zasnovane za preprečevanje, odkrivanje in blokiranje goljufivih plačilnih transakcij, bi bilo treba vklopiti pred zadnjo odobritvijo ponudnika plačilnih storitev; za sumljive ali zelo tvegane transakcije bi bilo treba izvesti poseben postopek preverjanja in presoje. Enakovredni varnostni mehanizmi za spremljanje in odobritev bi morali biti vzpostavljeni tudi za izdajo e-pooblastil.

10.1 Ponudniki plačilnih storitev bi morali uporabljati sisteme za odkrivanje in preprečevanje goljufij, da bi prepoznali sumljive transakcije, preden ponudnik plačilnih storitev dokončno odobri transakcije ali e-pooblastila. Taki sistemi bi morali temeljiti na primer na pravilih na podlagi parametrov (kot so črni seznami kompromitiranih ali ukradenih podatkov o karticah) in spremljati vzorce nenavadnega vedenja stranke ali

strankine dostopne naprave (kot so sprememba naslova IP (Internet Protocol)[16] ali razpona IP med postopkom spletne plačilne storitve, kar je včasih mogoče odkriti s preverjanjem geolokacije naslova IP[17], netipične skupine spletnih trgovcev za določeno stranko ali podatki o nenormalnih transakcijah itd.). Taki sistemi bi morali biti zmožni odkriti tudi znake okužbe programske opreme v postopku (npr. z avtomatiziranim preverjanjem proti ročnemu preverjanju) in znane scenarije goljufij. Obseg, kompleksnost in prilagodljivost rešitev za spremljanje bi morali biti ob upoštevanju ustrezne zakonodaje o varstvu podatkov sorazmerni z rezultati ocene tveganja.

10.2 Ponudniki plačilnih storitev pridobitelji bi morali imeti vzpostavljene sisteme za odkrivanje in preprečevanje goljufij, da bi lahko spremljali dejavnosti spletnih trgovcev.

10.3 Ponudniki plačilnih storitev bi morali izvesti vse postopke preverjanja in presoje transakcije v ustreznem časovnem obdobju, da ne bi neupravičeno zavlačevali začetka odreditve in/ali izvršitve zadevne plačilne storitve.

10.4 Kadar se ponudnik plačilnih storitev v skladu s svojo politiko obvladovanja tveganj odloči za blokado plačilne transakcije, za katero je bilo ugotovljeno, da gre morda za goljufijo, bi moral ohraniti blokado čim krajši čas, dokler se ne razrešijo vprašanja glede varnosti.

Zaščita občutljivih podatkov o plačilih

11. Občutljive podatke o plačilih bi bilo treba zaščititi med hrambo, obdelavo ali posredovanjem.

11.1 Vsi podatki, ki se uporabljajo za identifikacijo in avtentikacijo strank (npr. ob prijavi, na začetku odreditve spletnih plačil ter ob izdaji, spremembi ali preklicu e-pooblastil) in tudi vmesnika stranke (spletne strani ponudnika plačilnih storitev ali spletnega trgovca), bi morali biti ustrezno zavarovani pred krajo in nepooblaščenim dostopom ali spreminjanjem.

11.2 Ponudniki plačilnih storitev bi morali zagotoviti, da se pri izmenjavi občutljivih podatkov o plačilih prek spleta uporablja varno šifriranje od začetka do konca[18] med strankama, ki sta v stiku med zadevnim postopkom komuniciranja, da bi zaščitili zaupnost in celovitost podatkov z uporabo močnih in splošno priznanih tehnik šifriranja.

11.3 Ponudniki plačilnih storitev, ki ponujajo storitve pridobivanja, bi morali spodbuditi svoje spletne trgovce, naj občutljivih podatkov o plačilih ne shranjujejo. Če spletni trgovci obravnavajo, tj. shranjujejo, obdelujejo ali posredujejo, občutljive podatke o

[16] Naslov IP je edinstvena številčna koda, ki omogoča prepoznavanje vsakega računalnika, povezanega z internetom.

[17] S preverjanjem „geolokacije naslova IP“ preverimo, ali se država izdajatelja ujema z naslovom IP, s katerega uporabnik izvaja transakcijo.

[18] Šifriranje od začetka do konca se nanaša na šifriranje v ali pri izvornem končnem sistemu z ustreznim dešifriranjem samo v ali pri ciljnem končnem sistemu. ETSI EN 302 109 V1.1.1. 2003-06).

plačilih, bi morali taki ponudniki plačilnih storitev od spletnih trgovcev na podlagi pogodbe zahtevati, da zagotovijo potrebne ukrepe za zaščito teh podatkov. Ponudniki plačilnih storitev bi morali izvajati redne kontrole. Če ponudnik plačilnih storitev odkrije, da spletni trgovec, ki obravnava občutljive podatke o plačilih, ne zagotavlja potrebnih varnostnih ukrepov, bi moral ukrepati, da uveljavi to pogodbeno obveznost, ali pogodbo prekiniti.

Ozaveščanje, izobraževanje in obveščanje strank

Izobraževanje in obveščanje strank

12. Ponudniki plačilnih storitev bi morali zagotoviti pomoč in navodila za stranke, kjer je to potrebno, v zvezi z varno uporabo spletnih plačilnih storitev. Ponudniki plačilnih storitev bi morali komunicirati s svojimi strankami tako, da bi jim potrdili pristnost prejetih sporočil.

12.1 Ponudniki plačilnih storitev bi morali zagotoviti najmanj en zavarovan kanal[19] za stalno komunikacijo s strankami v zvezi s pravilno in varno uporabo spletne plačilne storitve. Ponudniki plačilnih storitev bi morali stranke obvestiti o tem kanalu in pojasniti, da sporočila v imenu ponudnika plačilnih storitev, poslana po drugih poteh, na primer po elektronski pošti, ki se nanašajo na pravilno in varno uporabo spletne plačilne storitve, niso zanesljiva. Ponudnik plačilnih storitev bi moral pojasniti:

- postopek, po katerem lahko stranke poročajo ponudniku plačilnih storitev o (domnevnih) nepravih plačilih, sumljivih incidentih ali nepravilnostih med postopkom spletne plačilne storitve in/ali morebitnih poskusih socialnega inženiringa[20];
- naslednje korake, tj. kako bo ponudnik plačilnih storitev odgovoril stranki;
- kako bo ponudnik plačilnih storitev obvestil stranko o (potencialnih) nepravih transakcijah ali o tem, da se niso začele izvajati, ali opozoril stranko o pojavu napadov (npr. e-pošta z lažnim predstavljanjem).

12.2 Ponudniki plačilnih storitev bi morali po zavarovanem kanalu obveščati stranke o posodobitvah varnostnih postopkov v zvezi s spletnimi plačilnimi storitvami. Tudi vsa opozorila o večjih porajajočih se tveganjih (npr. opozorila o socialnem inženiringu) bi bilo treba poslati po zavarovanem kanalu.

12.3 Ponudniki plačilnih storitev bi morali strankam zagotoviti pomoč za vsa vprašanja, pritožbe, zahtevke za podporo in obvestila o nepravilnostih ali incidentih v zvezi z spletnimi plačili in podobnimi storitvami, stranke pa bi bilo treba ustrezno obvestiti o tem, kako se taka pomoč lahko pridobi.

12.4 Ponudniki plačilnih storitev bi morali uvesti programe za izobraževanje in ozaveščanje strank, katerih namen bi bil zagotoviti, da bi stranke razumele vsaj to, da je treba:

- zaščititi svoja gesla, varnostne žetone, osebne podatke in druge zaupne podatke;

[19] Na primer temu namenjen poštni predal na spletni strani ponudnika plačilnih storitev ali zavarovani spletni strani.

[20] Socialni inženiring v tem smislu pomeni tehnike manipulacije z ljudmi za pridobivanje informacij (npr. po e-pošti ali s telefonskimi klici) ali priklic informacij s socialnih omrežij za namene goljufije ali pridobivanje nepooblaščenega dostopa do računalnika ali omrežja.

- ustrezno nadzorovati varnost osebnih naprav (npr. računalnika) z namestitvijo in nadgradnjo varnostnih komponent (protivirusna zaščita, požarni zidovi, varnostni popravki);

- upoštevati večje grožnje in tveganja, ki so povezani s prenašanjem programske opreme z interneta, če stranka ne more biti zares prepričana, da je programska oprema pristna in ni bila nedovoljeno spremenjena;

- uporabljati pravo spletno stran ponudnika plačilnih storitev za spletna plačila.

12.5 Ponudniki plačilnih storitev pridobitelji bi morali od spletnih trgovcev zahtevati, naj bodo postopki, povezani s plačili, jasno ločeni od spletne trgovine, da bodo stranke lažje ugotovile, kdaj komunicirajo s ponudnikom plačilnih storitev in ne s prejemnikom plačila (npr. s preusmerjanjem stranke in odprtjem novega okna, zato da se postopek plačevanja ne pokaže v okviru spletnega trgovca).

Obvestila, določanje omejitev

13. Ponudniki plačilnih storitev bi morali določiti omejitve za spletne plačilne storitve in svojim strankam v okviru teh omejitev zagotoviti možnosti za nadaljnje zmanjšanje tveganj. Prav tako lahko zagotovijo tudi storitve opozarjanja storitve upravljanja profilov strank.

13.1 Ponudniki plačilnih storitev bi morali, preden stranki zagotovijo spletne plačilne storitve, določiti omejitve[21], ki veljajo za te storitve (npr. najvišji znesek za vsako posamezno plačilo ali kumulativni znesek za določeno obdobje), o tem pa bi morali obvestiti svoje stranke. Ponudniki plačilnih storitev bi morali strankam omogočiti, da izklopijo funkcijo spletnega plačila.

Dostop strank do informacij o statusu postopka odreditve in izvršitve plačila

14. Ponudniki plačilnih storitev bi morali svojim strankam potrditi, da je bilo plačilo odrejeno, in jim pravočasno zagotoviti vse potrebne informacije, s katerimi lahko preverijo, da se je plačilna transakcija začela izvajati in/ali je bila izvršena pravilno.

14.1 [kreditna plačila/e-pooblastilo] Ponudniki plačilnih storitev bi morali strankam zagotoviti možnost, da skoraj v realnem času preverijo status izvrševanja transakcij ter v vsakem trenutku tudi saldo računov[22] v varnem in zanesljivem okolju.

14.2 Vsi podrobni elektronski izpiski bi morali biti na voljo v varnem in zanesljivem okolju. Kadar ponudniki plačilnih storitev obveščajo stranke o razpoložljivosti elektronskih izpiskov (npr. redno ob izdaji rednega e-izpiska ali ad hoc po izvršitvi transakcije) po alternativnem kanalu, kot so kratka sporočila, e-pošta ali pismo, ta sporočila ne bi

[21] Take omejitve se lahko uporabljajo na splošno (tj. za vse plačilne instrumente, ki omogočajo spletna plačila) ali v posamičnih primerih.

[22] Razen v primeru izjemne nerazpoložljivosti te možnosti zaradi tehničnega vzdrževanja ali zaradi večjih incidentov.

smela vsebovati občutljivih podatkov o plačilih, če pa jih vsebujejo, bi morali biti prikriti.

Naslov III – Končne določbe in izvajanje

15. Smernice se začnejo uporabljati 01.08.2015.

Priloga 1: Primeri najboljše prakse

Poleg zgoraj določenih zahtev te smernice opisujejo nekatere najboljše prakse, h katerim se ponudnike plačilnih storitev sicer spodbuja, ne zahteva pa se, da jih upoštevajo. Zaradi lažjega sklicevanja so poglavja, na katera se te najboljše prakse nanašajo, izrecno navedena.

Splošno kontrolno in varnostno okolje

Upravljanje

NP 1: Varnostna politika bi lahko bila zapisana v posebnem dokumentu.

Nadzor in zmanjševanje tveganj

NP 2: Ponudniki plačilnih storitev bi lahko zagotovili varnostna orodja (npr. ustrezno zavarovane naprave in/ali prirejene brskalnike), da bi zaščitili strankin vmesnik pred nezakonito rabo ali napadi (npr. napadi „prestrezanja v brskalniku“).

Sledljivost

NP 3: Ponudniki plačilnih storitev, ki ponujajo storitve pridobivanja, bi lahko na podlagi pogodbe zahtevali, da morajo spletni trgovci, ki shranjujejo podatke o plačilih, uvesti ustrezne postopke, ki podpirajo sledljivost.

Posebni kontrolni in varnostni ukrepi za spletna plačila

Začetna identifikacija stranke, podatki

NP 4: Stranka bi lahko podpisala posebno pogodbo o storitvah za izvajanje spletnih plačilnih transakcij, namesto da bi bili pogoji vključeni v širšo splošno pogodbo o storitvah s ponudniki plačilnih storitev.

NP 5: Ponudniki plačilnih storitev bi lahko tudi poskrbeli, da imajo stranke stalno ali ad hoc, kjer je to primerno, in po ustreznih kanalih (npr. letakih, spletnih straneh) na voljo točna in preprosta navodila z obrazložitvijo njihovih odgovornosti v zvezi z varno uporabo storitve.

Močna avtentikacija strank

NP 6: [kartice] Spletni trgovci bi lahko podprli močno avtentikacijo imetnikov kartice, ki bi jo izvajal izdajatelj pri spletnih kartičnih transakcijah.

NP 7: Ponudniki plačilnih storitev bi lahko zaradi strank razmislili o uporabi enotnega orodja za močno avtentikacijo strank za vse spletne plačilne storitve. To bi lahko povečalo sprejetost te rešitve med strankami in olajšalo pravilno uporabo.

NP 8: Močna avtentikacija stranke bi lahko vključevala elemente, ki povezujejo avtentikacijo z določenim zneskom in prejemnikom plačila. To bi strankam lahko zagotovilo večjo gotovost pri odobravanju plačil. Tehnološka rešitev, ki omogoča povezavo med podatki za

močno avtentikacijo in podatki o transakciji, bi morala biti odporna proti nedovoljenemu spreminjanju.

Zaščita občutljivih podatkov o plačilih

NP 9: Zaželeno je, da spletni trgovci, ki obravnavajo občutljive podatke o plačilih, ustrezno usposobijo svoje osebje, ki upravlja z goljufijami, in to usposabljanje redno posodabljajo, da je vsebina vedno usklajena z dinamičnim varnostnim okoljem.

Izobraževanje in obveščanje strank

NP 10: Zaželeno je, da ponudniki plačilnih storitev, ki ponujajo storitve pridobivanja, pripravijo izobraževalne programe za svoje spletne trgovce o preprečevanju goljufij.

Obvestila, določanje omejitev

NP 11: Ponudniki plačilnih storitev bi lahko v okviru določenih omejitev zagotovili svojim strankam možnost upravljanja omejitev za spletne plačilne storitve v varnem in zanesljivem okolju.

NP 12: Ponudniki plačilnih storitev bi stranke lahko opozarjali, na primer prek telefonskih klicev ali kratkih sporočil, pri sumljivih ali zelo tveganih plačilnih transakcijah na podlagi svojih politik upravljanja tveganj.

NP 13: Ponudniki plačilnih storitev bi lahko strankam omogočili, da določajo splošna, osebna pravila kot parametre za svoje ravnanje v zvezi s spletnimi plačili in podobnimi storitvami, npr. odrejanje plačil samo iz določenih držav in blokiranje plačil, ki bi se izvajala od drugod, ali možnost vnašanja določenih prejemnikov na bele ali črne sezname.