EBA/GL/2014/12_Rev1

19 december 2014

Definitieve richtsnoeren

met betrekking tot de veiligheid van internetbetalingen

Inhoud

Richtsnoeren met betrekking tot de veiligheid van internetbetalingen

Status van deze richtsnoeren

Dit document bevat richtsnoeren die zijn uitgevaardigd op grond van artikel 16 van Verordening (EU) nr. 1093/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Bankautoriteit), tot wijziging van Besluit nr. 716/2009/EG en tot intrekking van Besluit 2009/78/EG van de Commissie ('de EBA-verordening'). Overeenkomstig artikel 16, lid 3, van de EBA-verordening moeten bevoegde autoriteiten en financiële instellingen zich tot het uiterste inspannen om aan de richtsnoeren te voldoen.

In de richtsnoeren wordt aangegeven welke toezichtpraktijken binnen het Europees Systeem voor financieel toezicht naar de mening van EBA passend zijn, of hoe het EU-recht op een specifiek gebied moet worden toegepast. EBA verwacht dan ook van alle bevoegde autoriteiten en financiële instellingen tot wie de richtsnoeren zijn gericht, dat zij hieraan voldoen door ze op passende wijze in hun toezichtpraktijk te integreren (bijvoorbeeld door hun wettelijk kader of toezichtprocessen aan te passen), ook wanneer de richtsnoeren in de eerste plaats tot instellingen zijn gericht.

Kennisgevingsverplichtingen

Overeenkomstig artikel 16, lid 3, van de EBA-verordening moeten de bevoegde autoriteiten uiterlijk op 5 mei 2015 aan EBA kenbaar maken of zij aan deze richtsnoeren voldoen of voornemens deze op te volgen, dan wel aangeven waarom zij hier niet aan voldoen of niet voornemens zijn deze op te volgen. Bij gebreke van kennisgeving binnen deze termijn worden bevoegde autoriteiten door EBA geacht niet aan de richtsnoeren te hebben voldaan. De kennisgevingen moeten worden ingediend door het hiervoor bedoelde formulier, dat te vinden is in hoofdstuk 5, te versturen naar compliance@eba.europa.eu onder vermelding van referentienummer 'EBA/GL/2014/12'. De kennisgevingen dienen te worden ingezonden door personen die gemachtigd zijn om namens hun bevoegde autoriteit mee te delen of deze al dan niet aan de richtsnoeren voldoet.

Overeenkomstig artikel 16, lid 3, zullen de kennisgevingen op de website van EBA worden bekendgemaakt.

Titel 1 - Toepassingsgebied en definities

Toepassingsgebied

1. Deze richtsnoeren stellen de minimale vereisten vast op het gebied van veiligheid van internetbetalingen. De richtsnoeren zijn gebaseerd op de regels van Richtlijn 2007/64/EG[1] (Richtlijn betalingsdiensten of RBD) met betrekking tot de informatievereisten voor betalingsdiensten en verplichtingen van betalingsdienstaanbieders met betrekking tot de verlening van betalingsdiensten. Bovendien wordt op grond van artikel 10, lid 4, van de Richtlijn vereist dat de betalingsinstellingen over solide governancesystemen en adequate interne beheersmaatregelen beschikken.

2. De richtsnoeren hebben betrekking op de verlening van betalingsdiensten die via het internet worden aangeboden door betalingsdienstaanbieders zoals omschreven in artikel 1 van die Richtlijn.

3. De richtsnoeren zijn gericht aan financiële instellingen zoals omschreven in artikel 4, lid 1, van Verordening (EU) nr. 1093/2010 en aan bevoegde autoriteiten zoals omschreven in artikel 4, lid 2, van Verordening (EU) nr. 1093/2010. De bevoegde autoriteiten in de 28 lidstaten van de Europese Unie moeten garanderen dat onder hun toezicht deze richtsnoeren door de betalingsdienstaanbieders worden toegepast, zoals omschreven in artikel 1 van de RBD.

4. Daarnaast kunnen de bevoegde autoriteiten besluiten dat de betalingsdienstaanbieders aan de bevoegde autoriteit moeten rapporteren dat ze voldoen aan de richtsnoeren.

5. Deze richtsnoeren hebben geen gevolg voor de rechtsgeldigheid van de „Recommendations for the security of internet payments" van de Europese Centrale Bank (het Verslag).[2] Het Verslag blijft vooral het document op grond waarvan centrale banken in het kader van hun oversightfunctie voor betalingssystemen en -instrumenten de naleving moeten beoordelen met betrekking tot de veiligheid van internetbetalingen.

6. De richtsnoeren vormen minimale verwachtingen. Zij doen geen afbreuk aan de verantwoordelijkheid van betalingsdienstaanbieders om de risico's met betrekking tot het betalingsverkeer te monitoren en te beoordelen, hun eigen gedetailleerde veiligheidsbeleid te ontwikkelen en adequate veiligheidsmaatregelen, noodplannen, incidentbeheer en bedrijfscontinuïteitsmaatregelen in te voeren, die in proportie zijn met de risico's van de verleende betalingsdiensten.

[1] Richtlijn 2007/64/EG van het Europees Parlement en de Raad van 13 november 2007 betreffende betalingsdiensten in de interne markt tot wijziging van de Richtlijnen 97/7/EG, 2002/65/EG, 2005/60/EG en 2006/48/EG, en tot intrekking van Richtlijn 97/5/EG; PB L 319 van 5.12.2007,

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

7. Het doel van de richtsnoeren is om de minimale vereisten voor internetbetalingsdiensten vast te stellen, zoals hieronder vermeld, ongeacht welk toegangsapparaat hiervoor wordt gebruikt:

    - [kaarten] de uitvoering van kaartbetalingen via internet, inclusief virtuele kaartbetalingen, en de registratie van kaartbetalingsgegevens om te gebruiken voor „toepassingen voor een elektronische portemonnee";

    - [overschrijvingen] de uitvoering van overmakingen via internet;

    - [elektronische machtiging] de uitgifte en wijziging van machtigingen voor automatische afschrijvingen;

    - [elektronisch geld] overschrijvingen van elektronisch geld tussen twee elektronischgeldrekeningen via internet.

8. Als de richtsnoeren naar een uitkomst verwijzen, kan deze uitkomst op verschillende manieren bereikt worden. Deze richtsnoeren, in aanvulling op de volgende vereisten, bieden ook voorbeelden van goede praktijken (in bijlage 1). Betalingsdienstaanbieders worden niet verplicht, maar wel aangespoord deze na te leven.

9. Wanneer de verlening van betalingsdiensten en de levering van -instrumenten worden aangeboden via een betalingssysteem (bv. betaalkaartsystemen, betalingsschema's voor overmakingen en automatische afschrijvingen, enz.) dienen de bevoegde autoriteiten en de desbetreffende centrale bank belast met het toezicht op de betalingsinstrumenten, samen te werken om een consequente toepassing van de richtsnoeren door de deelnemers die verantwoordelijk zijn voor de werking van de regeling, te waarborgen.

10. Betalingsintegratoren[3] die betalingsinitiatiediensten aanbieden, worden beschouwd als acquirers van internetbetalingsdiensten (en dus als betalingsdienstaanbieders) of als externe aanbieders van technische diensten van de desbetreffende regelingen of betalingsdiensten. In het laatste geval zijn de betalingsintegratoren contractueel vereist om aan de richtsnoeren te voldoen.

11. Het volgende valt niet onder het toepassingsgebied van de richtsnoeren:

    - andere internetdiensten verleend door een betalingsdienstaanbieder via zijn betalingswebsite (bv. elektronische bemiddeling, online contracten);

    - betalingen waarvan de opdracht is gegeven per post, telefonische opdracht, voicemail of een technologie gebaseerd op sms;

    - mobiele betalingen anders dan betalingen via een browser;

[3] Betalingsintegratoren bieden de begunstigde (d.w.z. de webwinkel) een gestandaardiseerde interface voor betalingsinitiatiediensten geleverd door betalingsdienstaanbieders.

- overmakingen waarbij een derde partij toegang heeft tot de betaalrekening van de klant;

- betalingstransacties, uitgevoerd door een onderneming via specifieke netwerken;

- kaartbetalingen die gebruikmaken van anonieme en niet-herlaadbare fysieke of virtuele prepaidkaarten, waarbij geen verdere relatie is tussen de uitgever en de kaarthouder;

- clearing en afwikkeling van betalingstransacties.

Definities

12. Ten behoeve van deze richtsnoeren, en in aanvulling op de definities die geboden zijn in de RBD, zijn de volgende definities van toepassing:

- „authenticatie”: een procedure die de betalingsdienstaanbieder in staat stelt de identiteit van de klant te controleren;

- „sterke authenticatie van de klant”: een procedure die ten behoeve van deze richtsnoeren gebaseerd is op het gebruik van twee of meer van de volgende elementen - ingedeeld als kennis, eigendom en inherentie: i) iets dat alleen de gebruiker weet, bv. een statisch wachtwoord, code of persoonlijk identificatienummer; ii) iets dat alleen de gebruiker bezit, bv. een token, smartcard of mobiele telefoon; iii) iets dat de gebruiker is, bv. een biometrisch kenmerk, zoals een vingerafdruk. Daarnaast moeten de geselecteerde elementen van elkaar onafhankelijk zijn, d.w.z. de schending van één element mag de andere elementen/het andere element niet beïnvloeden. Ten minste een van de elementen dient niet-herbruikbaar en niet-reproduceerbaar te zijn (met uitzondering van inherentie), en het mag niet heimelijk via internet gestolen kunnen worden. Het ontwerp van de procedure voor sterke authenticatie moet de vertrouwelijkheid van de authenticatiegegevens beschermen;

- „autorisatie”: een procedure die controleert of de klant of de betalingsdienstaanbieder het recht heeft om een bepaalde actie uit te voeren, bv. het recht om geld over te schrijven, of toegang te hebben tot gevoelige gegevens;

- „gebruikersgegevens”: de informatie, in het algemeen vertrouwelijk, die verstrekt wordt door een klant of een betalingsdienstaanbieder voor de authenticatie. De gebruikersgegevens kunnen ook het bezit betekenen van een fysiek apparaat met daarop de informatie (bv. een generator voor een eenmalig wachtwoord, smartcard), of iets dat de gebruiker zich herinnert of vertegenwoordigt (zoals biometrische kenmerken);

- „belangrijk betalingsveiligheidsincident”: een incident dat een wezenlijk effect heeft of kan hebben op de veiligheid, integriteit of continuïteit van de betalingsgerelateerde

systemen van de betalingsdienstaanbieder, en/of de veiligheid van gevoelige betalingsgegevens of -middelen. Bij de beoordeling of iets wezenlijk is of niet, dient het aantal mogelijk getroffen klanten in ogenschouw worden genomen, evenals het effect op andere betalingsdienstaanbieders of andere betalingsinfrastructuren;

- „risicoanalyse van transacties”: het evalueren van het risico met betrekking tot een specifieke transactie, rekening houdend met criteria zoals betalingspatroon van de klant (gedrag), waarde van de desbetreffende transactie, producttype en profiel van de begunstigde.

- „virtuele kaart”: een betalingsoplossing op basis van een kaart, waarbij een alternatief, tijdelijk kaartnummer met een verkorte geldigheidstermijn, een beperkt gebruik en een vastgesteld bestedingslimiet wordt gegenereerd, dat gebruikt kan worden voor internetaankopen;

- „toepassingen voor een elektronische portemonnee”: een toepassing waarbij een klant gegevens registreert met betrekking tot een of meer betalingsinstrumenten, voor het maken van betalingen bij verschillende webwinkels.

Titel II - Richtsnoeren met betrekking tot de veiligheid van internetbetalingen

Algemene beheers- en veiligheidsomgeving

Governance

1. Betalingsdienstaanbieders dienen een formeel veiligheidsbeleid voor betalingsdiensten per internet in te voeren en dit regelmatig te evalueren.

   1.1 Het veiligheidsbeleid dient op de juiste manier te worden gedocumenteerd en regelmatig te worden geëvalueerd (overeenkomstig richtsnoer 2.4) en goedgekeurd door het hoger management. Het moet de veiligheidsdoelstellingen en de aanvaardbare risico's vaststellen.

   1.2 Het veiligheidsbeleid moet de taken .en verantwoordelijkheden vaststellen, met inbegrip van de risicobeheersfunctie met een rechtstreekse verantwoording aan het bestuur, en de rapportagelijnen voor de geleverde internetbetalingsdiensten, inclusief het beheer van gevoelige betalingsgegevens met betrekking tot beoordeling, beheersing en beperking van risico's.

Risicobeoordeling

2. Betalingsdienstaanbieders moeten nauwkeurige risicobeoordelingen uitvoeren en documenteren met betrekking tot de veiligheid van internetbetalingen en gerelateerde diensten, zowel vóór het instellen van de dienst(en) als regelmatig daarna.

   2.1 Betalingsdienstaanbieders moeten gedetailleerde risicobeoordelingen voor internetbetalingen en gerelateerde diensten uitvoeren en documenteren, door middel van hun risicobeheersfunctie. Betalingsdienstaanbieders moeten de resultaten van het voortdurend monitoren van de veiligheidsdreigingen met betrekking tot de internetbetalingsdiensten die zij aanbieden of van plan zijn aan te bieden, beoordelen, rekening houdend met: i) de gebruikte technologie, ii) diensten die uitbesteed zijn aan externe aanbieders en, iii) de technische omgeving van de klant. Betalingsdienstaanbieders moeten de risico's beoordelen, die verband houden met de gekozen technologieplatforms, architectuur van de toepassingen, programmeertechnieken en routines zowel aan hun kant[4] als aan de kant van de klanten [5], alsmede de resultaten van het proces voor de monitoring van veiligheidsincidenten (zie richtsnoer 3).

[4] Zoals de kwetsbaarheid van het systeem voor het kapen van een betalingssessie, SQL-injectie, cross-site scripting, bufferoverloop enz.

[5] Zoals risico's die samenhangen met het gebruik van multimedia-toepassingen, invoegtoepassingen voor de browser (plug-ins), kaders, externe verbindingen enz.

2.2 Op grond hiervan moeten betalingsdienstaanbieders bepalen of en in welke mate wijzigingen nodig kunnen zijn voor de bestaande veiligheidsmaatregelen, de gebruikte technologieën en de procedures of de aangeboden diensten. Betalingsdienstaanbieders moeten rekening houden met de tijd die nodig is om veranderingen in te voeren (inclusief de uitrol naar de klant) en de benodigde tijdelijke maatregelen nemen om de kans op veiligheidsrisico's en fraude en de kans op mogelijke verstorende effecten te beperken.

2.3 De risicobeoordeling moet de noodzaak van het beschermen en beveiligen van gevoelige betalingsgegevens betreffen.

2.4 Betalingsdienstaanbieders moeten de risicoscenario's en bestaande veiligheidsmaatregelen evalueren na grote incidenten die hun diensten hebben getroffen, voordat er een grote verandering aan de infrastructuur of procedures wordt aangebracht, en zodra nieuwe dreigingen zijn vastgesteld door het monitoren van risico's. Daarnaast moet er ten minste één keer per jaar een algemene evaluatie van de risicobeoordeling worden uitgevoerd. De resultaten van de risicobeoordelingen en -evaluaties moeten aan het hoger management ter goedkeuring worden voorgelegd.

Monitoren en rapportage van incidenten

3. Betalingsdienstaanbieders moeten veiligheidsincidenten, inclusief klachten van klanten met betrekking tot de veiligheid, consequent en integraal monitoren, afhandelen en opvolgen. Betalingsdienstaanbieders moeten een procedure vaststellen voor het rapporteren van dergelijke incidenten aan het management en, in het geval van grote incidenten op het gebied van betalingsveiligheid, de bevoegde autoriteiten.

3.1 Betalingsdienstaanbieders moeten over een proces beschikken voor het monitoren, afhandelen en opvolgen van veiligheidsincidenten en klachten van klanten met betrekking tot de veiligheid, en deze incidenten rapporteren aan het management.

3.2 Betalingsdienstaanbieders moeten een procedure hebben voor het onmiddellijk inlichten van de bevoegde autoriteiten (d.w.z. toezichthouders en gegevensbeschermingsautoriteiten), voor zover deze bestaan, in het geval van grote betalingsveiligheidsincidenten met betrekking tot de geleverde betalingsdiensten.

3.3 Betalingsdienstaanbieders moeten een procedure hebben voor samenwerking met de betrokken wetshandhavingsinstanties in het geval van betalingsveiligheidsincidenten, inclusief inbreuk op gegevens.

3.4 Acquiring betalingsdienstaanbieders moeten contractueel eisen dat webwinkeliers die gevoelige betalingsgegevens opslaan, verwerken of overdragen, in het geval van grote betalingsveiligheidsincidenten, inclusief inbreuk op gegevens, samenwerken met zowel henzelf als de betrokken wetshandhavingsinstanties. Als een betalingsdienstaanbieder ontdekt dat een webwinkelier niet meewerkt zoals vereist op grond van het contract,

moet deze stappen ondernemen om de contractuele verplichting af te dwingen, of het contract beëindigen.

Risicobeheersing en -inperking

4. Betalingsdienstaanbieders moeten veiligheidsmaatregelen invoeren die overeenstemmen met hun veiligheidsbeleid om vastgestelde risico's te beperken. Deze maatregelen moeten verschillende lagen van veiligheidsbescherming bevatten; als een verdedigingslinie faalt, moet dit opgevangen worden door een volgende verdedigingslinie („verdediging in de diepte").

4.1 De betalingsdienstaanbieders moeten bij het ontwerpen, ontwikkelen en onderhouden van internetbetalingsdiensten extra aandacht schenken aan een adequate scheiding van taken in informatietechnologieomgevingen (IT) (bv. de ontwikkel-, test- en productieomgevingen) en de correcte implementatie van het „least privilege"-beginsel (minimale toegangsrechten) als basis voor een deugdelijk identiteitsbeheersysteem en toegangsbeheersysteem.[6]

4.2 Betalingsdienstaanbieders moeten geschikte veiligheidsoplossingen hebben om netwerken, websites, servers en communicatieverbindingen te beschermen tegen misbruik of aanvallen. Betalingsdienstaanbieders zullen de servers ontdoen van alle overbodige functies om deze te beschermen (te wapenen) en de kwetsbaarheid van risicotoepassingen uit te sluiten of te verminderen. Toegang door de verschillende toepassingen tot de gegevens en benodigde bronnen dienen tot een minimum beperkt te worden overeenkomstig het „least privilege"-beginsel. Om het gebruik van „valse" websites te beperken (imitatie van een echte website van een betalingsdienstaanbieder), moeten transactionele websites die internetbetalingsdiensten aanbieden, identificeerbaar zijn door middel van uitgebreide geldigheidscertificaten, opgemaakt in naam van de betalingsdienstaanbieder of door andere gelijksoortige authenticatiemethoden.

4.3 Betalingsdienstaanbieders moeten over de juiste processen beschikken om de toegang te monitoren, te volgen en te beperken tot: i) gevoelige betalingsgegevens en ii) logische en fysieke kritieke middelen, zoals netwerken, systemen, gegevensbestanden, veiligheidsmodules enz. Betalingsdienstaanbieders moeten de juiste logboeken en controlesporen maken, opslaan en analyseren.

4.4 De betalingsdienstaanbieders moeten bij het ontwerpen,[7] ontwikkelen en onderhouden van de internetbetalingsdiensten ervoor zorgen dat minimalisatie van de

[6] „Elk programma en elke gemachtigde gebruiker van het systeem moet zo min mogelijk machtigingen hebben om het werk te doen." Zie Saltzer, J.H. (1974), „Protection and the Control of Information Sharing in Multics", Communications of the ACM, Vol. 17, Nr. 7, blz. 388.

[7] „Privacy by design".

gegevens[8] een essentieel onderdeel is van de kernfunctionaliteit: het verzamelen, routeren, verwerken, opslaan en/of archiveren, en visualiseren van de gevoelige betalingsgegevens moeten tot een absoluut minimum beperkt worden.

4.5 Veiligheidsmaatregelen voor internetbetalingsdiensten moeten worden getest onder toezicht van de risicobeheersfunctie die de deugdelijkheid en doeltreffendheid garandeert. Alle veranderingen moeten onderhevig zijn aan beheersprocessen die waarborgen dat de veranderingen op de juiste manier gepland, getest, gedocumenteerd en geautoriseerd worden. Op basis van de gemaakte veranderingen en de geobserveerde veiligheidsdreigingen, moeten de testen regelmatig herhaald worden en scenario's bevatten met relevante en bekende, mogelijke aanvallen.

4.6 De veiligheidsmaatregelen van de betalingsdienstaanbieder voor internetbetalingsdiensten moeten periodiek worden geverifieerd om hun deugdelijkheid en doeltreffendheid te garanderen. De invoering en het functioneren van internetbetalingsdiensten moeten ook worden geverifieerd. De frequentie en het aandachtspunt van deze controles moeten rekening houden met, en in verhouding staan tot, de betrokken veiligheidsrisico's. Betrouwbare en onafhankelijke (interne of externe) experts moeten deze controles uitvoeren. Deze zullen op geen enkele wijze betrokken zijn bij de ontwikkeling, de implementatie of het operationeel beheer van de geleverde internetbetalingsdiensten.

4.7 Wanneer betalingsdienstaanbieders functies met betrekking tot de veiligheid van internetbetalingsdiensten uitbesteden, moet het contract voorzieningen bevatten die overeenkomen met de principes en richtsnoeren, die zijn uiteengezet in deze richtsnoeren.

4.8 Betalingsdienstaanbieders die acquiringdiensten aanbieden, moeten contractueel eisen dat webwinkeliers die handelingen uitvoeren met gevoelige betalingsgegevens (zoals opslag, verwerken of overmaken), veiligheidsmaatregelen implementeren in hun IT-infrastructuur, overeenkomstig de richtsnoeren 4.1 tot 4.7, teneinde diefstal van deze gevoelige betalingsgegevens via hun systemen te voorkomen. Als een betalingsdienstaanbieder ontdekt dat een webwinkelier niet de vereiste veiligheidsmaatregelen heeft genomen, moet deze stappen ondernemen om de contractuele verplichting af te dwingen, of het contract beëindigen.

Traceerbaarheid

5. Betalingsdienstaanbieders moeten over processen beschikken om te waarborgen dat alle transacties en het stroomschema van de elektronische machtiging, op de juiste manier gevolgd worden.

[8] Minimalisering van gegevens betreft het beleid om zo min mogelijk persoonsgegevens te verzamelen die nodig zijn om een bepaalde functie uit te voeren.

5.1 Betalingsdienstaanbieders moeten waarborgen dat hun dienst veiligheidsmechanismes bevat voor het gedetailleerd bijhouden van transactiegegevens en gegevens van elektronische machtigingen, inclusief het volgnummer van de transactie, tijdstempels voor transactiegegevens, wijzigingen van parameters en toegang tot de transactiegegevens en gegevens van de elektronische machtiging.

5.2 Betalingsdienstaanbieders moeten logbestanden invoeren die alle aanvullingen, veranderingen of verwijderingen van transactiegegevens en elektronische machtigingsgegevens bijhouden.

5.3 Betalingsdienstaanbieders moeten de transactiegegevens en elektronische machtigingsgegevens bekijken en analyseren, en waarborgen dat ze de juiste middelen hebben om deze logbestanden te evalueren. Deze toepassingen mogen alleen beschikbaar zijn voor bevoegde medewerkers.

Specifieke beheers- en veiligheidsmaatregelen voor internetbetalingen

Eerste identificatie van de klant, informatie

6. Klanten moeten op de juiste manier geïdentificeerd worden in overeenstemming met de Europese antiwitwaswetgeving[9], en hun bereidheid bevestigen om internetbetalingen te maken met gebruik van de diensten, voordat ze toegang krijgen tot dergelijke diensten. Betalingsdienstaanbieders moeten adequaat „eerdere", „periodieke" of, indien van toepassing, „ad-hocinformatie" verstrekken aan de klant over de noodzakelijke vereisten (bv. benodigdheden, procedures) voor het uitvoeren van veilige betalingstransacties via internet en de inherente risico's.

6.1 Betalingsdienstaanbieders moeten garanderen dat de klant de klantenonderzoeksprocedures heeft gevolgd, en de adequate identiteitsdocumenten[10] en gerelateerde informatie heeft verstrekt, voordat deze toegang heeft gekregen tot de internetbetalingsdiensten.[11]

[9] Zie bv. Richtlijn 2005/60/EG van het Europees Parlement en de Raad van 26 oktober 2005 tot voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld en de financiering van terrorisme. PB L 309 van 25.11.2005, blz. 15-36. Zie ook Richtlijn 2006/70/EG van de Commissie van 1 augustus 2006 tot vaststelling van uitvoeringsmaatregelen van Richtlijn 2005/60/EG van het Europees Parlement en de Raad wat betreft de definitie van politiek prominente personen en wat betreft de technische criteria voor vereenvoudigde klantenonderzoeksprocedures en voor vrijstellingen op grond van occasionele of zeer beperkte financiële activiteiten. PB L 214 van 4.8.2006, blz. 29-34.

[10] Bv. paspoort, nationale identiteitskaart of geavanceerde elektronische handtekening.

[11] Het identificatieproces van de klant is behoudens enkele uitzonderingen vastgelegd in de bestaande antiwitwaswetgeving. Betalingsdienstaanbieders hoeven geen apart identificatieproces van de klant uit te voeren voor internetbetalingsdiensten, indien een dergelijke identificatie van de klant al is uitgevoerd, bv. voor bestaande betalingsgerelateerde diensten of voor het openen van een rekening.

6.2 Betalingsdienstaanbieders moeten garanderen dat de eerdere informatie[12] die aan de klanten is verstrekt, specifieke details bevat met betrekking tot internetbetalingsdiensten. Deze moeten, voor zover van toepassing, het volgende omvatten:

- duidelijke informatie over alle vereisten met betrekking tot de benodigdheden van de klant, software of andere benodigde hulpmiddelen (bv. antivirussoftware, firewalls);
- richtsnoeren voor het juiste en veilige gebruik van gepersonaliseerde veiligheidskenmerken;
- een procedure voor de klant, waarin stap voor stap beschreven staat hoe een betalingstransactie moet worden uitgevoerd en geautoriseerd, en/of hoe informatie moet worden verkregen, met inbegrip van de gevolgen van elke actie;
- richtsnoeren voor het juiste en veilige gebruik van alle hardware en software die aan de klant verstrekt zijn;
- de te volgen procedures in het geval van verlies of diefstal van de gepersonaliseerde veiligheidskenmerken, of van de hardware of software van de klant om in te loggen of transacties uit te voeren;
- de te volgen procedures wanneer misbruik wordt ontdekt of vermoed;
- een beschrijving van de verantwoordelijkheden en aansprakelijkheden van respectievelijk de betalingsdienstaanbieder en de klant met betrekking tot het gebruik van de internetbetalingsdiensten.

6.3 Betalingsdienstaanbieders moeten waarborgen dat in de raamcontracten met de klant vermeld staat dat de betalingsdienstaanbieder een specifieke transactie of het betalingsinstrument mag blokkeren[13] omwille van veiligheidsredenen. Het contract moet de methoden en voorwaarden uiteenzetten hoe de klant geïnformeerd wordt en hoe de klant contact kan opnemen met de betalingsdienstaanbieder om de internetbetalingstransactie of dienst „gedeblokkeerd" te krijgen, zulks in overeenstemming met de RBD.

[12] Deze informatie is een aanvulling op artikel 42 van de RBD, waarin de informatie wordt gespecificeerd die de betalingsdienstaanbieder moet aanbieden aan de gebruiker van de betalingsdienst voordat de gebruiker een contract voor de verlening van betalingsdiensten aangaat.

[13] Zie artikel 55 van de RBD inzake restricties op het gebruik van het betaalinstrument.

Sterke authenticatie van de klant

7. Het initiëren van internetbetalingen en de toegang tot gevoelige betalingsgegevens moeten beschermd worden door een sterke authenticatie van de klant. Betalingsdienstaanbieders moeten een procedure hebben voor een sterke authenticatie van de klant, in overeenstemming met de definitie in deze richtsnoeren.

7.1 [Overmakingen/elektronische machtiging/elektronisch geld] Betalingsdienstaanbieders moeten een sterke authenticatie van de klant verrichten ten behoeve van de autorisatie door de klant van internetbetalingstransacties (inclusief gebundelde overmakingen) en de uitgifte of wijziging van machtigingen voor automatische afschrijvingen. Betalingsdienstaanbieders moeten echter voor het volgende ook overwegen om alternatieve maatregelen voor de authenticatie van de klant in te voeren:

- uitgaande betalingen naar betrouwbare begunstigden die op eerdere witte lijsten van die klant vermeld staan;
- transacties tussen twee rekeningen van dezelfde klant bij dezelfde betalingsdienstaanbieder;
- overschrijvingen binnen dezelfde betalingsdienstaanbieder, gerechtvaardigd door een risicoanalyse van de transactie;
- betalingen van kleine bedragen, zoals vermeld in de RBD.[14]

7.2 Het verkrijgen van toegang tot of het wijzigen van gevoelige betalingsgegevens (inclusief het maken en wijzigen van witte lijsten) vereisen sterke authenticatie van de klant. Als een betalingsdienstaanbieder slechts adviesdiensten verleent, zonder inzage in gevoelige informatie van klanten of betalingsinformatie, zoals betaalkaartgegevens, die eenvoudig misbruikt kunnen worden om fraude te plegen, kan de betalingsdienstaanbieder de eisen voor authenticatie baseren op zijn risicobeoordeling.

7.3 [kaarten] Alle betalingsdienstaanbieders die kaarten uitgeven, moeten sterke authenticatie van de kaarthouder ondersteunen voor kaarttransacties. Alle uitgegeven kaarten moeten technisch in staat zijn (geregistreerd) om gebruikt te worden met sterke authenticatie.

7.4 [kaarten] Betalingsdienstaanbieders die acquiringdiensten aanbieden, moeten technologieën ondersteunen die de uitgever in staat stelt om sterke authenticatie van

[14] Zie de definitie voor instrumenten voor betalingen van een lage waarde in artikel 34, lid 1, en artikel 53, lid 1, van de RBD.

de kaarthouder uit te voeren voor betaalkaartsystemen waaraan de acquirer deelneemt.

7.5 [kaarten] Betalingsdienstaanbieders die acquiringdiensten aanbieden, moeten van de webwinkeliers eisen dat zij toepassingen ondersteunen die de uitgever in staat stelt om sterke authenticatie van de kaarthouder uit te voeren voor kaarttransacties via het internet. Het gebruik van alternatieve maatregelen voor authenticatie kan in aanmerking genomen worden voor vooropgestelde categorieën van transacties met een klein risico, bv. gebaseerd op risicoanalyse van een transactie, of met betrekking tot betalingen van kleine bedragen, zoals vermeld in de RBD.

7.6 [kaarten] Voor betaalkaartsystemen die door de dienst geaccepteerd worden, moeten de aanbieders van toepassingen voor een elektronische portemonnee sterke authenticatie vereisen door de uitgever, op het moment dat de rechtmatige houder voor het eerst de kaartgegevens registreert.

7.7 Aanbieders van toepassingen voor een elektronische portemonnee moeten sterke authenticatie van de klant ondersteunen wanneer klanten inloggen voor de betalingsdiensten van de elektronische portemonnee of bij het uitvoeren van kaarttransacties via het internet. Het gebruik van alternatieve maatregelen voor authenticatie kunnen in aanmerking genomen worden voor vooropgestelde categorieën van transacties met een klein risico, bv. gebaseerd op risicoanalyse van een transactie, of met betrekking tot betalingen van kleine bedragen, zoals vermeld in de RBD.

7.8 [kaarten] Voor virtuele kaarten moet de eerste registratie plaatsvinden in een veilige en betrouwbare omgeving.[15] Als de kaart wordt uitgegeven via internet, moet sterke authenticatie van de klant vereist zijn voor het proces van genereren van virtuele kaartgegevens.

7.9 Betalingsdienstaanbieders moeten de juiste bilaterale authenticatie waarborgen wanneer er gecommuniceerd wordt met webwinkels bij het initiëren van internetbetalingen en wanneer er toegang verkregen wordt tot gevoelige betalingsgegevens.

[15] Omgevingen waarvoor de betalingsdienstaanbieder verantwoordelijk is, waar adequate authenticatie van de klant en van de betalingsdienstaanbieder en de bescherming van vertrouwelijke/gevoelige informatie worden verzekerd, zijn onder meer i) de gebouwen van de betalingsdienstaanbieder; ii) internetbankieren of andere veilige websites, bv. waar de GA vergelijkbare veiligheidskenmerken aanbiedt, zoals onder andere gedefinieerd in richtsnoer 4; of iii) diensten voor geldautomaten. (In het geval van geldautomaten wordt sterke authenticatie van de klant vereist. Dergelijke authenticatie wordt normaal gesproken gedaan door een chip en een pincode, of een chip en biometrie).

Registratie en levering van middelen voor authenticatie en/of geleverde software aan de klant

8. Betalingsdienstaanbieders moeten waarborgen dat de registratie van de klant en de eerste levering van authenticatiemiddelen die nodig zijn om gebruik te maken van internetbetalingsdiensten en/of de levering van betalingsgerelateerde software aan klanten, op een veilige manier worden uitgevoerd.

8.1 Het registreren en het leveren van middelen voor authenticatie en/of betalingsgerelateerde software die aan klanten geleverd wordt, moeten aan de volgende eisen voldoen.

- De gerelateerde procedures moeten in een veilige en betrouwbare omgeving uitgevoerd worden, rekening houdend met mogelijke risico's in verband met apparaten die niet beheerst worden door de betalingsdienstaanbieder.

- Er moeten effectieve en veilige procedures zijn voor de levering van gepersonaliseerde veiligheidskenmerken, betalingsgerelateerde software en alle apparaten die betrekking hebben op internetbetalingen. Software die via het internet geleverd wordt, moet digitaal ondertekend worden door de betalingsdienstaanbieder, zodat de klant de echtheid kan verifiëren en kan zien dat er niet mee geknoeid is.

- [kaarten] De klant moet de mogelijkheid hebben om zich aan te melden voor sterke authenticatie bij kaarttransacties, onafhankelijk van een specifieke aankoop via internet. Als er tijdens het online winkelen registratie vereist is, moet dit gedaan worden aan de hand van het doorsturen van de klant naar een veilige en betrouwbare omgeving.

8.2 [kaarten] Uitgevers moeten kaarthouders aanmoedigen zich voor sterke authenticatie aan te melden en kaarthouders toestaan om registratie alleen in uitzonderlijke en een beperkt aantal gevallen te omzeilen, wanneer dit gerechtvaardigd is door het risico met betrekking tot die specifieke kaarttransactie.

Inlogpogingen, sessietime-out, geldigheid van de authenticatie

9. Betalingsdienstaanbieders moeten het aantal pogingen om in te loggen of zich te identificeren, beperken, regels vaststellen voor sessietime-out van internetbetalingsdiensten en tijdsbeperkingen voor het valideren van authenticatie invoeren.

9.1 Wanneer er een eenmalig wachtwoord gebruikt wordt voor authenticatiedoeleinden, moeten de betalingsdienstaanbieders waarborgen dat de geldigheidsperiode van dit wachtwoord beperkt wordt tot een strikt noodzakelijk minimum.

9.2 Betalingsdienstaanbieders moeten het maximum aantal foutieve inlogpogingen of authenticatiepogingen vaststellen, waarna de toegang tot de internetbetalingsdienst

(tijdelijk of permanent) geblokkeerd wordt. Zij moeten beschikken over een veilige procedure om geblokkeerde internetbetalingsdiensten te deblokkeren.

9.3 Betalingsdienstaanbieders moeten een maximumperiode vaststellen waarna inactieve internetbetalingsdiensten automatisch beëindigd worden.

Transactiemonitoring

10. Voor de uiteindelijke autorisatie van de betalingsdienstaanbieder moeten er mechanismen worden gehanteerd, die ontworpen zijn om frauduleuze betalingstransacties te voorkomen, te ontdekken en te blokkeren; verdachte transacties of transacties met een hoog risico moeten worden onderworpen aan een specifieke onderzoeks- en evaluatieprocedure. Er moet een soortgelijk, veilig monitoring- en autorisatiemechanisme zijn voor het uitgeven van elektronische machtigingen.

10.1 Betalingsdienstaanbieders moeten fraudedetectie- en preventiesystemen gebruiken om verdachte transacties te identificeren voordat de betalingsdienstaanbieder de transacties of elektronische machtigingen uiteindelijk goedkeurt. Deze systemen moeten gebaseerd worden op bijvoorbeeld regels op basis van parameters (zoals zwarte lijsten van verdachte of gestolen kaartgegevens) en het monitoren van abnormale gedragspatronen van de klant of van het invoerapparaat van de klant (zoals een verandering van IP-adres [16] of het IP-bereik tijdens de internetbetalingsdienstsessie, soms geïdentificeerd door IP-controles van de locatie,[17] atypische categorieën voor een bepaalde klant bij een webwinkel of abnormale transactiegegevens enz.). Dergelijke systemen moeten in staat zijn om signalen van malware-infectie in de sessie (bv. via een script versus menselijke validatie) en bekende frauduleuze scenario's te ontdekken. De omvang, de complexiteit en het aanpassingsvermogen van de controles, die in overeenstemming moeten zijn met de relevante gegevensbeschermingswetgeving, moeten gelijk zijn aan de uitkomst van de risicobeoordeling.

10.2 Aanbieders van acquiringdiensten moeten fraudedetectie- en preventiesystemen hebben om activiteiten van webwinkeliers te controleren.

10.3 Betalingsdienstaanbieders moeten binnen een bepaalde periode transacties onderzoeken en evalueren, zodat de initiatie en/of uitvoering van de betrokken betalingsdienst niet onnodig uitgesteld wordt.

10.4 Wanneer de betalingsdienstaanbieder op grond van diens zijn risicobeleid besluit een betalingstransactie die als mogelijk frauduleus wordt geïdentificeerd, te blokkeren, moet deze blokkade zo kort mogelijk zijn totdat de veiligheidsproblemen zijn opgelost.

[16] Een IP-adres is een uniek nummer dat elke computer die aan het internet verbonden is, identificeert.

[17] Een „Geo-IP-controle" verifieert of het land van uitgifte correspondeert met het IP-adres van de gebruiker die de transactie doet.

Bescherming van gevoelige betalingsgegevens

11. Gevoelige betalingsgegevens moeten bij de opslag, verwerking of overdracht worden beschermd.

11.1 Alle gegevens die gebruikt worden om klanten te identificeren en te authentiseren (bv. bij het inloggen, wanneer internetbetalingen geïnitieerd worden, en bij het uitgeven, veranderen of annuleren van elektronische machtigingen), alsmede bij de interface van de klant (website van een betalingsdienstaanbieder of webwinkel), moeten op de juiste manier beveiligd worden tegen diefstal en ongeautoriseerde toegang of modificatie.

11.2 Betalingsdienstaanbieders moeten garanderen dat wanneer er gevoelige betalingsgegevens worden uitgewisseld via het internet, tijdens de gehele communicatiesessie veilige end-to-endencryptie [18] wordt toegepast tussen de communicerende partijen, teneinde de vertrouwelijkheid en integriteit van de gegevens te waarborgen met behulp van sterke en algemeen erkende encryptietechnieken.

11.3 Betalingsdienstaanbieders die acquiringdiensten aanbieden moeten hun elektronische winkels aanmoedigen om geen gevoelige betalingsgegevens op te slaan. In het geval dat webwinkeliers gevoelige betalingsgegevens behandelen, bv. in de vorm van opslag, verwerking of overdracht, moeten de betalingsdienstaanbieders contractueel eisen dat de webwinkeliers de benodigde maatregelen hebben getroffen om deze gegevens te beschermen. Betalingsdienstaanbieders moeten regelmatig controles verrichten en zodra een betalingsdienstaanbieder ontdekt dat een webwinkelier die gevoelige betalingsgegevens behandelt, niet de vereiste veiligheidsmaatregelen heeft genomen, moet deze stappen ondernemen om de contractuele verplichting af te dwingen, of het contract beëindigen.

[18] End-to-end encryptie betreft versleuteling in of bij het eindsysteem van de bron, waarbij de overeenkomstige ontsleuteling alleen plaatsvindt in of bij het eindsysteem van bestemming. ETSI NL 302 109 V1.1.1. (2003-06).

Klantenbewustzijn, -educatie en -communicatie

12. Klanteneducatie en -communicatieBetalingsdienstaanbieders moeten waar nodig ondersteuning en hulp bieden aan klanten, met betrekking tot het veilige gebruik van internetbetalingsdiensten. Betalingsdienstaanbieders moeten zodanig met hun klanten communiceren, dat deze verzekerd zijn van de authenticiteit van de ontvangen berichten.

12.1 Betalingsdienstaanbieders moeten ten minste één beveiligd kanaal[19] aanbieden voor voortdurende communicatie met klanten met betrekking tot het juiste en veilige gebruik van de internetbetalingsdiensten. Betalingsdienstaanbieders moeten klanten op de hoogte brengen van dit kanaal en uitleggen dat elk bericht uit naam van de betalingsdienstaanbieder op wat voor andere manier dan ook, zoals e-mail, met betrekking tot het juiste en veilige gebruik van de internetbetalingsdienst, niet betrouwbaar is. De betalingsdienstaanbieder moet het volgende uitleggen:

- de manier waarop klanten (verdachte) frauduleuze betalingen, verdachte incidenten of afwijkingen tijdens de internetbetalingsdienst-sessies en/of mogelijke pogingen via social engineering[20] aan de betalingsdienstaanbieder kunnen rapporteren;

- de vervolgstappen, d.w.z. hoe de betalingsdienstaanbieder zal antwoorden op de melding van de klant;

- hoe de betalingsdienstaanbieder de klant zal informeren met betrekking tot (potentiële) frauduleuze transacties of niet-initiatie, of de klant waarschuwen over de aangetroffen aanvallen (bv. phishing e-mails).

12.2 De betalingsdienstaanbieders moeten de klanten via dit beveiligde kanaal informeren over wijzigingen in de veiligheidsprocedures met betrekking tot internetbetalingsdiensten. Alle alarmsignalen over belangrijke nieuwe risico's (bv. waarschuwingen over social engineering) moeten ook via het beveiligde kanaal worden verstrekt.

12.3 De betalingsdienstaanbieders moeten assistentie voor de klant beschikbaar stellen voor alle vragen, klachten, verzoeken tot ondersteuning en meldingen van afwijkingen of incidenten met betrekking tot internetbetalingen en gerelateerde diensten, en klanten moet op de juiste wijze geïnformeerd worden hoe deze assistentie verkregen kan worden.

[19] Zoals een specifiek postvak op de website van de betalingsdienstaanbieder of een veilige website.

[20] Social engineering verwijst in deze context naar technieken om mensen te manipuleren om informatie te verkrijgen (bv. via e-mail of telefoongesprekken), of het verkrijgen van informatie van sociale netwerken, met fraude als doel of het verkrijgen van ongeautoriseerde toegang tot een computer of een netwerk.

12.4 Betalingsdienstaanbieders moeten programma's starten voor voorlichting en bewustwording van de klant, die zodanig ontworpen zijn dat de klant in ieder geval goed doordrongen is van de noodzaak:

- om wachtwoorden, beveiligingstokens, persoonlijke gegevens en andere vertrouwelijke gegevens te beschermen;
- om op de juiste manier de beveiliging van het invoerapparaat (bv. computer) te beheren door het installeren en bijwerken van veiligheidscomponenten (antivirusprogramma's, firewalls, veiligheidspatches);
- om rekening te houden met de belangrijke dreigingen en risico's met betrekking tot het downloaden van software via het internet, als de klant er niet zeker van kan zijn dat de software authentiek is of dat er niet mee geknoeid is;
- om de juiste website voor internetbetalingen van de betalingsdienstaanbieder te gebruiken.

12.5 Betalingsdienstaanbieders die acquiringdiensten aanbieden moeten eisen dat webwinkeliers de betalingsgerelateerde processen duidelijk afscheiden van de webwinkel, zodat het gemakkelijker is voor klanten om na te gaan of ze communiceren met de betalingsdienstaanbieder en niet met de begunstigde (bv. door de klant door te sturen en een apart scherm te openen, zodat het betalingsproces niet getoond wordt in het venster van de webwinkel).

Berichten, instellen van limieten

13. Betalingsdienstaanbieders moeten limieten instellen voor internetbetalingsdiensten en mogelijkheden aan hun klanten bieden voor verdere risicobeperking binnen deze limieten. Ze kunnen mogelijk ook waarschuwingsdiensten en beheersdiensten voor klantenprofielen aanbieden.

13.1 Voorafgaand aan het aanbieden van internetbetalingsdiensten aan een klant, moeten betalingsdienstaanbieders limieten [21] instellen voor deze diensten (bv. een maximumbedrag voor elke individuele betaling, of een cumulatief bedrag over een bepaalde periode) en de klant hierover informeren. Betalingsdienstaanbieders moeten klanten toestaan om de internetbetalingsfunctionaliteit uit te schakelen.

[21] Dergelijke limieten kunnen algemeen van toepassing zijn (d.w.z. voor alle betalingsinstrumenten die internetbetalingen mogelijk maken) of individueel.

De klant moet toegang hebben tot de informatie met betrekking tot de status van de betalingsinitiatie en -uitvoering.

14. Betalingsdienstaanbieders moeten de betalingsinitiatie bevestigen aan de klant en de klant binnen een redelijke tijd voorzien van de informatie die nodig is om te controleren of een betalingstransactie op de juiste manier geïnitieerd en/of uitgevoerd is.

    14.1 [Overmaking/elektronische machtiging] Betalingsdienstaanbieders moeten de klanten de mogelijkheid bieden om bijna „real-time" de status van de uitvoering van de transacties en de rekeningsaldi op elk moment[22] te controleren in een veilige en betrouwbare omgeving.

    14.2 Alle gedetailleerde elektronische afschriften moeten beschikbaar gemaakt worden in een veilige en betrouwbare omgeving. In het geval betalingsdienstaanbieders via een alternatief kanaal, zoals SMS, e-mail of brief, klanten informeren over de beschikbaarheid van elektronische afschriften (bv. regelmatig wanneer een periodiek elektronische afschrift is uitgegeven, of op ad-hoc basis na de uitvoering van een transactie), mogen er in deze berichten nooit gevoelige betalingsgegevens worden vermeld of moeten deze gegevens, indien ze wel vermeld worden, afgeschermd worden.

Titel III – Definitieve bepalingen en uitvoering

15. Deze richtsnoeren zijn vanaf 01.08.2015 van toepassing.

[22] Behalve wanneer de faciliteit in uitzonderlijke gevallen niet beschikbaar is door technisch onderhoud, of door ernstige incidenten.

Bijlage 1: Voorbeelden van goede praktijken

In aanvulling op de bovengenoemde vereisten, beschrijven deze richtsnoeren enkele voorbeelden van goede praktijken. Betalingsdienstaanbieders en relevante marktdeelnemers worden aangemoedigd, maar niet verplicht, deze in te voeren. De hoofdstukken waar deze goede praktijken betrekking op hebben, worden voor referentiedoeleinden apart vermeld.

Algemene beheers en veiligheidsomgeving

Governance

Goede praktijk 1: Het veiligheidsbeleid kan vastgelegd worden in een specifiek document.

Risicobeheersing en -inperking

Goede praktijk 2: Betalingsdienstaanbieders kunnen veiligheidsmiddelen aanbieden (bv. apparaten en/of aangepaste browsers, die naar behoren zijn beveiligd) om de interface van de klant te beschermen tegen onwettig gebruik of aanvallen (bv. „man-in-the-browser”-aanvallen).

Traceerbaarheid

Goede praktijk 3: Betalingsdienstaanbieders die acquiringdiensten aanbieden, kunnen contractueel eisen dat elektronische winkels die betalingsinformatie opslaan, adequate processen hebben om de traceerbaarheid te ondersteunen.

Specifieke beheers- en veiligheidsmaatregelen voor internetbetalingen

Eerste identificatie van de klant, informatie

Goede praktijk 4: De klant kan een specifieke dienstverleningsovereenkomst afsluiten voor het uitvoeren van internetbetalingstransacties, in plaats van dat de voorwaarden deel uitmaken van een ruimere algemene dienstverleningsovereenkomst met de betalingsdienstaanbieder.

Goede praktijk 5: Betalingsdienstaanbieders kunnen waarborgen dat klanten op continue of, waar van toepassing, ad-hoc basis en via de juiste middelen (bv. brochures, websitepagina’s) worden voorzien van duidelijke en directe instructies over de verantwoordelijkheden met betrekking tot het veilig gebruik van de dienst.

Sterke authenticatie van de klant

Goede praktijk 6: [kaarten] Webwinkeliers kunnen sterke authenticatie van de kaarthouder door de uitgever van kaarttransacties via het internet ondersteunen.

Goede praktijk 7: Voor het gemak van de klant kunnen de betalingsdienstaanbieders overwegen om één instrument voor sterke authenticatie van de klant te gebruiken voor

alle internetbetalingsdiensten. Dit kan de acceptatie van de oplossing tussen klanten vergroten en een juist gebruik daarvan bevorderen.

Goede praktijk 8: Sterke authenticatie van de klant kan elementen bevatten die de authenticatie verbinden aan een specifiek bedrag en begunstigde. Dit biedt de klant verhoogde zekerheid bij het autoriseren van betalingen. Indien een technologieoplossing een koppeling tussen sterke authenticatiegegevens en transactiegegevens mogelijk maakt, moet dit resistent zijn tegen geknoei.

Bescherming van gevoelige betalingsgegevens

Goede praktijk 9: Het is wenselijk dat webwinkeliers die gevoelige betalingsgegevens verwerken, naar behoren hun medewerkers voor fraudebeheer trainen en deze training ook regelmatig bijwerken teneinde te waarborgen dat de inhoud relevant blijft voor een dynamische veiligheidsomgeving.

Klanteneducatie en -communicatie

Goede praktijk 10: Het is wenselijk dat betalingsdienstaanbieders die acquiringdiensten aanbieden, educatieve programma's over het voorkomen van fraude voor hun webwinkeliers opzetten.

Berichten, instellen van limieten

Goede praktijk 11: Binnen de gestelde limieten kunnen betalingsdienstaanbieders hun klanten de mogelijkheid bieden om de limieten voor internetbetalingsdiensten te beheren in een veilige en betrouwbare omgeving.

Goede praktijk 12: Betalingsdienstaanbieders kunnen invoeren dat de klant een waarschuwing ontvangt, per telefoon of sms, met betrekking tot verdachte transacties of betalingstransacties met een hoog risico, uitgaande van hun beleid voor risicobeheer.

Goede praktijk 13: Betalingsdienstaanbieders kunnen klanten de mogelijkheid bieden om algemene, gepersonaliseerde regels te specificeren als parameters voor hun gedrag met betrekking tot internetbetalingen en gerelateerde diensten, bv. dat klanten alleen betalingen vanuit bepaalde landen initiëren en dat betalingen die elders geïnitieerd zijn, worden geblokkeerd, of dat klanten specifieke begunstigden toevoegen aan een witte of zwarte lijst.