ABE/GL/2014/12_Rev1

19 dicembre 2014

Orientamenti finali

sulla sicurezza dei pagamenti via Internet

Indice

Orientamenti sulla sicurezza dei pagamenti via Internet

Status giuridico degli orientamenti

Il presente documento contiene orientamenti emanati ai sensi dell'articolo 16 del regolamento (UE) n. 1093/2010 del Parlamento europeo e del Consiglio, del 24 novembre 2010, che istituisce l'Autorità europea di vigilanza (Autorità bancaria europea), modifica la decisione n. 716/2009/CE e abroga la decisione 2009/78/CE della Commissione (il "regolamento ABE"). Conformemente all'articolo 16, paragrafo 3, del regolamento ABE, le autorità competenti e gli enti finanziari compiono ogni sforzo per conformarsi agli orientamenti.

Gli orientamenti presentano il parere dell'ABE in merito alle prassi di vigilanza adeguate all'interno del Sistema europeo di vigilanza finanziaria o alle modalità di applicazione del diritto dell'Unione in una particolare area. L'ABE si attende pertanto che tutte le autorità competenti e gli enti finanziari si conformino agli orientamenti loro rivolti. Le autorità competenti sono tenute a conformarsi agli orientamenti che si applicano a esse mediante il loro inserimento nelle rispettive prassi di vigilanza in modo opportuno (ad esempio modificando il proprio quadro giuridico o le proprie procedure di vigilanza), anche quando gli orientamenti si rivolgono principalmente agli enti.

Obblighi di comunicazione

Ai sensi dell'articolo 16, paragrafo 3, del regolamento ABE, le autorità competenti sono tenute a comunicare all'ABE entro il 5 maggio 2015 se sono conformi o se intendono conformarsi agli orientamenti in questione; in alternativa sono tenute a indicare le ragioni della mancata conformità. Qualora entro il termine indicato non sia pervenuta alcuna comunicazione da parte delle autorità competenti, esse sono ritenute dall'ABE non conformi. Le comunicazioni devono essere inviate presentando il modulo fornito nella sezione 5 all'indirizzo compliance@eba.europa.eu con il riferimento "EBA/GL/2014/12". Le comunicazioni devono essere inviate da persone debitamente autorizzate a segnalare la conformità per conto delle rispettive autorità competenti.

Le comunicazioni sono pubblicate sul sito web dell'ABE ai sensi dell'articolo 16, paragrafo 3.

Titolo I – Ambito di applicazione e definizioni

Ambito di applicazione

1. I presenti orientamenti stabiliscono una serie di requisiti minimi in materia di sicurezza dei pagamenti via Internet. I presenti orientamenti si basano sulle disposizioni della direttiva 2007/64/CE[1] ("direttiva sui servizi di pagamento") relative ai requisiti informativi per i servizi di pagamento e agli obblighi dei prestatori di servizi di pagamento in relazione alla prestazione di servizi di pagamento. Inoltre, l'articolo 10, paragrafo 4, della direttiva impone agli istituti di pagamento di disporre di solidi dispositivi di governo societario e di adeguati meccanismi di controllo interno.

2. Gli orientamenti si applicano alla prestazione di servizi di pagamento offerti via Internet da prestatori di servizi di pagamento, come definiti all'articolo 1 della direttiva.

3. Gli orientamenti sono rivolti agli enti finanziari, di cui all'articolo 4, paragrafo 1, del regolamento (UE) n. 1093/2010 e alle autorità competenti di cui all'articolo 4, paragrafo 2, del regolamento (UE) n. 1093/2010. Le autorità competenti dei 28 Stati membri dell'Unione europea dovrebbero garantire l'applicazione dei presenti orientamenti da parte dei prestatori di servizi di pagamento, come definiti all'articolo 1 della direttiva sui servizi di pagamento, soggetti alla loro vigilanza.

4. Inoltre, le autorità competenti possono decidere di imporre ai prestatori di servizi di pagamento di segnalare all'autorità competente la loro osservanza degli orientamenti.

5. I presenti orientamenti non pregiudicano la validità delle raccomandazioni della Banca centrale europea "*Recommendations for the security of internet payments*" (Il "rapporto'')[2]. Il rapporto in particolare, continua a rappresentare il documento a fronte del quale le banche centrali, nella loro funzione di sorveglianza sui sistemi e sugli strumenti di pagamento, dovrebbero valutare la conformità di questi ultimi con riferimento alla sicurezza dei pagamenti via Internet.

6. Gli orientamenti costituiscono aspettative minime. Essi non inficiano la responsabilità dei prestatori di servizi di pagamento di monitorare e valutare i rischi connessi alle loro operazioni di pagamento, sviluppare proprie politiche di sicurezza dettagliate e porre in essere adeguate misure di sicurezza, emergenza, gestione degli incidenti e continuità operativa, che siano commisurate ai rischi inerenti ai servizi di pagamento prestati.

7. Gli orientamenti mirano a definire requisiti minimi comuni per i servizi di pagamento via Internet elencati di seguito, indipendentemente dal dispositivo di accesso utilizzato:

[1] Direttiva 2007/64/CE del Parlamento europeo e del Consiglio, del 13 novembre 2007, relativa ai servizi di pagamento nel mercato interno, recante modifica delle direttive 97/7/CE, 2002/65/CE, 2005/60/CE e 2006/48/CE, che abroga la direttiva 97/5/CE (GU L 319 del 5.12.2007).

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

- [carte] l'esecuzione dei pagamenti con carta via Internet, compresi i pagamenti con carta virtuale, così come la registrazione dei dati relativi alle carte di pagamento per l'utilizzo in "soluzioni di tipo "Wallet" ;

- [bonifici] l'esecuzione dei bonifici via Internet;

- [mandato elettronico] l'emissione e la modifica dei mandati elettronici di addebito diretto;

- [moneta elettronica] trasferimenti di moneta elettronica tra due conti di moneta elettronica via Internet.

8. Quando gli orientamenti indicano un risultato, tale risultato può essere raggiunto attraverso vari mezzi. I presenti orientamenti, oltre ai requisiti riportati di seguito, forniscono altresì esempi delle prassi migliori (allegato 1) che i prestatori di servizi di pagamento sono invitati, ma non sono tenuti, a seguire.

9. Qualora la prestazione dei servizi e degli strumenti di pagamento venga offerta attraverso uno schema di pagamento (per es., schemi di pagamento con carta, schemi di bonifico, schemi di addebito diretto, ecc.), le autorità competenti e la relativa banca centrale avente funzioni di sorveglianza sugli strumenti di pagamento dovrebbero cooperare al fine di garantire un'applicazione coerente degli orientamenti da parte degli operatori responsabili del funzionamento dello schema.

10. Gli integratori di servizi di pagamento [3] che offrono i servizi di inizializzazione di pagamenti possono essere prestatori di servizi di acquisizione (acquiring) di pagamenti via Internet (e quindi prestatori di servizi di pagamento) oppure prestatori esterni di servizi tecnici degli schemi o dei prestatori dei servizi di pagamento interessati. In quest'ultimo caso, gli integratori di servizi di pagamento dovrebbero essere contrattualmente vincolati ad attenersi ai presenti orientamenti.

11. Sono esclusi dall'ambito di applicazione dei presenti orientamenti:

- altri servizi via Internet forniti da un prestatore di servizi di pagamento tramite il proprio sito web (per esempio intermediazione online, contratti online);

- i pagamenti le cui istruzioni sono trasmesse per posta, per telefono, posta vocale o utilizzando la tecnologia basata su SMS;

- i pagamenti mobili diversi dai pagamenti su browser (brower-based);

- i bonifici in cui un soggetto terzo accede al conto di pagamento del cliente;

[3] Gli integratori di servizi di pagamento sono coloro che forniscono al beneficiario (per esempio l'operatore commerciale online) un'interfaccia standardizzata per i servizi di inizializzazione dei pagamenti forniti dai prestatori di servizi di pagamento.

- le operazioni di pagamento effettuate da un'impresa tramite reti dedicate;

- i pagamenti con carta effettuati con carte prepagate fisiche o virtuali, anonime e non ricaricabili, per i quali non esiste alcun rapporto continuativo tra l'emittente e il proprietario della carta;

- la compensazione e il regolamento delle operazioni di pagamento.

Definizioni

12. Ai fini dei presenti orientamenti, e oltre alle definizioni fornite nella direttiva sui servizi di pagamento, valgono le seguenti definizioni:

- *autenticazione,* una procedura che consente al prestatore di servizi di pagamento di verificare l'identità di un cliente;

- *autenticazione forte del cliente* è, ai fini dei presenti orientamenti, una procedura basata sull'impiego di due o più dei seguenti elementi - classificati nelle categorie della conoscenza, del possesso e dell'inerenza: i) qualcosa che solo l'utente conosce, per esempio una password statica, un codice, un numero di identificazione personale; ii) qualcosa che solo l'utente possiede, per esempio un token, una smart card, un cellulare; iii) qualcosa che caratterizza l'utente, per esempio una caratteristica biometrica, quale può essere un'impronta digitale. Inoltre, gli elementi selezionati devono essere reciprocamente indipendenti, ossia la violazione di un elemento non compromette l'altro o gli altri. Almeno uno degli elementi dovrebbe essere non riutilizzabile e non replicabile (eccettuata la categoria dell'inerenza) e non atto a essere indebitamente carpito via Internet. La procedura di autenticazione forte dovrebbe essere concepita in modo tale da proteggere la riservatezza dei dati di autenticazione;

- *autorizzazione,* una procedura che verifica se un cliente o un prestatore di servizi di pagamento ha il diritto di eseguire una determinata azione, per esempio il diritto di trasferire fondi o di avere accesso a dati sensibili;

- *credenziali*, le informazioni — generalmente riservate — fornite da un cliente o da un prestatore di servizi di pagamento ai fini dell'autenticazione. Per credenziali si può anche intendere lo strumento fisico contenente le informazioni (per esempio un generatore di one-time password, una smart card) o qualcosa che l'utente memorizza o rappresenta (come per esempio le caratteristiche biometriche);

- *grave incidente per la sicurezza dei pagamenti:* un incidente che ha o può avere un impatto significativo sulla sicurezza, sull'integrità e sulla continuità dei sistemi di pagamento dei prestatori di servizi di pagamento e/o sulla sicurezza dei dati sensibili sui pagamenti o dei fondi. La valutazione della rilevanza dovrebbe prendere in considerazione il numero di clienti potenzialmente interessati, l'importo a rischio e l'impatto su altri prestatori di servizi di pagamento o altre infrastrutture di pagamento;

- *analisi del rischio dell'operazione,* la valutazione del rischio relativo a un'operazione specifica tenendo conto di criteri quali, per esempio, i modelli di pagamento del cliente (comportamento), il valore delle relative operazioni, il tipo di prodotto e il profilo del beneficiario;

- *"virtual card"* , una soluzione di pagamento con carta in cui viene generato un numero di carta temporaneo e alternativo con ridotto periodo di validità, utilizzo limitato e limite di spesa predefinito, che può essere utilizzato per effettuare acquisti via Internet;

- *soluzioni "wallet",* soluzioni che permettono al cliente di registrare i dati relativi a uno o più strumenti di pagamento, al fine di effettuare pagamenti con diversi operatori commerciali online.

Titolo II – Orientamenti sulla sicurezza dei pagamenti via Internet

Controllo generale e ambiente di sicurezza

Governance

1. I prestatori di servizi di pagamento dovrebbero attuare e riesaminare periodicamente una formale policy di sicurezza per i servizi di pagamento via Internet.

   1.1 La policy di sicurezza dovrebbe essere adeguatamente documentata e riesaminata periodicamente (in linea con l'orientamento 2.4) e approvata dall'alta dirigenza. Essa dovrebbe definire gli obiettivi di sicurezza e la propensione al rischio.

   1.2 La policy di sicurezza dovrebbe definire ruoli e responsabilità, compresa la funzione di gestione del rischio con linee di responsabilità dirette a livello di vertici aziendali, e linee di responsabilità per i servizi di pagamento prestati via Internet, compresa la gestione dei dati sensibili relativi ai pagamenti con riguardo alla valutazione, al controllo e alla mitigazione dei rischi.

Valutazione dei rischi

2. I prestatori di servizi di pagamento dovrebbero svolgere valutazioni dei rischi approfondite per quanto riguarda la sicurezza dei pagamenti via Internet e dei servizi connessi, e documentarle , sia prima di avviare l'offerta dei servizi, sia successivamente con frequenza regolare.

   2.1 Attraverso la loro funzione di gestione del rischio, i prestatori di servizi di pagamento, dovrebbero svolgere e documentare valutazioni dei rischi approfondite per i pagamenti via Internet e i servizi connessi. I prestatori di servizi di pagamento dovrebbero tenere conto dei risultati del monitoraggio costante delle minacce alla sicurezza dei servizi di pagamento via Internet che offrono o intendono offrire, tenendo in considerazione: i) le soluzioni tecnologiche da essi utilizzate, ii) i servizi affidati a operatori esterni e iii) l'ambiente tecnico dei clienti. I prestatori di servizi di pagamento dovrebbero tener conto dei rischi associati alle piatteforme tecnologiche scelte, all'architettura dell'applicazione, alle tecniche di programmazione e alle procedure, per quanto riguarda sia i prestatori in questione[4] sia i loro clienti[5], come pure i risultati del processo di monitoraggio degli incidenti riguardanti la sicurezza (cfr. l'orientamento 3).

[4] Per esempio la suscettibilità del sistema al dirottamento delle sessioni di pagamento (payment session hijacking), iniezioni di linguaggio d'interrogazione strutturato (SQL injection), cross-site scripting, buffer overflow, ecc.

[5] Per esempio i rischi associati all'uso di applicazioni multimediali, browser plug-in, frame, link esterni, ecc.

2.2 Su questa base, i prestatori di servizi di pagamento dovrebbero stabilire se e quanto possono rivelarsi necessarie modifiche alle misure di sicurezza esistenti, alle tecnologie utilizzate e alle procedure o ai servizi resi. I prestatori di servizi di pagamento dovrebbero tener conto del tempo necessario per mettere in atto le modifiche (compreso il roll-out dell'utente) e adottare i provvedimenti provvisori necessari per ridurre al minimo gli incidenti di sicurezza e le frodi, nonché i potenziali effetti pregiudizievoli.

2.3 La valutazione dei rischi dovrebbe considerare l'esigenza di proteggere e tutelare i dati sensibili relativi ai pagamenti.

2.4 I prestatori di servizi di pagamento dovrebbero prevedere una revisione degli scenari di rischio e delle misure di sicurezza esistenti dopo gli incidenti gravi che interessano i loro servizi, prima di un cambiamento importante delle infrastrutture o delle procedure, e quando nuove minacce sono individuate attraverso attività di monitoraggio dei rischi. Inoltre, una revisione generale della valutazione dei rischi dovrebbe essere effettuata almeno una volta all'anno. I risultati delle valutazioni dei rischi e delle revisioni dovrebbero essere sottoposti all'approvazione dell'alta dirigenza.

Monitoraggio e segnalazione degli incidenti

3. I prestatori di servizi di pagamento dovrebbero garantire il monitoraggio , la gestione e il follow-up costanti e integrati degli incidenti relativi alla sicurezza, compresi i reclami dei clienti in materia di sicurezza. I prestatori di servizi di pagamento dovrebbero stabilire una procedura per la segnalazione di tali incidenti alla dirigenza e, in caso di gravi incidenti relativi alla sicurezza dei pagamenti, alle autorità competenti.

3.1 I prestatori di servizi di pagamento dovrebbero porre in essere un processo utile a monitorare, gestire e seguire gli incidenti relativi alla sicurezza e i reclami dei clienti in materia di sicurezza, e riferire tali incidenti alla dirigenza.

3.2 I prestatori di servizi di pagamento dovrebbero avvalersi di una procedura di comunicazione immediata alle autorità competenti (vale a dire alle autorità di vigilanza e alle autorità preposte alla protezione dei dati), laddove esistano, in caso di gravi incidenti relativi alla sicurezza dei pagamenti con riferimento ai servizi di pagamento prestati.

3.3 I prestatori di servizi di pagamento dovrebbero disporre di una procedura per la cooperazione, in caso di gravi incidenti relativi alla sicurezza dei pagamenti, compresa la violazioni dei dati, con i competenti organismi di esecuzione della legge.

3.4 I prestatori di servizi di acquiring dovrebbero contrattualmente richiedere agli operatori commerciali online, che conservano, elaborano o trasmettono i dati sensibili relativi ai pagamenti, di cooperare sia con essi sia con i competenti organismi di

esecuzione della legge qualora si verificassero gravi incidenti relativi alla sicurezza dei pagamenti, comprese le violazioni dei dati. Se un prestatore di servizi di pagamento viene a conoscenza del fatto che un operatore commerciale online non sta cooperando, come richiesto in base al contratto, dovrebbe procedere all'applicazione di tale obbligo contrattuale o alla risoluzione del contratto.

Controllo e mitigazione dei rischi

4. I prestatori di servizi di pagamento dovrebbero attuare misure di sicurezza in linea con le rispettive politiche di sicurezza, al fine di mitigare i rischi individuati. Tali misure dovrebbero includere più livelli di difesa della sicurezza, di modo che se una linea di difesa viene meno, questa è sostituita dalla linea di difesa successiva ("difesa in profondità").

4.1 Nella progettazione, nello sviluppo e nel mantenimento dei servizi di pagamento via Internet, i prestatori di servizi di pagamento dovrebbero prestare particolare attenzione all'adeguata separazione dei compiti e dei ruoli negli ambienti della tecnologia dell'informazione (IT) (per esempio gli ambienti di sviluppo, di prova e di produzione) e alla corretta applicazione del principio del "privilegio minimo" quale base per una sana gestione delle identità e degli accessi[6].

4.2 I prestatori di servizi di pagamento dovrebbero disporre di soluzioni di sicurezza adeguate per proteggere le reti, i siti web, i server e i collegamenti di comunicazione contro abusi o attacchi. I prestatori di servizi di pagamento dovrebbero disattivare nei server tutte le funzioni superflue al fine di proteggerli ('*hardening*') e di eliminare o ridurre le vulnerabilità delle applicazioni a rischio. L'accesso mediante le varie applicazioni ai dati e alle risorse necessarie dovrebbe essere ridotto al minimo indispensabile secondo il principio del "privilegio minimo". Al fine di limitare l'uso di "falsi" siti web (che imitano i siti legittimi dei prestatori di servizi di pagamento), i siti web transazionali che offrono servizi di pagamento via Internet dovrebbero essere identificati mediante estesi certificati di convalida redatti a nome del prestatore di servizi di pagamento o con altri metodi di autenticazione equivalenti.

4.3 I prestatori di servizi di pagamento dovrebbero avvalersi di processi idonei per monitorare, tenere traccia e limitare l'accesso a: i) dati sensibili relativi ai pagamenti e ii) risorse critiche, logiche e fisiche, quali reti, sistemi, banche dati, moduli di sicurezza, ecc. I prestatori di servizi di pagamento dovrebbero creare, conservare e analizzare adeguati registri e procedimenti di tracciabilità dei dati (piste di controllo).

[6] Ogni programma e ogni utente privilegiato del sistema dovrebbe funzionare con la minor quantità di privilegi necessari per completare il lavoro. Cfr. Saltzer, J. H. (1974), "Protection and the Control of Information Sharing in Multics", Communications of the ACM, Vol. 17, n. 7, pag. 388.

4.4 Nella progettazione[7], nello sviluppo e nel mantenimento dei servizi di pagamento via Internet, i prestatori di servizi di pagamento dovrebbero assicurare che la "*Data minimisation*" [8] sia una componente essenziale della funzionalità di base: la raccolta, il routing, l'elaborazione, la conservazione e/o l'archiviazione e la visualizzazione dei dati sensibili relativi ai pagamenti dovrebbero essere mantenute al livello minimo assoluto.

4.5 Le misure di sicurezza per i servizi di pagamento via Internet dovrebbero essere sottoposte a test sotto la supervisione della funzione di gestione dei rischi per garantire la loro robustezza ed efficacia. Tutte le modifiche dovrebbero formare l'oggetto di un processo formale di gestione dei cambiamenti che garantisca che i cambiamenti siano correttamente ideati, sottoposti a prove, documentati e autorizzati. Sulla base dei cambiamenti effettuati e delle minacce alla sicurezza osservate, le prove dovrebbero essere ripetute regolarmente e comprendere scenari di attacchi potenziali pertinenti e noti.

4.6 Le misure di sicurezza del prestatore di servizi di pagamento per i servizi di pagamento via Internet dovrebbero essere periodicamente oggetto di verifica interna (*audit*) per garantire la loro robustezza ed efficacia. L'attuazione e il funzionamento dei servizi di pagamento via Internet dovrebbero essere oggetto di verifica interna. La frequenza e l'oggetto di tali controlli dovrebbero essere attinenti e proporzionali ai rischi per la sicurezza implicati. Esperti (interni o esterni) attendibili e indipendenti dovrebbero svolgere i controlli in questione. Tali esperti non dovrebbero essere coinvolti in alcun modo nello sviluppo, nella realizzazione o nella gestione operativa dei servizi di pagamento via Internet prestati.

4.7 Ogniqualvolta i prestatori di servizi di pagamento esternalizzano funzioni relative alla sicurezza dei servizi di pagamento via Internet, il contratto dovrebbe includere disposizioni che prevedano il rispetto dei principi e degli orientamenti definiti nei presenti orientamenti.

4.8 I prestatori di servizi di pagamento che offrono servizi di acquiring dovrebbero contrattualmente richiedere agli operatori commerciali online, che trattano (per esempio conservano, elaborano o trasmettono) dati sensibili relativi ai pagamenti, di attuare misure di sicurezza nella propria infrastruttura IT, in linea con gli orientamenti 4.1-4.7, al fine di evitare il furto dei dati sensibili relativi ai pagamenti attraverso i loro sistemi. Se un prestatore di servizi di pagamento viene a conoscenza del fatto che un operatore commerciale online non ha attuato le misure di sicurezza richieste, dovrebbe procedere all'adozione di misure per l'adempimento di tale obbligo contrattuale o alla risoluzione del contratto.

[7] "Privacy by design".

[8] La "*Data minimisation*" si riferisce alla politica di raccogliere la quantità minima di informazioni personali necessarie per svolgere una data funzione.

Tracciabilità

5. I prestatori di servizi di pagamento dovrebbero predisporre processi per garantire che tutte le transazioni e i processi di gestione del mandato elettronico ("*e-mandate*") siano opportunamente tracciati.

   5.1 I prestatori di servizi di pagamento dovrebbero garantire che il loro servizio includa meccanismi di sicurezza per la registrazione dettagliata dei dati delle operazioni e dei mandati elettronici, fra cui il numero sequenziale dell'operazione, la marcatura temporale per i dati delle operazioni, le modifiche alla parametrizzazione, e l'accesso ai dati delle operazioni e dei mandati elettronici.

   5.2 I prestatori di servizi di pagamento dovrebbero porre in essere file di registrazione (log file) che consentano la tracciabilità di aggiunte, rettifiche o cancellazioni dei dati riguardanti le transazioni o dati dei mandati elettronici sottoposti a tracciatura.

   5.3 I prestatori di servizi di pagamento dovrebbero analizzare i dati delle transazioni e dei mandati elettronici, e possedere gli strumenti per valutare tali "log file". Le rispettive applicazioni dovrebbero essere disponibili solo al personale autorizzato.

Misure specifiche di controllo e di sicurezza per i pagamenti via Internet

Identificazione iniziale dei clienti, informazioni

6. I clienti dovrebbero essere adeguatamente identificati in linea con la normativa europea antiriciclaggio[9] e confermare la loro volontà di effettuare pagamenti via Internet utilizzando i servizi prima di poter accedere a tali servizi. I prestatori di servizi di pagamento dovrebbero fornire un'adeguata informazione "preventiva", "regolare" o, se del caso, "ad hoc" al cliente circa i requisiti necessari (per esempio, apparecchiature, procedure) per l'esecuzione in sicurezza di operazioni di pagamento via Internet, nonché i rischi inerenti.

   6.1 I prestatori di servizi di pagamento dovrebbero garantire che il cliente si sia sottoposto alle procedure di adeguata verifica della clientela e abbia fornito validi documenti di identità[10] e le relative informazioni prima che sia autorizzato ad accedere ai servizi di pagamento via Internet[11].

[9] Per esempio, la direttiva 2005/60/CE del Parlamento europeo e del Consiglio, del 26 ottobre 2005, relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo. GU L 309 del 25.11.2005, pagg. 15-36. Cfr. anche la direttiva 2006/70/CE del 1° agosto 2006, recante misure di esecuzione della direttiva 2005/60/CE del Parlamento europeo e del Consiglio per quanto riguarda la definizione di «persone politicamente esposte» e i criteri tecnici per le procedure semplificate di adeguata verifica della clientela e per l'esenzione nel caso di un'attività finanziaria esercitata in modo occasionale o su scala molto limitata. GU L 214 del 4.8.2006, pagg. 29-34.

[10] Per esempio, il passaporto, la carta d'identità o la firma elettronica avanzata.

[11] Il processo di identificazione del cliente non pregiudica eventuali esenzioni previste nella normativa vigente contro il riciclaggio di denaro. I prestatori di servizi di pagamento non devono condurre un processo di identificazione del cliente distinto per i servizi di pagamento via Internet, a condizione che l'identificazione di tali clienti sia stata già effettuata, per esempio per altri servizi di pagamento esistenti o per l'apertura di un conto.

6.2 I prestatori di servizi di pagamento dovrebbero garantire che le informazioni preliminari[12] fornite al cliente contengano dettagli specifici relativi ai servizi di pagamento via Internet. Queste dovrebbero includere, a seconda dei casi:

- informazioni chiare sui requisiti del cliente in termini di apparecchiature utilizzate dall'utente, software o altri strumenti necessari (per esempio software antivirus, firewall);
- orientamenti per l'uso corretto e sicuro delle credenziali di sicurezza personalizzate;
- una descrizione passo passo della procedura con la quale il cliente inoltra e autorizza un'operazione di pagamento e/o ottiene informazioni, inclusi gli esiti di ogni azione;
- orientamenti per l'uso corretto e sicuro di tutto l'hardware e il software fornito al cliente;
- le procedure da seguire in caso di perdita o furto delle credenziali di sicurezza personalizzate, o dell'hardware o del software del cliente per l'accesso o l'esecuzione delle operazioni;
- le procedure da seguire in caso di abuso riscontrato o sospetto;
- una descrizione delle responsabilità e degli oneri del prestatore di servizi di pagamento e del cliente, rispettivamente, per quanto riguarda l'uso del servizio di pagamento via Internet.

6.3 I prestatori di servizi di pagamento dovrebbero garantire che il contratto quadro con il cliente stabilisca che il prestatore di servizi di pagamento può bloccare una specifica operazione o lo strumento di pagamento[13] per problemi di sicurezza. Si dovrebbe stabilire il metodo e i termini della comunicazione al cliente e le modalità per contattare il prestatore di servizi di pagamento per "sbloccare" l'operazione di pagamento via Internet o il servizio, in linea con la direttiva sui servizi di pagamento.

Autenticazione forte del cliente

7. L'inoltro dei pagamenti via Internet, così come l'accesso ai dati sensibili relativi ai pagamenti, dovrebbero essere protetti da un'autenticazione forte del cliente. I prestatori di servizi di pagamento dovrebbero avvalersi di una solida procedura di autenticazione dei clienti, che sia in linea con la definizione fornita nei presenti orientamenti.

[12] Tali informazioni integrano l'articolo 42 della direttiva sui servizi di pagamento, che specifica le informazioni che il prestatore di servizi di pagamento deve fornire all'utente dei servizi di pagamento prima di stipulare un contratto per la fornitura dei servizi di pagamento.

[13] Si veda l'articolo 55 della direttiva sui servizi di pagamento sui limiti dell'utilizzo degli strumenti di pagamento.

7.1 [bonifico/mandato elettronico/moneta elettronica] I prestatori di servizi di pagamento dovrebbero effettuare l'autenticazione forte del cliente per l'autorizzazione da parte del cliente delle operazioni di pagamento via Internet (inclusi i bonifici in "bundle") e il rilascio o la modifica dei mandati elettronici di addebito diretto. Tuttavia, i prestatori di servizi di pagamento potrebbero prendere in considerazione l'adozione di misure alternative di autenticazione del cliente per:

- pagamenti in uscita destinati ai beneficiari di fiducia inclusi nelle "*white list*" prestabilite per quel cliente;
- operazioni tra due conti di uno stesso cliente presso lo stesso prestatore di servizi di pagamento;
- trasferimenti all'interno dello stesso prestatore di servizi di pagamento giustificati da un'analisi dei rischi della transazione;
- pagamenti di basso valore, di cui alla direttiva sui servizi di pagamento[14].

7.2 Ottenere l'accesso o modificare i dati sensibili relativi ai pagamenti (fra cui la creazione e la modifica delle "white list") richiede l'autenticazione forte del cliente. Quando un prestatore di servizi di pagamento offre servizi puramente consultivi, senza fornire informazioni sensibili sui clienti o sui pagamenti, come i dati delle carte di pagamento, di cui potrebbe essere facilmente fatto un uso improprio a fini fraudolenti, il prestatore di servizi di pagamento può adattare i requisiti di autenticazione sulla base della propria valutazione dei rischi.

7.3 [carte] Per le operazioni con carta, tutti i prestatori di servizi di pagamento che emettono carte (issuer) dovrebbero supportare l'autenticazione forte del titolare della carta. Tutte le carte emesse devono essere tecnicamente pronte (registrate) per essere utilizzate con l'autenticazione forte del titolare della carta.

7.4 [carte] I prestatori di servizi di pagamento che offrono servizi di acquiring di carte di pagamento dovrebbero supportare le tecnologie che consentono all'emittente di eseguire l'autenticazione forte del titolare della carta agli schemi di carte di pagamento cui partecipa l'acquirer .

7.5 [carte] I prestatori di servizi di pagamento che offrono servizi di acquiring dovrebbero richiedere ai loro operatori commerciali online di supportare soluzioni che permettano all'emittente di eseguire l'autenticazione forte del titolare della carta per le transazioni con carta via Internet. L'uso di misure di autenticazione alternative potrebbe essere preso in considerazione per categorie di operazioni a basso rischio pre-identificate, per

[14] Cfr. la definizione di strumenti di pagamento di basso valore agli articoli 34, paragrafo 1, e 53, paragrafo 1, della direttiva sui servizi di pagamento.

esempio sulla base di un'analisi del rischio delle operazioni, o che coinvolgono pagamenti di basso valore, di cui alla direttiva sui servizi di pagamento.

7.6 [carte] Per gli schemi di pagamento con carta accettati dal servizio, i fornitori di soluzioni di tipo "*wallet*" dovrebbero richiedere l'autenticazione a forte dall'emittente quando il legittimo possessore registra per la prima volta i dati della propria carta.

7.7 I fornitori di "*wallet solutions*" dovrebbero supportare un'autenticazione forte del cliente quando i clienti procedono all'accesso ai suddetti servizi di pagamento o effettuano operazioni con carta via Internet. L'uso di misure di autenticazione alternative potrebbe essere preso in considerazione per categorie di operazioni a basso rischio pre-identificate, per esempio sulla base di un'analisi del rischio delle operazioni, o che coinvolgono pagamenti di basso valore, di cui alla direttiva sui servizi di pagamento.

7.8 [carte] Per le "*virtual cards*", la prima registrazione dovrebbe avvenire in un ambiente sicuro e affidabile[15]. L'autenticazione forte del cliente dovrebbe essere richiesta per il processo di generazione di dati della "virtual card", se questa viene emessa nell'ambiente Internet.

7.9 I prestatori di servizi di pagamento dovrebbero garantire una corretta autenticazione bilaterale durante la comunicazione con gli operatori commerciali online, al fine di inoltrare i pagamenti via Internet e accedere ai dati sensibili relativi ai pagamenti.

Iscrizione (enrolment) e fornitura di strumenti e/o software di autenticazione al cliente

8. I prestatori di servizi di pagamento dovrebbero garantire che la registrazione iniziale al servizio (*enrolment*) del cliente e la fornitura iniziale degli strumenti di autenticazione (necessari per utilizzare il servizio di pagamento via Internet) e/o la fornitura di software agli utenti per effettuare i pagamenti, avvengano in modo sicuro.

8.1 L'enrolment e la fornitura all'utente di strumenti di autenticazione e/o software per effettuare pagamenti, dovrebbero soddisfare i seguenti requisiti.

- Le relative procedure dovrebbero essere effettuate in un ambiente sicuro e affidabile, tenendo conto dei possibili rischi derivanti da dispositivi che non sono sotto il controllo del prestatore di servizi di pagamento.

[15] Gli ambienti sotto la responsabilità del prestatore di servizi di pagamento in cui è garantita un'adeguata autenticazione del cliente e del prestatore di servizi di pagamento che offre il servizio e la protezione delle informazioni riservate/sensibili sono: i) i locali del prestatore di servizi di pagamento; ii) internet banking o altri siti web sicuri, per esempio quando la governance authority dello schema offre funzioni di sicurezza paragonabili, fra l'altro, come definito nell'orientamento 4 o iii) servizi di sportelli automatici. (Nel caso degli sportelli automatici, è necessaria un'autenticazione a due fattori del cliente. Tale autenticazione viene in genere fornita mediante Chip e PIN, o chip e biometria).

- Procedure efficaci e sicure dovrebbero essere poste in essere per la consegna delle credenziali di sicurezza personalizzate, dei software per effettuare pagamenti e di tutti i dispositivi personalizzati riguardanti i pagamenti via Internet. I software forniti via Internet dovrebbero essere digitalmente firmati da parte del prestatore di servizi di pagamento per consentire al cliente di verificare la loro autenticità e accertare che non siano stati falsificati.

- [carte] Per le operazioni con carta, il cliente dovrebbe avere la possibilità di registrarsi per l'autenticazione forte indipendentemente da uno specifico acquisto su Internet. Qualora sia disponibile l'attivazione durante lo shopping online, questa dovrebbe essere fatta reindirizzando il cliente verso un ambiente sicuro e affidabile.

8.2 [carte] Gli emittenti dovrebbero incoraggiare attivamente il titolare della carta a chiedere l'autenticazione forte e consentire di saltare la procedura dell'iscrizione (enrolment) solo in un numero eccezionale e limitato di casi, motivati dal rischio legato all'operazione specifica con carta.

Tentativi di accesso, sessione scaduta, validità di autenticazione

9. I prestatori di servizi di pagamento dovrebbero limitare il numero dei tentativi di accesso o di autenticazione, definire le regole per la "scadenza" delle sessioni dei servizi di pagamento via Internet e definire i termini per la validità dell'autenticazione.

9.1 Quando si utilizza una one-time password (OTP) per l'autenticazione, i prestatori di servizi di pagamento dovrebbero garantire che il periodo di validità di tali password sia limitato allo stretto necessario.

9.2 I prestatori di servizi di pagamento dovrebbero fissare il numero massimo di tentativi falliti di accesso o di autenticazione dopodiché l'accesso al servizio di pagamento via Internet viene (temporaneamente o permanentemente) bloccato. Essi dovrebbero avvalersi di una procedura sicura per riattivare i servizi di pagamento via Internet bloccati.

9.3 I prestatori di servizi di pagamento dovrebbero stabilire il periodo massimo dopo il quale le sessioni dei servizi di pagamento via Internet inattive vengono automaticamente terminate.

Monitoraggio delle operazioni

10. I meccanismi per il monitoraggio delle operazioni volti a prevenire, rilevare e bloccare il traffico dei pagamenti fraudolenti dovrebbero essere attivati prima dell'autorizzazione finale del prestatore di servizi di pagamento; le operazioni sospette o ad alto rischio dovrebbero essere oggetto di una specifica analisi e procedura di valutazione. Meccanismi

di monitoraggio della sicurezza e di autorizzazione equivalenti dovrebbero essere disponibili per l'emissione dei mandati elettronici.

10.1 I prestatori di servizi di pagamento dovrebbero utilizzare sistemi di rilevamento e prevenzione delle frodi per individuare operazioni sospette prima che il prestatore di servizi di pagamento autorizzi da ultimo le operazioni o i mandati elettronici. Tali sistemi dovrebbero essere basati, per esempio, su regole parametrizzate (come le "Black-list" dei dati relativi alle carte compromesse o rubate) e monitorare i modelli di comportamento anomalo del cliente o del dispositivo di accesso del cliente (per esempio, un cambiamento dell'indirizzo Internet Protocol (IP)[16] o dell'intervallo IP durante la sessione dei servizi di pagamento via Internet, a volte identificati mediante controlli di geolocalizzazione IP[17], categorie di operatori commerciali online atipici per un cliente specifico o transazioni con dati anomali, ecc.). Tali sistemi dovrebbero anche essere in grado di rilevare i segnali di infezione da malware nella sessione (per esempio tramite script a fronte di convalida umana) e scenari di frode noti. L'entità, la complessità e l'adattabilità delle soluzioni di monitoraggio, nel rispetto della normativa in materia di protezione dei dati, dovrebbero essere commisurate al risultato della valutazione dei rischi.

10.2 I prestatori di servizi di pagamento dovrebbero disporre di sistemi di rilevamento e prevenzione delle frodi per monitorare le attività degli operatori commerciali online.

10.3 I prestatori di servizi di pagamento dovrebbero eseguire analisi delle transazioni e procedure di valutazione sulle stesse entro un periodo di tempo adeguato, in modo da non ritardare indebitamente l'ordine e/o l'esecuzione del servizio di pagamento in questione.

10.4 Se il prestatore di servizi di pagamento, secondo la sua politica del rischio, decide di bloccare un'operazione di pagamento identificata come potenzialmente fraudolenta, il prestatore di servizi di pagamento dovrebbe mantenere il blocco per il più breve tempo possibile finché non saranno risolti i problemi di sicurezza.

Protezione dei dati sensibili relativi ai pagamenti

11. I dati sensibili relativi ai pagamenti dovrebbero essere protetti se conservati, trattati o trasmessi.

11.1 Tutti i dati utilizzati per identificare e autenticare i clienti (per esempio in fase di accesso, in occasione dell'ordine dei pagamenti via Internet e del rilascio, della modifica o della cancellazione dei mandati elettronici), così come l'interfaccia dei

[16] Un indirizzo IP è un codice numerico univoco che identifica ogni computer collegato a Internet.

[17] Un controllo "Geo-IP" verifica se il paese di emissione corrisponde all'indirizzo IP da cui l'utente avvia l'operazione.

clienti (i prestatori di servizi di pagamento o il sito web degli operatori commerciali online), dovrebbero essere adeguatamente protetti contro il furto e l'accesso o la modifica non autorizzati.

11.2 I prestatori di servizi di pagamento dovrebbero garantire che, durante lo scambio di dati sensibili relativi ai pagamenti via Internet, sia applicata la cifratura sicura da punto a punto (end-to-end encryption)[18] tra le parti comunicanti in tutta la rispettiva sessione di comunicazione, al fine di salvaguardare la riservatezza e l'integrità dei dati, utilizzando tecniche di cifratura forti e ampiamente riconosciute.

11.3 I prestatori di servizi di pagamento che offrono servizi di acquiring dovrebbero incoraggiare i loro operatori commerciali online a non conservare i dati sensibili relativi ai pagamenti. Nel caso in cui gli operatori commerciali online gestiscano, ossia conservino, trattino o trasmettano dati sensibili relativi ai pagamenti, tali prestatori di servizi di pagamento dovrebbero contrattualmente richiedere agli operatori commerciali online di predisporre delle misure necessarie per proteggere i dati. I prestatori di servizi di pagamento dovrebbero svolgere controlli periodici e, se un prestatore di servizi di pagamento viene a conoscenza del fatto che un operatore commerciale online che tratta dati sensibili relativi ai pagamenti non ha attuato come richiesto le misure di sicurezza, dovrebbe procedere all'adozione di misure per l'adempimento di tale obbligo contrattuale o alla risoluzione del contratto.

Sensibilizzazione, educazione e comunicazione riguardanti il cliente

Educazione e comunicazione riguardanti il cliente

12. I prestatori di servizi di pagamento dovrebbero fornire assistenza e orientamento ai clienti, ove necessario, per quanto riguarda l'uso sicuro dei servizi di pagamento via Internet. I prestatori di servizi di pagamento dovrebbero comunicare con i propri clienti in modo tale da rassicurarli circa l'autenticità dei messaggi ricevuti.

12.1 I prestatori di servizi di pagamento dovrebbero fornire almeno un canale protetto e sicuro [19] per la comunicazione periodica con i clienti per quanto riguarda l'uso corretto e sicuro del servizio di pagamento via Internet. I prestatori di servizi di pagamento dovrebbero informare i clienti riguardo all'esistenza di questo canale e comunicare che eventuali messaggi a nome del prestatore di servizi di pagamento forniti tramite altri mezzi, come per esempio le e-mail, e riguardanti l'utilizzo corretto e sicuro del servizio di pagamento via Internet, non sono affidabili. Il prestatore di servizi di pagamento dovrebbe spiegare:

[18] La cifratura da punto a punto (end-to-end encryption) si riferisce alla cifratura all'interno o alla fine del sistema di origine, con la cifratura corrispondente che si verifica solo all'interno o alla fine del sistema di destinazione. ETSI EN 302 109 V1.1.1. (2003-06).

[19] Come una casella di posta dedicata sul sito web del prestatore di servizi di pagamento o un sito web protetto.

- la procedura riservata ai clienti per segnalare al prestatore di servizi di pagamento (presunti) pagamenti fraudolenti, incidenti sospetti o anomalie durante la sessione per i servizi di pagamento via Internet e/o possibili tentativi di *social engineering*[20];

- le fasi successive, cioè in che modo il prestatore di servizi di pagamento risponderà al cliente;

- in che modo il prestatore di servizi di pagamento informerà il cliente circa (potenziali) operazioni fraudolente o il loro mancato ordine, o metterà in guardia il cliente circa il verificarsi di attacchi (per esempio le e-mail di phishing).

12.2 Attraverso il canale protetto, i prestatori di servizi di pagamento dovrebbero mantenere i clienti informati sugli aggiornamenti riguardanti le procedure di sicurezza in relazione ai servizi di pagamento via Internet. Eventuali avvisi sui rischi emergenti significativi (per esempio allerta circa il social engineering) dovrebbero essere forniti attraverso il canale protetto.

12.3 Servizi di assistenza dovrebbero essere messi a disposizione dei clienti dai prestatori di servizi di pagamento per qualsiasi domanda, reclamo, richiesta di supporto e comunicazione di anomalie o incidenti riguardanti i pagamenti via Internet e relativi servizi, e i clienti dovrebbero essere adeguatamente informati su come ottenere tale assistenza.

12.4 I prestatori di servizi di pagamento dovrebbero avviare programmi di educazione e di sensibilizzazione dei clienti destinati a garantire che i clienti comprendano, come minimo, la necessità di:

- proteggere le proprie password, token di sicurezza, dati personali e altri dati riservati;

- di gestire correttamente la sicurezza del dispositivo personale (per esempio il computer), attraverso l'installazione e l'aggiornamento di componenti di sicurezza (antivirus, firewall, patch di sicurezza);

- di prendere in considerazione le minacce e i rischi significativi legati al trasferimento di software via Internet, se il cliente non può essere ragionevolmente sicuro che il software sia autentico e che non sia stato manipolato;

- di utilizzare il sito web autentico del prestatore di servizi di pagamento per i pagamenti via Internet.

[20] Per social engineering in questo contesto si intendono le tecniche impiegate per manipolare le persone allo scopo di ottenere informazioni (per esempio, via e-mail o telefonate) o recuperare informazioni dai social network, per finalità fraudolente o per ottenere l'accesso non autorizzato a un computer o alla rete.

12.5 I prestatori di servizi di acquiring dovrebbero richiedere agli operatori commerciali online di separare chiaramente i processi relativi ai pagamenti da quelli inerenti il negozio online onde rendere più agevole per i clienti identificare quando comunicano con il prestatore di servizi di pagamento e non con il beneficiario (per esempio reindirizzando il cliente e aprendo una finestra separata in modo che il processo di pagamento non venga visualizzato all'interno di un contesto di commercio online).

Comunicazioni, fissazione di limiti

13. I prestatori di servizi di pagamento dovrebbero fissare limiti per i servizi di pagamento via Internet e potrebbero fornire ai loro clienti opzioni per ulteriori limitazioni del rischio entro tali limiti. Essi possono anche fornire servizi di gestione degli avvisi e dei profili dei clienti.

13.1 Prima di fornire a un cliente servizi di pagamento via Internet, i prestatori di servizi di pagamento dovrebbero fissare i limiti[21] applicabili a quei servizi (per esempio, un importo massimo per ogni singolo pagamento o un importo complessivo nel corso di un certo periodo di tempo) e dovrebbero informarne i loro clienti di conseguenza. I prestatori di servizi di pagamento dovrebbero consentire ai clienti di disattivare la funzionalità di pagamento via Internet.

Accesso dei clienti alle informazioni sullo stato dell'ordine e dell'esecuzione dei pagamenti

14. I prestatori di servizi di pagamento dovrebbero confermare ai propri clienti l'ordine del pagamento e fornire ai clienti in tempo utile le informazioni necessarie per verificare che l'operazione di pagamento sia stata avviata e/o eseguita correttamente.

14.1 [bonifici/mandato elettronico] I prestatori di servizi di pagamento dovrebbero garantire ai clienti una funzione quasi in tempo reale per controllare lo stato di esecuzione delle operazioni e i saldi contabili in qualsiasi momento[22] in un ambiente sicuro e affidabile.

14.2 Tutti gli estratti elettronici dettagliati dovrebbero essere messi a disposizione in un ambiente sicuro e affidabile. Se i prestatori di servizi di pagamento informano i clienti circa la disponibilità degli estratti conto elettronici (per esempio regolarmente quando un estratto conto elettronico periodico è stato emesso o su base ad hoc dopo l'esecuzione di un'operazione) attraverso un canale alternativo, come per esempio SMS, e-mail o per lettera, i dati sensibili relativi ai pagamenti non dovrebbero essere inclusi in tali comunicazioni o, se previsto, dovrebbero essere criptati.

[21] Tali limiti possono applicarsi globalmente (cioè a tutti gli strumenti di pagamento che consentono pagamenti via Internet) o singolarmente.

[22] Escludendo i casi eccezionali di mancata disponibilità della struttura per motivi di manutenzione tecnica o in ragione di incidenti.

Titolo III – Disposizioni finali e attuazione

15. I presenti orientamenti si applicano a partire dal 01.08/2015.

Allegato 1: Esempi di migliori prassi (MP)

Oltre ai requisiti di cui sopra, i presenti orientamenti descrivono alcune procedure che i prestatori di servizi di pagamento e gli operatori di mercato coinvolti sono invitati, ma non tenuti, ad adottare. Per facilità di riferimento, i capitoli cui si applicano le migliori prassi (MP) sono indicati in modo esplicito.

Controllo generale e ambiente di sicurezza

Governance

MP 1: La politica di sicurezza potrebbe essere delineata in un apposito documento.

Controllo e mitigazione dei rischi

MP 2: I prestatori di servizi di pagamento potrebbero fornire strumenti di sicurezza (per esempio, dispositivi e/o browser personalizzati, resi adeguatamente sicuri) per proteggere l'interfaccia applicativa resa disponibile all'utente contro l'uso illegale o attacchi (per esempio gli attacchi di tipo "man in the browser").

Tracciabilità

MP 3: I prestatori di servizi di pagamento che offrono servizi di acquiring potrebbero richiedere contrattualmente agli operatori commerciali online di conservare le informazioni di pagamento per avere adeguati processi in essere a supporto della tracciabilità.

Misure specifiche di controllo e di sicurezza per i pagamenti via Internet

Identificazione iniziale dei clienti, informazioni

MP 4: Il cliente potrebbe sottoscrivere un contratto di servizio dedicato per lo svolgimento di operazioni di pagamento via Internet, anziché le condizioni contrattuali incluse in un contratto di servizio generale più ampio con il prestatore di servizi di pagamento.

MP 5: I prestatori di servizi di pagamento potrebbero anche garantire che i clienti ricevano, in modo continuativo o, se del caso, ad hoc, e con mezzi adeguati (per esempio volantini, pagine di siti web), istruzioni chiare e semplici che spieghino le loro responsabilità nell'uso sicuro del servizio.

Autenticazione forte del cliente

MP 6: [carte] Gli operatori commerciali online (e-merchant) potrebbero supportare l'autenticazione forte del titolare della carta da parte dell'emittente nell'ambito delle operazioni con carta via Internet.

MP 7: Per comodità del cliente, i prestatori di servizi di pagamento potrebbero valutare la possibilità di utilizzare un unico strumento di autenticazione forte degli utenti per tutti i servizi di pagamento via Internet. Questo potrebbe aumentare l'accettazione della soluzione fra i clienti e facilitare un uso corretto.

MP 8: L'autenticazione forte dei clienti potrebbe includere elementi in grado di collegare l'autenticazione di un importo specifico e del beneficiario. Ciò potrebbe fornire ai clienti una maggiore certezza quando autorizzano i pagamenti. La soluzione tecnologica che consente il collegamento fra i dati di autenticazione forte e i dati delle operazioni dovrebbe essere a prova di manipolazioni.

Protezione dei dati sensibili relativi ai pagamenti

MP 9: È auspicabile che gli operatori commerciali online che gestiscono dati sensibili relativi ai pagamenti formino adeguatamente il loro personale che si occupa di gestione delle frodi e aggiornino regolarmente la loro formazione per garantire che il contenuto rimanga pertinente a un ambiente di sicurezza dinamico.

Educazione e comunicazione riguardanti il cliente

MP 10: È auspicabile che i prestatori di servizi di acquiring organizzino programmi educativi per i loro operatori commerciali online in materia di prevenzione delle frodi.

Comunicazioni, fissazione di limiti

MP 11: Entro i limiti stabiliti, i prestatori di servizi di pagamento potrebbero fornire ai propri clienti la possibilità di gestire i limiti per i servizi di pagamento via Internet in un ambiente sicuro e affidabile.

MP 12: I prestatori di servizi di pagamento potrebbero prevedere avvisi per i clienti, per esempio attraverso telefonate o SMS, per le operazioni di pagamento sospette o a rischio elevato in base alle proprie politiche di gestione dei rischi.

MP 13: I prestatori di servizi di pagamento potrebbero consentire ai clienti di specificare le regole generali, e quelle personalizzate come parametri per il loro comportamento nei pagamenti via Internet e nei servizi correlati, per esempio specificando che essi ordineranno pagamenti solo da alcuni paesi specifici e che i pagamenti avviati da altri luoghi dovrebbero essere bloccati, o che essi possono includere beneficiari specifici figuranti nelle "white list" o "black list".