

**Osservazioni di Assofin al Documento di consultazione di
Banca d'Italia**

**“Recepimento in Italia degli Orientamenti dell’ABE in
materia di sicurezza dei pagamenti tramite canale
Internet”**

OTTOBRE 2015



Premessa

Assofin, Associazione Italiana del Credito al Consumo ed Immobiliare, desidera anzitutto esprimere apprezzamento per l'iniziativa di Banca d'Italia finalizzata a modificare la disciplina dei prestatori di servizio di pagamento per recepire gli "Orientamenti in materia di sicurezza dei pagamenti via internet" adottati dall'Autorità Bancaria Europea (ABE) il 18 dicembre 2014.

Il presente Position Paper contiene osservazioni e richieste di chiarimento su aspetti controversi degli indirizzi espressi da Banca d'Italia per il recepimento e degli stessi Orientamenti dell'EBA.

Vista la rilevanza del tema trattato per le nostre Associate, si confida in un dialogo fruttuoso con l'Autorità di Vigilanza, per il quale la scrivente resta a disposizione.

Osservazioni e richieste di chiarimento a documento in consultazione "Recepimento in Italia degli Orientamenti dell'ABE in materia di sicurezza dei pagamenti tramite canale Internet".

RECEPIMENTO IN ITALIA DEGLI ORIENTAMENTI DELL'ABE IN MATERIA DI SICUREZZA DEI PAGAMENTI TRAMITE CANALE INTERNET – Paragrafo 2

Andrebbe chiarito in che misura i prestatori di servizi di pagamento abbiano la facoltà di declinare il rispetto dei principi secondo proporzionalità, derogando dai contenuti degli Orientamenti dell'EBA. Occorrerebbe in altre parole che la suddetta proporzionalità fosse qualificata in relazione ai principi stessi e alle migliori prassi, mettendola al tempo stesso in relazione con il contrastante venir meno della facoltà di "comply or explain".

RECEPIMENTO IN ITALIA DEGLI ORIENTAMENTI DELL'ABE IN MATERIA DI SICUREZZA DEI PAGAMENTI TRAMITE CANALE INTERNET – Paragrafo 3

L'adeguamento richiesto alle migliori prassi specificate nell'allegato 1 degli Orientamenti dell'EBA, a cui Banca d'Italia attribuisce natura obbligatoria diversamente da quanto statuito negli Orientamenti, potrebbe comportare minori margini di manovra e conseguentemente costi più significativi per i soggetti italiani sottoposti a vigilanza, che si troverebbero in posizione di svantaggio rispetto ai loro omologhi europei.

Un esempio particolarmente rilevante a questo riguardo è quello della raccomandazione MP8, in cui si introduce la possibilità di verificare importo e beneficiario di una transazione con carta, cosa che precluderebbe



l'impiego per l'autenticazione forte di codici di verifica di tipo "3D Secure" già adottati dai principali Brand, ponendo quindi l'intermediario nell'obbligo di fatto di sviluppare soluzioni ad hoc.

ORIENTAMENTI FINALI DELL'EBA SULLA SICUREZZA DEI PAGAMENTI VIA INTERNET

Titolo I - AMBITO DI APPLICAZIONE E DEFINIZIONI

Premettendo che le disposizioni in esame sono applicabili alle transazioni effettuate su internet successivamente all'entrata in vigore delle medesime, si chiede di chiarire se le stesse siano riferibili anche ai rapporti sorti anteriormente rispetto a tale termine. In tal caso si chiede di chiarire in che modo fornire ai clienti le informazioni previste dalle medesime disposizioni.

Punto 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:

- [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.

Si chiede di chiarire se siano ricompresi nella nozione di "bonifici via internet" le richieste di utilizzo del fido disponibile residente sulla carta di credito mediante erogazione di somme su conto del cliente effettuate da quest'ultimo tramite area riservata on line.

In particolare, si chiede se l'esecuzione di tali bonifici via internet in situazioni di rischio particolarmente ridotto (quando l'unico beneficiario può essere lo stesso utilizzatore dello strumento di pagamento) possa essere considerato al di fuori dell'ambito di applicazione degli Orientamenti per limitare gli aggravii conseguenti all'applicazione letterale del testo agli intermediari.



Titolo II – ORIENTAMENTI SULLA SICUREZZA DEI PAGAMENTI VIA INTERNET

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

Identificazione iniziale dei clienti, informazioni

Punto 6.

I clienti dovrebbero essere adeguatamente identificati in linea con la normativa europea antiriciclaggio 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.

"... i clienti dovrebbero ... confermare la loro volontà di effettuare pagamenti via Internet utilizzando i servizi prima di poter accedere a tali servizi": si chiede di chiarire se in assenza di un'esplicita accettazione da parte del cliente all'utilizzo di quegli strumenti l'intermediario debba escludere la possibilità di transare su web.

Si chiede di chiarire in che modo l'emittente della carta di credito possa consentire ai clienti di confermare la volontà di effettuare pagamenti via internet prima di poter accedere al servizio di pagamento ed in particolare se sia sufficiente l'inserimento nel contratto quadro di un riferimento alla possibilità di utilizzare la carta di credito per effettuare operazioni di pagamento su internet.

Si chiede di chiarire in che modo l'emittente della carta di credito debba fornire al cliente l'informativa di cui all'art. 6 ed in particolare se sia sufficiente l'indicazione della stessa nel sito internet dello stesso ovvero se sia necessario integrare la stessa nel contratto quadro.

Punto 6.2

I prestatori di servizi di pagamento dovrebbero garantire che le informazioni preliminari 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.

Si chiede di chiarire se le richiamate informazioni possano essere riportate nell'informativa di cui all'art. 6.

Punto 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 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.

Si chiede di chiarire se sia sufficiente che il contratto quadro preveda il blocco dello strumento di pagamento per problemi di sicurezza ovvero se sia necessario, per gli stessi motivi, prevedere anche un blocco della singola operazione di pagamento, anche alla luce di quanto previsto dalle vigenti disposizioni in tema di servizi di pagamento.

Si chiede di chiarire se sia sufficiente prevedere nel contratto quadro che lo strumento di pagamento sarà sbloccato al venir meno dei rilevati problemi di sicurezza ovvero se sia necessario prevedere una procedura che consenta al cliente di chiedere lo sblocco dello stesso, anche alla luce di quanto previsto dalle vigenti disposizioni in tema di servizi di pagamento.

Autenticazione forte del cliente

Punto 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.

Punto 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.

Si chiede di chiarire quali siano gli adempimenti a carico dell'emittente della carta di credito per supportare l'identificazione forte del titolare della carta ed in particolare se sia necessario corredare la carta di dispositivi come token o smart card o di codici di accesso a prescindere dal fatto che il sito su cui verrà effettuato l'acquisto ne consenta l'utilizzo, quindi impedendo al titolare di fruire degli stessi.

Risulta chiaro che l'issuer debba essere predisposto all'autenticazione forte del titolare, appare meno chiaro se il titolare possa scegliere se aderire o meno.

Si chiede di chiarire se, ai fini dell'assolvimento dell'obbligo di autenticazione forte del titolare della carta, sarebbe sufficiente l'adozione da parte di un emittente per le proprie carte di un sistema 3D secure.

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

Punto 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

Si chiede di chiarire se gli emittenti di carte di credito siano tenuti ad incoraggiare il cliente ad adottare le misure di sicurezza messe in atto o debbano obbligare il cliente ad aderire.

Inoltre, in caso di obbligo ad aderire e non di semplice incoraggiamento, andrebbe chiarito se l'emittente deve obbligare il cliente ad "iscriversi" al servizio, lasciando a questo la libertà di attivare/disattivare il servizio, oppure se il servizio di sicurezza debba obbligatoriamente essere attivo al fine di poter effettuare transazioni su web.



Nel 7.3 si richiede all'emittente di supportare l'autenticazione forte, mentre nell'8.2 si lascia spazio al cliente di aderire o meno al servizio. I due articoli sembrano contraddittori.

Inoltre, si chiede di chiarire se la valutazione del rischio legato all'operazione specifica con carta possa essere totalmente in carico all'emittente. Si chiede di specificare eventuali criteri per poter definire un'operazione rischiosa e di chiarire se ci si possa basare su statistiche interne aziendali.

Comunicazioni, fissazioni di limiti

Punto 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.

Art. 13.1

Prima di fornire a un cliente servizi di pagamento via Internet, i prestatori di servizi di pagamento dovrebbero fissare i limiti 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.

Si chiede di chiarire se le facoltà di limitare l'utilizzo dello strumento di pagamento per operazioni via internet debba essere inserita nel contratto quadro ovvero se si ritenga sufficiente darne informazione tramite il sito internet dell'emittente.