**RESOCONTO DELLA 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
RESOCONTO DELLA CONSULTAZIONE**

<i>Rispondenti</i>	<p>Hanno risposto alla consultazione:</p> <ul style="list-style-type: none"> • ABI • Assofin • Federcasse • Mastercard <p>Due rispondenti hanno chiesto di mantenere riservati i propri commenti.</p>
--------------------	---

<i>Legenda</i>	PSP	Prestatori di servizi di pagamento
	MP	Migliori prassi
	PSD	Direttiva 2007/64/CE
	PSD2	Direttiva (UE) 2015/2366

Commenti alle disposizioni

ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/in parte/Chiarimento)	COMMENTO
<i>Ambito di applicazione</i>	<p>È stato evidenziato che l'applicazione degli Orientamenti, destinati ai prestatori di servizi di pagamento come attualmente definiti dalla PSD, potrebbe generare distorsioni nella concorrenza alla luce del diverso ambito di applicazione previsto dalla nuova direttiva sui servizi di pagamento (PSD2), pubblicata lo scorso 23 dicembre, che prevede:</p> <p>(i) rinnovate condizioni per l'esenzione delle operazioni di pagamento effettuate per il tramite degli operatori di telefonia; e</p> <p>(ii) l'inclusione tra i soggetti destinatari delle norme delle cc.dd. "Terze Parti".</p>	Chiarimento	<p>Si fa presente che sia gli Orientamenti, sia le disposizioni della Banca d'Italia si attengono all'ambito di applicazione definito dal quadro normativo vigente, rappresentato dalla PSD e, in Italia, dal d.lgs. 11/2010.</p> <p>Con riferimento agli esempi riportati:</p> <p>i) le ipotesi di esenzione sono definite dal legislatore UE con l'obiettivo di realizzare un bilanciamento tra servizi di pagamento riservati a intermediari autorizzati e fattispecie escluse dall'ambito di applicazione in ragione di alcune loro particolari caratteristiche;</p> <p>ii) le cc.dd. "Terze Parti" non rientrano, in base alla normativa vigente, tra i soggetti sottoposti alla PSD.</p>

**RECEPIMENTO IN ITALIA DEGLI ORIENTAMENTI DELL'ABE IN MATERIA DI SICUREZZA DEI PAGAMENTI TRAMITE CANALE INTERNET
RESOCONTO DELLA CONSULTAZIONE**

ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/in parte/Chiarimento)	COMMENTO
<p>Rimozione del principio di “comply or explain” e tempi di adeguamento</p>	<p>È stato osservato che la rimozione del principio del “<i>comply or explain</i>” richiederebbe un’ulteriore analisi delle attività già realizzate e dei progetti in corso di realizzazione presso le banche, con un conseguente impatto sui tempi di adeguamento.</p> <p>È stato infine chiesto di mantenere la clausola del “<i>comply or explain</i>” ovvero di concedere a tutti i PSP un anno per l’adeguamento al contenuto degli Orientamenti.</p>	<p align="center">In parte</p>	<p>La rimozione del principio del “<i>comply or explain</i>” rappresenta uno dei principali elementi di novità derivanti dall’incorporazione delle Raccomandazioni della Banca Centrale Europea negli Orientamenti dell’EBA, che, con tale trasposizione, si propone di accrescere il grado di armonizzazione e sicurezza nel settore dei pagamenti via internet.</p> <p>Alla luce degli elementi acquisiti nel corso della consultazione sugli impatti derivanti dalla rimozione del principio di “<i>comply or explain</i>”, agli operatori è stato riconosciuto un congruo periodo di tempo entro il quale implementare le disposizioni di recepimento degli Orientamenti.</p>
	<p>È stato evidenziato che la rimozione del principio del “<i>comply or explain</i>”, cui conseguirebbe, in particolare, l’obbligo di applicare l’autenticazione forte ad ogni transazione, introdurrebbe delle rigidità non opportune né per gli esercenti né per i clienti. In tale ottica, è suggerita l’adozione di un approccio “<i>risk-based</i>” che consenta di assoggettare ad autenticazione forte solo le transazioni che presentino un elevato livello di rischiosità.</p>	<p align="center">Chiarimento</p>	<p>Considerata la rilevanza che il raggiungimento di elevati livelli di sicurezza nel settore dei pagamenti via internet assume per il sano sviluppo del mercato dei pagamenti europeo, gli Orientamenti, in linea con le Raccomandazioni della BCE, prevedono come regola di carattere generale il ricorso all’autenticazione forte per l’inoltro di operazioni di pagamento.</p> <p>L’approccio “<i>risk-based</i>” nel ricorso all’autenticazione forte è comunque parte integrante anche del quadro regolamentare introdotto con gli Orientamenti.</p> <p>L’Orientamento n. 7 identifica infatti determinate tipologie di operazioni per le quali l’autenticazione può essere effettuata con modalità alternative a quelle previste in via generale, qualora tale scelta sia supportata da una adeguata analisi dei rischi connessi alle transazioni in parola (cfr. ad esempio, le transazioni</p>

**RECEPIMENTO IN ITALIA DEGLI ORIENTAMENTI DELL'ABE IN MATERIA DI SICUREZZA DEI PAGAMENTI TRAMITE CANALE INTERNET
RESOCONTO DELLA CONSULTAZIONE**

ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/in parte/Chiarimento)	COMMENTO
			effettuate con carte di pagamento di cui al Titolo II, par. 7.5).
Migliori prassi	<p>È stato messo in evidenza che il livello di rischio del settore dei pagamenti informatici sarebbe allo stato non significativo (nel 2014, sarebbe infatti stato bloccato oltre il 97% dei tentativi di attacco ai servizi di internet banking). Pur condividendo in generale l'adozione di soluzioni tecniche evolutive, l'imposizione dei presidi previsti dalle Migliori prassi (MP), con particolare riferimento all'autenticazione della transazione di cui alla MP 8, risulterebbe eccessivamente onerosa rispetto al rischio effettivamente sopportato dal sistema. Essa rischierebbe inoltre di incidere negativamente sull'usabilità dei servizi di pagamento da parte dei clienti. In generale, è stato chiesto di non prevedere l'obbligatorietà delle Migliori prassi, valutandone preliminarmente rischi e benefici.</p> <p>È stato altresì evidenziato che:</p> <p>(a) la PSD2 concederebbe ai prestatori di servizi di pagamento tempi più lunghi per l'implementazione di misure analoghe a quelle previste dalle Migliori prassi. Tale imposizione rischierebbe pertanto di incidere negativamente sulla competitività degli operatori nazionali;</p>	Sì	<p>Il perseguimento di elevati livelli di sicurezza nelle transazioni via internet rappresenta un obiettivo primario del legislatore europeo ed è condiviso dalla Banca d'Italia. Per perseguire tale finalità, gli Orientamenti richiedono l'adozione di alcuni presidi di sicurezza, destinati ad essere ulteriormente rafforzati con l'entrata in vigore della PSD2. Il raggiungimento di tale obiettivo va tuttavia bilanciato con l'opportunità di favorire lo sviluppo dell'innovazione tecnologica e migliorare l'usabilità degli strumenti di pagamento da parte della clientela.</p> <p>Si tratta di un tema su cui il quadro normativo europeo risulta ancora in evoluzione. In particolare, la PSD2 disciplina gli obblighi di autenticazione della transazione con riferimento all'importo e al destinatario del pagamento, oggetto della MP 8, rimettendo all'EBA la definizione delle regole tecniche e dei casi di esenzione (cfr. al riguardo anche il documento dell'EBA "Discussion paper on Draft Regulatory Technical Standard on strong customer authentication and secure communication under the revised PSD2", disponibile all'indirizzo: https://www.eba.europa.eu/documents/10180/1303936/EBA-DP-2015-03+%28RTS+on+SCA+and+CSC+under+PSD2%29.pdf).</p> <p>Ciò posto, nelle more del consolidamento del quadro normativo europeo, la cui completa attuazione sarebbe</p>

**RECEPIMENTO IN ITALIA DEGLI ORIENTAMENTI DELL'ABE IN MATERIA DI SICUREZZA DEI PAGAMENTI TRAMITE CANALE INTERNET
RESOCONTO DELLA CONSULTAZIONE**

ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/in parte/Chiarimento)	COMMENTO
	(b) le attività necessarie per l'adozione delle MP, qualora imposte come obbligatorie, richiederebbero investimenti significativi i cui costi e tempi di attuazione risultano allo stato difficilmente stimabili, tenuto conto che sarebbe necessario procedere alla revisione dei progetti di <i>risk assessment</i> già realizzati o in corso e dei relativi <i>budget</i> .		prevista non prima di ottobre 2018, le disposizioni tengono conto delle osservazioni ricevute e non rendono obbligatorie le Migliori prassi. Resta ovviamente ferma la possibilità per gli intermediari di tenerne conto al momento della definizione delle scelte da assumere per conformarsi al contenuto degli Orientamenti.
Altri aspetti	È stato messo in evidenza che la trasposizione nel nostro ordinamento degli Orientamenti e delle Migliori prassi potrebbe generare disparità di natura competitiva per gli operatori italiani rispetto a quelli esteri e operativa per gli operatori con articolazione internazionale.	Chiarimento	<p>Si fa presente che non si ritiene che si creino disparità competitive tra operatori europei, posto che la maggior parte dei paesi dell'UE ha recepito o intende recepire gli Orientamenti nei rispettivi ordinamenti (cfr. http://www.eba.europa.eu/documents/10180/934179/EB_A-GL-2014-12+Compliance+Table-GL+security+of+internet+payments.pdf/34be3c3e-5521-4036-9805-3ee97162c4db).</p> <p>Per quanto concerne le MP, si rinvia a quanto esposto sopra.</p>
Titolo I – Ambito di applicazione e definizioni Paragrafo 12 – “Soluzioni wallet”	È stato chiesto di includere nella definizione di “ <i>soluzioni wallet</i> ” le fattispecie in cui la carta non viene utilizzata per effettuare un pagamento diretto nei confronti dell'esercente, ma per caricare il conto presso il PSP, con conseguente successivo trasferimento di fondi dal conto all'esercente.	No	<p>La definizione di “<i>soluzioni wallet</i>” è prevista dagli Orientamenti e si riferisce a soluzioni in cui il cliente può registrare i dati relativi ad uno o più strumenti di pagamento per effettuare pagamenti presso diversi esercenti.</p> <p>Ciò posto, fatte salve le ipotesi di esclusione espressamente previste, gli Orientamenti (con particolare riferimento all'autenticazione forte) trovano applicazione nel caso di utilizzo della carta per il caricamento del conto presso il PSP, con il conseguente successivo trasferimento di fondi dal conto all'esercente.</p>

**RECEPIMENTO IN ITALIA DEGLI ORIENTAMENTI DELL'ABE IN MATERIA DI SICUREZZA DEI PAGAMENTI TRAMITE CANALE INTERNET
RESOCONTO DELLA CONSULTAZIONE**

ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/in parte/Chiarimento)	COMMENTO
Titolo I – Ambito di applicazione e definizioni Paragrafo 7	È stato chiesto di limitare l'applicazione dell'autenticazione forte al solo processo di generazione dei dati delle carte virtuali su internet e non anche alle transazioni con carte virtuali.	No	La richiesta non può essere accolta in quanto non in linea con il contenuto degli Orientamenti, che nell'identificare le operazioni di pagamento soggette alla disciplina in esame, assimilano espressamente le operazioni di pagamento effettuate mediante carte virtuali a quelle effettuate mediante carte fisiche (cfr. Titolo I, par 7 primo alinea).
	È stato chiesto di chiarire se siano ricomprese nella nozione "bonifici via internet" le richieste di utilizzo del fido disponibile residente sulla carta di credito mediante erogazione di somme sul conto del cliente effettuate da quest'ultimo tramite area riservata on line. In particolare, è stato chiesto 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.	Chiarimento	Sulla base delle informazioni rese, la fattispecie in esame sembra configurare un pagamento con carta rientrante nell'ambito di applicazione degli Orientamenti. Si rammenta tuttavia quanto previsto dall'Orientamento 7.5, in base al quale, per le operazioni di pagamento effettuate tramite carte, è ammesso l'uso di misure di autenticazione alternative al ricorrere delle condizioni ivi specificate (ossia pre-identificazione delle tipologie di transazioni e profilo di rischio basso).
Titolo I – Ambito di applicazione e definizioni	È stato chiesto di chiarire se le disposizioni si applicano anche ai rapporti sorti anteriormente all'entrata in vigore delle medesime. In tal caso si chiede di chiarire in che modo fornire ai clienti le informazioni previste dalle disposizioni.	Chiarimento	Le disposizioni previste dagli Orientamenti si applicano ai rapporti sorti successivamente alla data di entrata in vigore delle nuove disposizioni.
Titolo I – Ambito di	È stato chiesto di introdurre margini di	No	L'interpretazione proposta non è in linea con il contenuto

**RECEPIMENTO IN ITALIA DEGLI ORIENTAMENTI DELL'ABE IN MATERIA DI SICUREZZA DEI PAGAMENTI TRAMITE CANALE INTERNET
RESOCONTO DELLA CONSULTAZIONE**

ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/in parte/Chiarimento)	COMMENTO
applicazione e definizioni Paragrafo 12	flessibilità nel ricorso all'autenticazione forte, ammettendo la derogabilità del principio in base al quale almeno uno degli elementi richiesti per l'autenticazione sia non riutilizzabile e non replicabile e non atto a essere indebitamente carpito via Internet.		degli Orientamenti, che nel definire l'autenticazione forte richiedono espressamente che almeno uno degli elementi che la compongono (di quelli classificati nelle categorie "conoscenza" e "possesso") sia non riutilizzabile, non replicabile e non atto a essere indebitamente carpito via Internet.
	È stato chiesto di chiarire che gli elementi di autenticazione debbano ritenersi "indipendenti" quando uno di essi non sia "direttamente" compromesso per effetto della compromissione dell'altro.	Chiarimento	Sulla base del quadro normativo vigente, il rispetto del principio in base al quale gli elementi costitutivi dell'autenticazione forte devono essere indipendenti l'uno dall'altro non può che essere valutato caso per caso in relazione alle specifiche soluzioni adottate. Tenuto conto che il tema è peraltro attualmente all'attenzione delle istituzioni comunitarie (cfr. <i>EBA's Discussion paper on Draft Regulatory Technical Standard on strong customer authentication and secure communication under the revised PSD2</i> "), si fa riserva di tornare in argomento quando saranno fornite indicazioni applicative del principio in esame.
Principio di proporzionalità	È stato chiesto di chiarire il principio di proporzionalità qualificandolo in relazione agli Orientamenti e alle Migliori prassi, mettendolo in relazione con il venir meno della facoltà di "comply or explain".	Chiarimento	Posto che le Migliori prassi non saranno obbligatorie, mentre lo saranno gli Orientamenti, ciascun presidio potrà essere individuato tenendo conto delle dimensioni del PSP e della sua complessità operativa, nonché dell'effettiva esposizione ai rischi (anche reputazionali) connessi all'offerta alla propria clientela di servizi di pagamento tramite il canale Internet.
Orientamento 3.4	È stato chiesto di non imporre ai PSP l'obbligo di inserire nei contratti stipulati con gli esercenti clausole che impongano a questi ultimi l'obbligo di cooperare in caso di gravi	Chiarimento	La cooperazione degli esercenti nel monitoraggio degli incidenti di sicurezza, prevista solo nel caso in cui gli esercenti conservino, processino o trasmettano dati sensibili relativi ai pagamenti (identificati secondo

**RECEPIMENTO IN ITALIA DEGLI ORIENTAMENTI DELL'ABE IN MATERIA DI SICUREZZA DEI PAGAMENTI TRAMITE CANALE INTERNET
RESOCONTO DELLA CONSULTAZIONE**

ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/in parte/Chiarimento)	COMMENTO
	<p>incidenti di sicurezza, qualora conservino, processino o trasmettano dati sensibili relativi ai pagamenti, tenuto conto che la modifica dei testi contrattuali risulterebbe eccessivamente costosa rispetto ai potenziali benefici, in assenza di efficaci strumenti per assicurarne il rispetto.</p> <p>È stato altresì evidenziato che la rimozione del principio di <i>"comply or explain"</i> avrebbe un considerevole impatto sui contratti di <i>acquiring</i> stipulati con gli esercenti <i>online</i> che conservano, elaborano o trasmettono dati sensibili relativi ai pagamenti, indipendentemente dal rischio correlato o dalle dimensioni degli esercenti stessi (Orientamento 3.4).</p>		<p>quanto richiamato nella presente Tavola nel Commento sub "Orientamento 7"), rappresenta un fattore di rilievo per l'innalzamento dei livelli di sicurezza nel settore dei pagamenti via internet.</p> <p>Indipendentemente dalle misure che possono essere previste contrattualmente per assicurare tale cooperazione, rimesse all'autonomia delle parti, che peraltro possono essere declinate secondo proporzionalità, è pertanto necessario che detti obblighi di cooperazione siano contrattualmente disciplinati.</p>
Orientamento 4	<p>È stato osservato che l'inserimento in un contratto di clausole che impongano all'esercente il rispetto delle misure di controllo e attenuazione dei rischi previste dai punti da 4.1 a 4.7 presenta criticità sia per il contenuto estremamente tecnico delle stesse, sia per la circostanza che le regole di sicurezza potrebbero richiedere la necessità di aggiornamenti frequenti e con caratteristiche di urgenza e immediatezza che mal si conciliano con le tempistiche richieste dalla normativa italiana (art. 126 sexies TUB) in tema di modifica unilaterale dei contratti.</p>	Chiarimento	<p>Si richiama preliminarmente l'attenzione sulla circostanza che la previsione in esame trova applicazione solo nel caso in cui gli esercenti conservino, processino o trasmettano dati sensibili relativi ai pagamenti (identificati secondo quanto richiamato nella presente Tavola nel Commento sub "Orientamento 7"). Risulta pertanto coerente con l'obiettivo degli Orientamenti e con gli obblighi imposti ai prestatori di servizi di pagamento assicurare che tali esercenti dispongano di presidi di sicurezza adeguati a evitare il furto di dette informazioni.</p> <p>Quanto alle specifiche regole di sicurezza, i principi richiamati nei punti da 4.1 a 4.7 hanno natura esemplificativa e generale. La loro concreta imposizione</p>

**RECEPIMENTO IN ITALIA DEGLI ORIENTAMENTI DELL'ABE IN MATERIA DI SICUREZZA DEI PAGAMENTI TRAMITE CANALE INTERNET
RESOCONTO DELLA CONSULTAZIONE**

ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/in parte/Chiarimento)	COMMENTO
			andrà valutata con riferimento all'effettivo livello di rischio rilevato dal PSP.
Orientamento 5	È stato rilevato che l'eliminazione del principio di "comply or explain" determinerebbe una maggiore complessità nella tracciabilità delle transazioni, che richiederebbe l'analisi periodica di cc.dd. "file di log" per la rilevazione di operazioni sospette e non più solo in caso di violazioni o di frodi.	Chiarimento	L'Orientamento in oggetto mira ad assicurare che i PSP abbiano in essere presidi che consentano di tracciare le transazioni e che i processi di gestione del mandato elettronico siano adeguatamente registrati. Resta ferma la possibilità di declinare le modalità di attuazione dell'Orientamento in esame secondo proporzionalità (inclusa la frequenza dell'analisi periodica dei "file di log"), calibrando i presidi in base alla dimensione e alla complessità del PSP, nonché all'effettiva esposizione ai rischi connessi al servizio di pagamento prestato.
Orientamento 6	È stato chiesto di chiarire come l'emittente della carta possa consentire ai clienti di confermare la loro 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.	Chiarimento	Gli Orientamenti non prescrivono modalità specifiche di adempimento. Tra le modalità possibili, rimesse alla valutazione dell'intermediario, nel rispetto della disciplina generale in materia di Trasparenza dei servizi bancari e finanziari - Correttezza delle relazioni tra intermediari e clienti, si ritiene adeguata anche una specifica previsione contenuta nel contratto quadro. In ogni caso, sarà cura dell'intermediario adottare ogni misura utile a far sì che il cliente abbia piena consapevolezza di tale possibilità di utilizzo dello strumento.
	È stato chiesto di chiarire in che modo l'emittente della carta di credito debba fornire al cliente l'informativa di cui all' Orientamento 6 (circa i requisiti necessari per l'esecuzione in sicurezza delle operazioni di pagamento via internet) ed, in particolare, se sia sufficiente l'indicazione della stessa sul sito internet dell'intermediario ovvero se sia	Chiarimento	In base alla struttura degli Orientamenti, si è dell'avviso che le informazioni da rendere ai sensi del paragrafo 6.2 (che includono informazioni su apparecchiature e procedure) rappresentano una specificazione del principio di carattere generale fissato dal paragrafo 6. Esse, pertanto, devono essere rese nell'ambito dell'informazione preventiva di cui all'art. 41 PSD, così come recepito in Italia dal D.lgs. n. 11/2010 e dalle

**RECEPIMENTO IN ITALIA DEGLI ORIENTAMENTI DELL'ABE IN MATERIA DI SICUREZZA DEI PAGAMENTI TRAMITE CANALE INTERNET
RESOCONTO DELLA CONSULTAZIONE**

ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/in parte/Chiarimento)	COMMENTO
	<p>necessario integrare la stessa nel contratto quadro. È stato inoltre chiesto di chiarire se le specifiche informazioni richieste al punto 6.2 (riguardanti, ad esempio, le apparecchiature disponibili, le modalità di utilizzo delle credenziali, procedure da seguire in caso di frodi) possano essere fornite con le stesse modalità previste per l'informativa di carattere più generale richiesta dall'Orientamento 6.</p>		<p>disposizioni della Banca d'Italia in materia di "Trasparenza dei servizi bancari e finanziari – Correttezza delle relazioni tra intermediari e clienti".</p>
	<p>È stato chiesto di chiarire se, in base a quanto previsto dall'Orientamento 6.3, 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.</p> <p>È stato inoltre chiesto se sia sufficiente prevedere nel contratto quadro che lo strumento di pagamento sarà sbloccato al venir meno dei rilevanti 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.</p>	<p>Chiarimento</p>	<p>In linea con quanto previsto dalle Disposizioni in materia di trasparenza dei servizi bancari e finanziari – Correttezza delle relazioni tra intermediari e clienti, Sezione VI, par. 4.1.1, lett. e), il contratto quadro include informazioni relative all'eventuale blocco/sblocco dello strumento di pagamento, nel rispetto di quanto previsto dall'art. 6 del d.lgs. n. 11/2010. Le condizioni per l'eventuale blocco di singole transazioni per problemi di sicurezza, ove previste, sono comunque regolate contrattualmente in forma scritta. Fermo restando che lo sblocco dello strumento di pagamento può avvenire solo al ricorrere delle condizioni previste dall'art. 6, comma 4, d.lgs. 11/2010, devono essere previste procedure specifiche per consentire al cliente di richiedere direttamente al prestatore di servizi di pagamento lo sblocco dello strumento, in linea con quanto previsto dall'art. 8, comma 1, lett. c), del medesimo decreto.</p>
	<p>È stato chiesto di consentire al PSP di fornire le informazioni relative all'utilizzo dei servizi via internet al cliente nella sede e nel</p>		<p>Le Disposizioni in materia di trasparenza delle operazioni e dei servizi bancari e finanziari – Correttezza delle relazioni tra intermediari e clienti, Sezione IV, par.</p>

**RECEPIMENTO IN ITALIA DEGLI ORIENTAMENTI DELL'ABE IN MATERIA DI SICUREZZA DEI PAGAMENTI TRAMITE CANALE INTERNET
RESOCONTO DELLA CONSULTAZIONE**

ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/in parte/Chiarimento)	COMMENTO
	<p>momento che ritiene opportuno (ad esempio, al momento in cui il cliente mostra interesse per l'operatività online) e con strumenti che ne consentano l'immediato aggiornamento in caso di evoluzioni tecnologiche e/o richieste da una mutazione dei rischi, non già nell'ambito dell'informazione precontrattuale prevista dalle Disposizioni in materia di trasparenza delle operazioni e dei servizi bancari e finanziari – Correttezza delle relazioni tra intermediari e clienti, per evitare di rendere al cliente una quantità eccessiva di informazioni.</p>		<p>4.1.1, richiedono che prima della conclusione del contratto siano rese al cliente informazioni, tra l'altro, sulle principali caratteristiche dei servizi, incluse forma e modalità per prestare o revocare il consenso ad un'operazione di pagamento. Le informazioni di cui all'Orientamento 6.2 si configurano, nella sostanza, come una specificazione di obblighi informativi già facenti capo ai PSP, che pertanto andranno rese anticipatamente nell'ipotesi di servizi di pagamento offerti tramite il canale internet. L'elenco delle informazioni previste dall'Orientamento ha peraltro natura esemplificativa.</p>
	<p>È stato chiesto di poter non inserire nel contratto quadro le informazioni previste dall'Orientamento 6.3 (diritto del PSP di bloccare lo strumento di pagamento), in quanto di norma inserite nel contratto relativo al canale o alla carta, per evitare la duplicazione delle informazioni.</p>	<p align="center">Chiarimento</p>	<p>Al riguardo, si rammenta che le Disposizioni in materia di trasparenza delle operazioni e dei servizi bancari e finanziari – Correttezza delle relazioni tra intermediari e clienti, Sezione IV, par. 4.1.1, lett. e), prevedono che siano preventivamente rese note al cliente le misure di tutela e correttive (incluse le eventuali condizioni in base alle quali l'intermediario si riserva il diritto di bloccare uno strumento di pagamento).</p> <p>Le medesime disposizioni prevedono che, per fornire tali informazioni ai clienti, gli intermediari consegnino tra l'altro un documento di sintesi e relativi allegati, che - come noto - costituisce il frontespizio del contratto.</p> <p>Eventuali ulteriori condizioni di dettaglio possono essere inserite nel contratto relativo al canale o alla carta.</p>
	<p>È stato rilevato che la firma elettronica avanzata, richiamata tra i mezzi di</p>	<p align="center">Chiarimento</p>	<p>L'Orientamento 6 prevede che <i>“i clienti dovrebbero essere adeguatamente identificati in linea con la</i></p>

**RECEPIMENTO IN ITALIA DEGLI ORIENTAMENTI DELL'ABE IN MATERIA DI SICUREZZA DEI PAGAMENTI TRAMITE CANALE INTERNET
RESOCONTO DELLA CONSULTAZIONE**

ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/in parte/Chiarimento)	COMMENTO
	identificazione del cliente, dal Titolo II, punto 6.1, nota 10, nella normativa italiana non costituisce un documento di identità.		<i>normativa europea antiriciclaggio...</i> . Indipendentemente dagli esempi forniti nel testo degli Orientamenti, i PSP si attengono pertanto a quanto previsto in materia dalla normativa antiriciclaggio nazionale (D. lgs n. 231/2007 e relative disposizioni attuative).
Orientamento 7	È stato osservato che l'eliminazione del principio di " <i>comply or explain</i> " produrrebbe impatti significativi sui sistemi di pagamento via internet in quanto la possibilità di utilizzare "misure di autenticazione alternative" sulla base di un'analisi dei rischi sarebbe di fatto possibile per i servizi di <i>acquiring</i> e di <i>e-wallet</i> , mentre non lo sarebbe per i bonifici. Ne deriverebbe un aumento delle transazioni soggette ad autenticazione forte (anche nel caso in cui i rischi relativi fossero ritenuti accettabili), con conseguenti impatti sulla " <i>user experience</i> ", sul numero di contatti del servizio di Servizio Clienti e sul costo del servizio.	Chiarimento	La scelta di rimuovere il principio del " <i>comply or explain</i> " originariamente previsto nelle Raccomandazioni della Banca Centrale Europea è stata effettuata direttamente dall'EBA, che ha "trasposto" le citate Raccomandazioni in Orientamenti allo specifico scopo di assicurarne un'attuazione armonizzata a livello europeo. Tale scelta, condivisa dalla Banca d'Italia, è mantenuta nel recepimento nazionale degli Orientamenti. Restano chiaramente ferme le esenzioni all'adozione dell'autenticazione forte previste, ad esempio, dai paragrafi 7.1, 7.2, 7.5, 7.7.
	È stato chiesto se, qualora l' <i>acquirer</i> si avvalga di sistemi di valutazione del rischio legati ai pagamenti <i>online</i> , la richiesta di autenticazione forte possa essere selettiva rispetto ai soli ordini valutati a rischio.	Chiarimento	I casi in cui è consentito non ricorrere all'autenticazione forte sono identificati direttamente dagli Orientamenti (cfr., ad esempio, le esenzioni previste dai paragrafi 7.1, 7.2, 7.5, 7.7).
	È stato chiesto di escludere le carte aziendali e corporate (così come definite ai sensi dell'articolo 2 del Regolamento (UE) n. 2015/751) dall'ambito di applicazione dell'Orientamento 7 (autenticazione forte).	No	Gli Orientamenti non prevedono per le carte aziendali specifiche esenzioni.

**RECEPIMENTO IN ITALIA DEGLI ORIENTAMENTI DELL'ABE IN MATERIA DI SICUREZZA DEI PAGAMENTI TRAMITE CANALE INTERNET
RESOCONTO DELLA CONSULTAZIONE**

ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/in parte/Chiarimento)	COMMENTO
	È stato chiesto 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 <i>token</i> o <i>smart card</i> o di codici di accesso anche se il sito su cui verrà effettuato l'acquisto non ne consente l'utilizzo.	Chiarimento	Gli emittenti devono supportare tecnicamente l'autenticazione forte relativamente alla propria sfera di competenza non essendo possibile stabilire a priori su quali siti verranno utilizzate le carte. L'emittente deve sempre fornire almeno un elemento dinamico che può essere generato con diverse modalità, incluse quelle citate (token, smart card, ecc.).
	È stato chiesto di chiarire se, una volta che l'emittente della carta abbia predisposto lo strumento di pagamento per l'autenticazione forte, l'utilizzatore di carte di pagamento sia comunque libero di scegliere se utilizzare o meno l'autenticazione forte.	Chiarimento	Gli obblighi previsti dagli Orientamenti hanno come destinatari i prestatori di servizi di pagamento. Resta ferma l'opportunità che questi ultimi incoraggino gli utilizzatori di carte ad avvalersi dell'autenticazione forte.
	È stato chiesto se l'adozione del sistema "3D Secure" consenta di ritenere assolti gli obblighi in materia di autenticazione forte previsti dagli Orientamenti.	Chiarimento	In linea generale, gli Orientamenti non impongono l'utilizzo di specifiche tecnologie e/o standard; nel caso di specie, l'utilizzo del sistema "3D secure" non è di per sé sufficiente, se non risulta abbinato all'utilizzo di un elemento c.d. "dinamico".
	È stato chiesto se l'invio di una <i>password</i> dinamica possa essere condizionato alla presenza di elementi di rischio (es bonifici verso IBAN non presenti in " <i>white list</i> " generate in base alle consuetudini operative dei clienti), anche in conformità a quanto disposto nel punto 7.1 in merito alle eccezioni	Chiarimento	Con riferimento alla fattispecie rappresentata, è possibile adottare misure alternative di autenticazione se il beneficiario è incluso in una " <i>white list</i> ". Qualora l'IBAN destinatario non sia incluso nella " <i>white list</i> ", sarà necessaria l'adozione dell'autenticazione forte, che prevede sempre l'utilizzo di almeno un elemento dinamico.

**RECEPIMENTO IN ITALIA DEGLI ORIENTAMENTI DELL'ABE IN MATERIA DI SICUREZZA DEI PAGAMENTI TRAMITE CANALE INTERNET
RESOCONTO DELLA CONSULTAZIONE**

ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/in parte/Chiarimento)	COMMENTO
	per le quali è possibile adottare misure alternative di autenticazione.		
Orientamento 7.1	È stato chiesto di chiarire se nei casi in cui gli Orientamenti richiedono che l'emittente/acquirer/fornitore di servizi <i>wallet</i> assicuri che le carte di pagamento/servizi <i>wallet</i> siano in grado di "supportare" l'autenticazione forte tale previsione possa intendersi come necessità che la carta /soluzione <i>wallet</i> sia "tecnicamente predisposta a essere utilizzata, [con l'autenticazione forte] se richiesto".	Chiarimento	L'interpretazione proposta è corretta, nella misura in cui gli Orientamenti sono concretamente applicabili ad ogni utilizzo della carta/servizio <i>wallet</i> . Cfr., inoltre, EBA's " <i>Final Guidelines on the security of internet payments</i> ", par. 4.3 " <i>Feedback on the public consultation</i> ".
Orientamenti 7.3, 7.4, 7.5 e 7.7	È stato chiesto di esentare dalla autenticazione forte la registrazione di una carta in un <i>wallet</i> .	No	La richiesta non è in linea con il contenuto degli Orientamenti, che non prevedono la possibilità di derogare all'uso dell'autenticazione forte per la registrazione di una carta di pagamento in un <i>wallet</i> (Titolo II, par. 7.6).
Orientamento 7.6	È stato chiesto di limitare l'applicazione dell'autenticazione forte per le transazioni effettuate con carte già registrate con autenticazione forte in un <i>wallet</i> solo laddove il rischio della transazione sia elevato.	Chiarimento	L'interpretazione proposta non è in linea con il contenuto degli Orientamenti. Ai sensi del Titolo II, paragrafo 7.6, infatti, l'autenticazione forte è sempre obbligatoria al momento della registrazione nonché per le singole operazioni di pagamento effettuate tramite il <i>wallet</i> . Il ricorso a forme di autenticazione alternativa è ammesso per singole transazioni solo al ricorrere delle condizioni previste dal paragrafo 7.7 (importo o analisi del rischio).
Orientamento 7.7	È stato chiesto di confermare che ai sensi dell'Orientamento 7.6. sia possibile, in	Chiarimento	L'interpretazione proposta è corretta. L'autenticazione forte di cui al paragrafo 7.6 è sempre obbligatoria;

**RECEPIMENTO IN ITALIA DEGLI ORIENTAMENTI DELL'ABE IN MATERIA DI SICUREZZA DEI PAGAMENTI TRAMITE CANALE INTERNET
RESOCONTO DELLA CONSULTAZIONE**

ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/in parte/Chiarimento)	COMMENTO
	<p>presenza di <i>wallet</i>, circoscrivere l'autenticazione forte in occasione della prima registrazione dei dati della carta da parte del titolare e, per le operazioni di pagamento, consentire che si possano applicare meccanismi di autenticazione alternativi al ricorrere delle condizioni espresse nel punto 7.7.</p>		<p>pertanto, le eccezioni del 7.7 sono riconducibili esclusivamente alle singole transazioni (sulla base dell'importo o dell'analisi del rischio).</p>
	<p>È stato chiesto di chiarire se sia sufficiente incoraggiare il cliente ad adottare l'autenticazione forte o se vi sia un obbligo.</p> <p>Nel caso di obbligo, potrebbe essere lasciata al cliente l'opzione di attivare o disattivare il servizio di autenticazione forte.</p>	Chiarimento	<p>Cfr. sopra, Commento sub "Orientamento 7".</p>
Orientamento 8	<p>È stato chiesto di chiarire se la valutazione del rischio possa essere totalmente a carico dell'emittente.</p>	Chiarimento	<p>La valutazione del rischio è a carico dell'emittente/PSP che offre il servizio di pagamento.</p>
	<p>Si chiede di specificare eventuali criteri per poter definire un'operazione rischiosa e di chiarire se ci si possa basare su statistiche aziendali.</p>	Chiarimento	<p>Laddove gli Orientamenti prevedano che sia effettuata un'analisi dei rischi essa è rimessa agli intermediari che a tal fine potranno utilizzare anche statistiche aziendali.</p>
	<p>È stato osservato che non sussisterebbero livelli di rischio tali da imporre requisiti di sicurezza aggiuntivi rispetto alle misure tecnologiche e di processo già adottate dalle banche in tema di monitoraggio delle</p>	Chiarimento	<p>L'Orientamento non richiede necessariamente la predisposizione di "requisiti di sicurezza aggiuntivi rispetto alle misure tecnologiche e di processo già in essere"; è rimessa alla responsabilità del singolo PSP valutare se i meccanismi esistenti risultano o meno in</p>

**RECEPIMENTO IN ITALIA DEGLI ORIENTAMENTI DELL'ABE IN MATERIA DI SICUREZZA DEI PAGAMENTI TRAMITE CANALE INTERNET
RESOCONTO DELLA CONSULTAZIONE**

ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/in parte/Chiarimento)	COMMENTO
	transazioni, sotto il profilo organizzativo, economico e di processo.		linea con il presente Orientamento e, in caso contrario, apportare le opportune modifiche.
Orientamento 10	È stato chiesto di definire quali siano i requisiti da adottare, esemplificando le regole e il tipo di «azioni» che si devono intraprendere, una volta individuati fenomeni di frode. È stato altresì chiesto se possano essere adottate soluzioni secondo il principio di proporzionalità “che implica in determinate realtà l'impossibilità di essere completamente conformi al requisito”.	Chiarimento	Non è possibile identificare ex ante le azioni da intraprendersi a seguito dell'individuazione di una eventuale frode; tale identificazione è rimessa alla valutazione dei competenti organi aziendali sulla base della tipologia di frode accertata e della normativa eventualmente applicabile alla specifica violazione. L'adozione di un processo di monitoraggio per prevenire, identificare e bloccare le frodi è obbligatoria per tutti i prestatori di servizi di pagamento destinatari degli Orientamenti. Resta ferma la possibilità per gli stessi di declinare modalità e processi per il suddetto monitoraggio delle transazioni secondo proporzionalità, nel rispetto dei vincoli e delle tutele accordate alla clientela dalla normativa applicabile.
	È stato rilevato che, nell'ambito dei servizi di <i>acquiring</i> , l'obbligo di separare i processi relativi ai pagamenti da quelli inerenti alla fase di acquisto online avrebbe impatti rilevanti, in quanto “contraria” alle attuali tendenze del mercato che mirano a ridurre il più possibile i passaggi nel processo di acquisto, per migliorare l'esperienza del cliente. È stato evidenziato, pertanto, il timore che i clienti possano rifiutarsi di adottare soluzioni che segmentano i processi, rivolgendosi ad operatori che non rientrano nel perimetro di applicazione	Chiarimento	L'Orientamento è volto ad accrescere la trasparenza nei confronti dell'utenza affinché essa sia consapevole del soggetto con il quale sta interagendo (esercente o prestatore di servizi di pagamento). Resta ferma la possibilità per gli intermediari di adottare la soluzione tecnica ritenuta più opportuna al fine di raggiungere gli obiettivi sottesi all'Orientamento. Quanto al rischio di perdita di competitività del sistema bancario italiano, si rammenta - come già sopra evidenziato - che quasi tutti gli Stati membri dell'UE hanno reso noto di aver recepito/voler recepire gli Orientamenti nella disciplina nazionale (cfr. Commento sub “Altri aspetti”).

**RECEPIMENTO IN ITALIA DEGLI ORIENTAMENTI DELL'ABE IN MATERIA DI SICUREZZA DEI PAGAMENTI TRAMITE CANALE INTERNET
RESOCONTO DELLA CONSULTAZIONE**

ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/in parte/Chiarimento)	COMMENTO
	dell'Orientamento, comportando anche in questo caso una perdita di competitività del settore bancario italiano.		
Orientamento 12.5	È stato chiesto di chiarire se, ai fini del rispetto dell'Orientamento 12.5, sia sufficiente che i prestatori di servizi di <i>acquiring</i> richiedano agli operatori commerciali online di fornire una visualizzazione chiara dei processi relativi ai pagamenti distinta dai processi relativi al sito internet del negozio, in modo da rendere più agevole per i clienti identificare quando comunicano con il prestatore di servizi di pagamento e non con il beneficiario, anche senza reindirizzare il cliente ad una finestra o sito internet separato.	Chiarimento	L'interpretazione fornita è corretta.