Spett.le
Servizio Regolamentazione e Analisi Macroprudenziale
Divisione Regolamentazione II
Banca d'Italia
Via Milano, 53
00184 Roma

Oggetto: "Recepimento in Italia degli Orientamenti dell'ABE in materia di Sicurezza dei Pagamenti tramite canale Internet" – position paper in risposta alla procedura di consultazione della Banca d'Italia

Premessa

Nel documento posto in consultazione vengono illustrate le modifiche che codesta spettabile Autorità intende apportare alla disciplina applicabile alle banche, agli istituti di moneta elettronica, agli intermediari finanziari autorizzati alla prestazione di servizi di pagamento e/o all'emissione di moneta elettronica e all'attività di Bancoposta, per recepire gli "Orientamenti finali sulla sicurezza dei pagamenti via internet" (di seguito, Orientamenti) emanati dall'Autorità Bancaria Europea (ABE) il 18 dicembre u.s. e finalizzati ad accrescere il livello di sicurezza dei pagamenti in argomento.
Le modifiche proposte riguardano in particolare:

- la disciplina prudenziale applicabile alle banche (Circolare n. 285/2013) che, peraltro, nell'attuale formulazione, già incorpora le raccomandazioni della Banca Centrale Europea dalle quali gli Orientamenti derivano;
- le disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica, che risultano destinatari degli Orientamenti in quanto prestatori di servizi di pagamento, ai sensi del d.lgs. 11/2010.

A seguito della pubblicazione del citato documento di consultazione, Federcasse ha sviluppato, insieme ai principali Centri Servizi che operano a supporto delle banche di Categoria, una rapida analisi finalizzata alla valutazione degli eventuali impatti tecnici delle disposizioni in consultazione.

Le valutazioni condotte sono state prevalentemente di tipo qualitativo e finalizzate ad acquisire una stima di larga massima degli impatti sui sistemi gestiti, nonché dei tempi necessari per l'adeguamento dei medesimi.

Nel corso dei citati confronti, in particolare, sono stati approfonditi:

- le implicazioni derivanti dal venir meno del principio del "*comply or explain*" che rende, di fatto, i contenuti degli orientamenti in argomento maggiormente prescrittivi rispetto alle Raccomandazioni BCE da cui gli stessi derivano;
- gli impatti derivanti dall'adozione delle migliori pratiche (allegato 1 degli orientamenti dell'ABE) come misure obbligatorie.

Sulla base delle evidenze condivise nel corso della ricognizione condotta con i principali Centri Servizi operanti a supporto delle banche di Categoria è stato predisposto il presente documento con il quale si riportano all'attenzione di codesta Autorità alcune osservazioni, sia di ordine generale, sia inerenti ai

singoli orientamenti e/o agli impatti derivanti dalla trasformazione delle "migliori prassi" in misure obbligatorie.

Si evidenzia a riguardo che le valutazioni condotte e le osservazioni conseguenti si basano sulla declinazione di soluzioni di adeguamento in base al principio di proporzionalità, quando questo non determina pregiudizio al livello minimo di sicurezza che gli orientamenti intendono assicurare sui sistemi di pagamento via Internet.

1. Osservazioni generali

Preliminarmente, nel condividere in via generale la rilevanza strategica delle finalità perseguite dagli orientamenti ABE e la conseguente decisione di recepirli nelle disposizioni di vigilanza rilevanti, preme sottolineare come **l'eliminazione del margine di flessibilità legato al principio del "*comply or explain*"** incida sull'autonoma valutazione delle scelte tecnologiche e procedurali per la sicurezza dei pagamenti via Internet da parte delle strutture coinvolte nei processi sottostanti; inoltre (e correlatamente), determina la necessità per le stesse, di rianalizzare criticamente le attività e le progettualità realizzate, con un conseguente impatto sui tempi di adeguamento, certamente non immediati.

Con riferimento alla decisione di **imporre le migliori prassi, come misure obbligatorie** si esprimono riserve in ordine alla necessità e opportunità di un simile intervento; l'anticipata introduzione a livello nazionale di misure di sicurezza che, in termini anche più stringenti, verranno introdotte a livello europeo con l'entrata in vigore della nuova *payment service directive,* potrebbe incidere sulla competitività degli operatori nazionali.

Più nello specifico, di seguito si riportano le osservazioni formulate su alcuni specifici orientamenti e migliori prassi. Le prime sono, inoltre, corredate di una valutazione di massima dei tempi ritenuti necessari al conseguimento della conformità ai nuovi più restrittivi riferimenti disciplinati nelle disposizioni poste in consultazione.

2. Osservazioni sui singoli Orientamenti

- ***Orientamento n. 2 : Valutazione dei rischi***

Presso i Centri Servizi di Categoria sono in corso le attività di implementazione di un processo di gestione del rischio informatico sulla base dei riferimenti metodologici declinati nella "Policy di metodologia di analisi del rischio informatico", sviluppata nell'ambito del Progetto di Categoria promosso da Federcasse per l'adeguamento alle nuove disposizioni in materia ICT e adottata, previa opportuna personalizzazione, dalla generalità delle BCC-CR.

La valutazione dei rischi per i sistemi di pagamento via Internet, pur con un diverso (più alto) livello di priorità e sulla base di specifici profili di analisi, rientra nell'ambito delle attività per l'implementazione del processo di gestione del rischio informatico, in corso da parte dei citati Centri Servizi; anche sulla base di quanto riferito nel corso delle occasioni di confronto sopra richiamate, si prevede che tale processo sarà a regime entro il primo semestre del 2016.

- ***Orientamento n. 3 : Monitoraggio e segnalazione degli incidenti***

I Centri Servizi di Categoria hanno programmato l'inserimento del monitoraggio e della segnalazione degli incidenti inerenti ai sistemi di pagamento via internet nel più ampio ambito del processo di gestione degli incidenti sul sistema informativo, pur con le necessarie specificità delle modalità di gestione degli eventi e

degli incidenti connessi (in termini, ad es., di tassonomia degli eventi, strumenti di rilevazione, modalità di comunicazione, etc.).

L'implementazione del processo di gestione degli incidenti afferenti il sistema informativo, inclusa la gestione degli incidenti sui sistemi di pagamento via Internet, è in corso di finalizzazione e consolidamento nell'ambito dei Centri Servizi e, anche sulla base di quanto riferito nelle occasioni di confronto sopra richiamate, si prevede sarà a regime entro il primo semestre del 2016.

Orientamento n. 4 : Controllo e mitigazione dei rischi

I sistemi di pagamento via Internet attualmente gestiti dai diversi Centri Servizi di Categoria evidenziano un adeguato livello di sicurezza che si ritiene in linea con i requisiti disciplinati nelle disposizioni in consultazione. La piena conformità alla luce dell'eliminazione del principio del "*comply or explain*" rende comunque necessario condurre analisi di dettaglio i cui risultati, unitamente a quelli che saranno prodotti dall'analisi del rischio in precedenza richiamati, evidenzieranno probabilmente la necessità di effettuare degli interventi su tali sistemi, al momento non valutabili benché - presumibilmente - non significativi.

Tenendo, quindi, presente i tempi in cui sarà effettuata l'analisi del rischio su tali sistemi e di quelli necessari per la messa a regime dei principali processi operativi dell'IT (quali, ad esempio, il processo di *change management*), si ritiene di poter ragionevolmente conseguire la conformità dei sistemi di pagamento via internet ai requisiti di tale orientamento entro il primo semestre del 2016.

Orientamento n. 5 : Tracciabilità

I sistemi di pagamento via Internet attualmente gestiti dai Centri Servizi di Categoria esprimono un buon livello di tracciabilità delle operazioni ritenuto in linea con i requisiti contenuti nelle disposizioni. La piena conformità alle disposizioni derivante dall'eliminazione del principio del "*comply or explain*" richiede comunque un'analisi di dettaglio i cui risultati, unitamente a quelli che saranno prodotti dall'analisi del rischio, porteranno molto probabilmente alla necessità di effettuare degli interventi su tali sistemi che si prevedono comunque non significativi.

Tenendo, quindi, presente i tempi in cui sarà effettuata l'analisi del rischio su tali sistemi, si ritiene di poter raggiungere la conformità ai requisiti di tale orientamento entro il primo semestre del 2016.

Orientamento n. 6 : Identificazione iniziale dei clienti, informazioni

Mentre le procedure adottate per l'identificazione iniziale dei clienti appaiono già in linea con le disposizioni, con riguardo a quanto previsto in merito alle informazioni fornite al cliente appare necessario intervenire per includere i maggiori dettagli richiesti dall'orientamento in argomento.

Sono già in corso iniziative in tal senso da parte di alcuni dei principali Centri Servizi di Categoria (quali ad esempio la predisposizione di un manuale della sicurezza da fornire al cliente), in stretto raccordo con le BCC-CR utenti e le federazioni di riferimento.

Alla luce di quanto riportato, non si ritiene che l'adeguamento a tale orientamento produca impatti significativi e si prevede il completamento delle attività necessarie al suo adempimento entro il primo semestre del 2016.

Orientamento n. 7 : Autenticazione forte

I sistemi dei pagamenti via internet attualmente gestiti dai Centri Servizi di Categoria implementano diverse soluzioni di autorizzazione forte che appaiono, per lo più, conformi agli Orientamenti dell'ABE.

Presso diverse BCC-CR sono, tuttavia, in uso meccanismi di accesso che utilizzano come elemento dispositivo per l'autorizzazione delle transazioni la fornitura di 3 simboli (lettere/numeri) scelti a caso dal sistema su un insieme di 48 simboli contenuti su una scheda posseduta dal Cliente. Tale meccanismo di autenticazione (certamente non tra i più diffusi) era stato adottato da tali banche perché ritenuto, sulla base dell'analisi dei rischi, atto ad assicurare al cliente un adeguato livello di sicurezza per le operazioni di pagamento e - al contempo - facilità di utilizzo.

Nella definizione di "autenticazione forte del cliente" contenuta negli orientamenti dell'ABE, è precisato che: "…*almeno uno degli elementi dovrebbe essere non riutilizzabile e non replicabile (eccettuata la categoria dell'inerenza)*…". Pur a fronte di un livello di sicurezza ritenuto elevato (e comunque adeguato), l'eliminazione del principio del "*comply or explain*" determinerebbe il venir meno della concreta possibilità di definire misure di autenticazione "alternative" e la conseguente necessità di adeguamenti che comporterebbero la migrazione dei clienti interessati su altri meccanismi di autenticazione forte, provvedendo alla sostituzione dell'elemento che l'utente possiede tra quelli forniti dall'*outsourcer* di riferimento (es. Token OTP).

Si evidenzia come la necessità di migrare la clientela da una soluzione all'altra comporti impatti significativi per le BCC-CR che ad oggi adottano il suddetto meccanismo di autenticazione, con costi elevati e tempi per l'adeguamento significativi, comunque non inferiori ai 18 mesi dal momento dell'avvio delle attività di adeguamento.

Orientamento n. 10 : Monitoraggio delle operazioni

Si condivide preliminarmente la puntualizzazione che le soluzioni da adottare debbano essere commisurate alla valutazione del rischio.

Ciò posto, sulla base delle riflessioni condivise nei già citati confronti, i Centri Servizi di Categoria hanno sviluppato sistemi di monitoraggio delle operazioni che implementano un discreto livello di monitoraggio rispetto ai tentativi di frode o di intrusione nei sistemi gestiti. La piena conformità alle disposizioni richiede comunque un'analisi di dettaglio i cui risultati, unitamente a quelli che saranno prodotti dall'analisi del rischio, porteranno presumibilmente alla necessità di effettuare interventi di adeguamento di tali sistemi di monitoraggio la cui realizzazione potrà richiedere tempi lunghi, anche tenuto conto del diverso livello di "maturità" dei sistemi attualmente utilizzati dai Centri Servizi attivi nel movimento.

Alla luce di quanto richiamato, si prevede di poter raggiungere la conformità dei sistemi di pagamento via internet ai requisiti di tale orientamento entro la fine del 2016.

Orientamento n. 12 : Educazione e comunicazione riguardanti il cliente

Le attuali modalità di comunicazione verso il cliente e l'informativa fornita, anche se considerate adeguate allo scopo, non sono pienamente conformi a quanto richiesto dagli Orientamenti dell'ABE (che prevedono, tra l'altro, l'attivazione di canali di comunicazione protetti e programmi di educazione del cliente – *awareness program*). Per tale ragione, l'eliminazione del principio di "*comply or explain*", genera impatti significativi in quanto sarà necessario sviluppare soluzioni di comunicazione sicura e programmi di "awareness" per i clienti sfruttando al massimo la natura web dei servizi. Ovviamente tali soluzioni e programmi potranno essere differenziati tra le varie BCC-CR, anche in applicazione del principio di proporzionalità.

Nel complesso, si ritiene che l'adeguamento a tale orientamento produca impatti significativi per i quali si può prevedere il conseguimento della conformità entro la fine del 2016.

3. Osservazioni sulle Migliori Prassi

Migliore Prassi 2: la trasformazione della prassi in misura obbligatoria determinerebbe impatti economici, organizzativi, di sviluppo applicativo, di gestione e manutenzione delle soluzioni da fornire - rilevanti. La protezione dell'interfaccia applicativa attraverso la fornitura di dispositivi e/o browser personalizzati richiede, infatti, investimenti notevoli e riduce l'usabilità di tali servizi.

Migliore Prassi 7: l'obbligo di utilizzare un unico strumento di autenticazione forte degli utenti per tutti i servizi di pagamento via internet determinerebbe elevati impatti in termini economici, organizzativi e di usabilità da parte della clientela che non si ritengono adeguatamente controbilanciati in termini di conseguente presidio dei rischi.

Migliore Prassi 8: l'implementazione di una *strong transaction authentication* avrebbe impatti significativi in termini economici, organizzativi e di usabilità per la clientela.

Nel richiamare le considerazioni già espresse in merito all'inopportunità di anticipare per gli operatori nazionali l'applicazione di requisiti di sicurezza che saranno introdotti a livello europeo solo con l'entrata in vigore della PSD II, si evidenzia come, in particolare, il collegamento dell'autenticazione di un importo specifico e del beneficiario al momento non sia presente sui sistemi in uso e il relativo sviluppo richiederebbe il sostenimento di costi estremamente elevati.

Anche alla luce degli impatti valutati, non si condivide, quindi, la conversione della migliore prassi in argomento in una misura obbligatoria, ritenendo che l'adozione delle misure contemplate nella stessa debba essere valutata dagli operatori in funzione dell'analisi dei rischi e delle collegate valutazioni costi/benefici.

Migliore Prassi 11: la gestione dei limiti è in questo momento una funzionalità utilizzata dalle BCC-CR e non in autonomia dalla clientela. L'implementazione sui sistemi di questa funzionalità anche per i clienti comporterebbe notevoli costi di sviluppo e avrebbe impatti elevati.

Migliore Prassi 13: la personalizzazione del proprio profilo da parte del cliente attraverso parametri opportunamente definiti e agganciati ai sistemi di monitoraggio delle operazioni non è al momento disponibile e una loro implementazione comporterebbe notevoli costi di sviluppo ed impatti rilevanti anche in termini organizzativi.