Position Paper in risposta alla procedura di consultazione della Banca d'Italia sul "Recepimento in Italia degli Orientamenti dell'ABE in materia di sicurezza dei pagamenti tramite canale internet"

12 ottobre 2015

Introduzione

L'Associazione Bancaria Italiana (ABI) ha predisposto il presente documento di risposta alla consultazione pubblicata dalla Banca d'Italia in merito al "Recepimento in Italia degli Orientamenti dell'ABE in materia di sicurezza dei pagamenti tramite canale internet", raccogliendo i contributi forniti dagli Associati, nonché dalle banche del Consorzio ABI Lab, del Consorzio Bancomat e del Consorzio CBI (Corporate Banking Interbancario).

Il documento posto in consultazione illustra l'approccio che la Banca d'Italia intende seguire per recepire gli "Orientamenti in materia di sicurezza dei pagamenti via internet", adottati dall'Autorità Bancaria Europea (ABE) il 18 dicembre 2014, nell'ambito della disciplina applicabile alle banche, agli istituti di pagamento, agli istituti di moneta elettronica e all'attività di Bancoposta.

In particolare, la Banca d'Italia indica che gli Orientamenti dell'ABE sono da recepirsi integralmente nelle disposizioni di Vigilanza e, pertanto, gli intermediari interessati saranno tenuti ad adeguare i propri sistemi e procedure (tra cui quelli di governo e gestione dei rischi), per assicurare il pieno rispetto delle misure di sicurezza previste dagli Orientamenti con le modalità dagli stessi indicate, venendo meno il principio di "*comply or explain*" esistente per le pregresse Raccomandazioni emanate dalla Banca Centrale Europea.

Inoltre, la Banca d'Italia propone il recepimento integrale nelle disposizioni di Vigilanza delle Migliori Prassi (MP), indicate nell'Allegato 1 degli Orientamenti ABE e al momento non prescrittive. Tali Prassi, identificando modalità specifiche di attuazione dei principi previsti dagli Orientamenti, indirizzano il comportamento dei prestatori di servizi di pagamento (PSP) verso soluzioni in grado di assicurare il pieno raggiungimento della normativa. Per tale ragione, la Banca d'Italia ha valutato l'opportunità di considerarle come parte integrante del quadro normativo nazionale.

Nella risposta alla consultazione si riportano gli impatti collegati all'eliminazione del principio di "*comply or explain*" e alla trasformazione delle Migliori Prassi da esempi a misure obbligatorie, insieme con i tempi necessari per l'adeguamento. Nello specifico, si presentano di seguito le osservazioni principali espresse dalle banche in merito ai quesiti della consultazione e alcune considerazioni di dettaglio su Orientamenti e Migliori Prassi.

1. Osservazioni generali

In relazione agli Orientamenti pubblicati dall'ABE, **è condivisa l'importanza strategica di garantire elevati livelli di sicurezza nell'erogazione di servizi di pagamento via internet, a beneficio sia del cliente sia del PSP stesso**.

Si ritiene quindi condivisibile la decisione di Banca d'Italia di recepire gli Orientamenti ABE nelle disposizioni di Vigilanza, in quanto tale scelta consentirebbe di avere una normativa unica e organica, diminuendo in tal modo il potenziale conflitto derivante da norme distinte che insistono sugli stessi temi e fissando delle regole comuni che contribuiscono ad accrescere la fiducia nei consumatori nei pagamenti via internet e a dare sostenibilità ai canali *online*.

D'altra parte si rileva, soprattutto nella prospettiva dell'ampliamento delle esenzioni previste dalla ormai emananda nuova Direttiva sui Servizi di Pagamento (nel seguito PSD2), ad esempio relative ad operazioni di pagamento effettuate da parte di operatori telefonici, che il regime che viene ad essere introdotto con il recepimento degli Orientamenti dell'ABE non coprirebbe tali soggetti che operano in deroga, determinando – anche se su porzioni limitate del mercato dei pagamenti – un piano di gioco non livellato.

Peraltro, tale "anticipazione" non si applicherebbe alle Terze Parti (c.d.TPP), dando così luogo ad una asimmetria normativa che non tutela i clienti dei PSP che difficilmente comprendono i diversi ambiti in cui PSP e TPP operano.

In aggiunta, come già evidenziato in precedenti interlocuzioni, **l'eliminazione del principio di "*comply or explain*" determinerebbe un'ulteriore analisi delle attività già realizzate e delle progettualità in corso presso le banche, con un conseguente impatto sui tempi di adeguamento.**

Appare invece non condivisibile l'intenzione di trasformare le MP in misure obbligatorie, per molteplici ragioni.

In primo luogo, le principali rilevazioni di settore in tema di frodi e sicurezza informatica[1] hanno evidenziato che nel corso del 2014 oltre il 97% dei tentativi di attacco in danno ai servizi di *Internet Banking* accessibili dalla clientela è stato efficacemente bloccato; pertanto, pur considerando opportuna l'adozione di soluzioni evolutive previste dai requisiti obbligatori, non sembrano sussistere livelli di rischio tali da richiedere l'anticipazione di ulteriore requisiti di sicurezza rispetto alle misure tecnologiche e di processo già adottate o pianificate dalle banche per armonizzarsi alle misure obbligatorie.

[1] ABI Lab – Osservatorio Sicurezza e Frodi Informatiche, Come prevenire e contrastare le frodi su *Internet* e *Mobile Banking* – 2015 – 25 rispondenti rappresentativi dell'80% del settore in termini di dipendenti.

In secondo luogo, appare non appropriato anticipare misure di sicurezza più stringenti, che verranno introdotte con l'entrata in vigore della PSD2 e che dovranno essere recepite secondo le tempistiche previste per l'adeguamento (entro 30 mesi dalla pubblicazione). A tal proposito, si rammenta come, a seguito della procedura di consultazione avviata lo scorso 20 ottobre 2014, la stessa ABE abbia deciso di rinviare l'applicazione delle misure di sicurezza previste dalla PSD2 – in particolare in merito all'adozione di strumenti di autenticazione forte in grado di collegare dinamicamente una transazione a uno specifico importo e beneficiario – alla fase di recepimento della stessa Direttiva.

Pertanto una qualunque volontà di anticipare previsioni della PSD2 dovrebbe seguire un percorso parallelo al recepimento degli Orientamenti ABE.

A questo proposito è importante ricordare che dal 4 novembre 2014 ha preso avvio il Meccanismo di Vigilanza Unico (MVU), primo pilastro del più ampio progetto di Unione Bancaria.

All'indomani di tale data, che rappresenta uno spartiacque tra passato, presente e futuro, qualsiasi nuova normativa che impatta sul settore bancario deve tener conto di questo nuovo percorso che chiama tutti – legislatori, autorità, banche, imprese, consumatori – a ragionare in termini europei. In tale contesto anche le norme che disciplinano i servizi di pagamento e la loro sicurezza non possono sfuggire ad una logica totalmente europea, poiché anche in questo segmento il permanere di regole nazionali - ovvero l'anticipata introduzione a livello nazionale di norme che gli operatori in altri Stati Membri della UE dovrebbero applicare in un orizzonte temporale più ampio e pertanto anche più consono ai propri cicli di investimento - si porrebbe in netta contraddizione con i principi fondanti dell'Unione Bancaria e dell'integrazione del mercato finanziario dei paesi dell'Area dell'Euro.

In altre parole, le MP non solo ad oggi rappresentano degli esempi di carattere generico difficilmente traducibili in modalità e prassi operative, ma si ritiene altresì che il disallineamento normativo derivante dalla loro adozione esclusivamente nel contesto italiano possa determinare una perdita di competitività per il settore nei confronti delle controparti europee, a causa degli ingenti investimenti che i PSP insediati in Italia dovrebbero sostenere ai fini dell'adeguamento ma ancor più in termini di *customer experience* e di impatti sulla clientela.

Il venir meno della clausola "*comply or explain"* e la previsione dell'obbligatorietà dei comportamenti indicati come migliori prassi rischierebbe infatti di creare delle possibili ridondanze nei sistemi e nelle logiche di sicurezza, generando anche "appesantimenti" dal punto di vista tecnico e dell'usabilità, con relativi impatti anche in termini di tempi necessari agli adeguamenti tecnologici e ai processi verso i clienti, nonché dei costi.

In particolare tale tematica risulta particolarmente rilevante per le realtà di gruppo europeo che sfruttano sinergie internazionali sulle piattaforme tecnologiche, in quanto si troverebbero a doversi confrontare con difficoltà aggiuntive sullo sviluppo di prodotti e piattaforme da differenziare nei diversi Paesi, oltre che nello sviluppo di una strategia di *business* comune.

Un ulteriore aspetto è il rilevante impatto che l'acquisizione obbligatoria di Orientamenti e Migliori Prassi avrà nell'ambito monetica (in merito al pagamento con carte via internet), sia lato *issuing* che lato *acquiring*, che dovrà essere adeguatamente gestito e richiederà tempi rilevanti, scontrandosi inoltre con numerosi *player* internazionali che si troverebbero fortemente avvantaggiati a livello competitivo potendo offrire una *customer experience* totalmente svincolata dagli Orientamenti.

Infine, si evidenzia che la volontà di rendere obbligatorie le Migliori Prassi sembra essere non congruente con la possibilità di declinare le previsioni secondo il principio di proporzionalità.

Entrando nel dettaglio degli impatti derivanti dall'adeguamento alle previsioni della Banca d'Italia e oggetto della presente consultazione, si distinguono gli aspetti legati all'eliminazione del principio di "*comply or explain*" da quelli connessi alla trasformazione delle Migliori Prassi in misure obbligatorie.

1.1 Impatti derivanti dall'eliminazione del principio di "comply or explain"

In riferimento alla rimozione del principio di "*comply or explain*", si registrano in media per il settore impatti di portata contenuta, pur permanendo alcuni elementi di perplessità, esposti di seguito. Al momento della consultazione si rileva infatti una prevalente conformità ai requisiti previsti dagli Orientamenti, con la previsione di concludere il processo di adeguamento entro il primo quadrimestre 2016. In particolare ciò deve intendersi per l'Orientamento 7 per il quale si prevedono impatti e tempistiche più lunghe in considerazione delle progettualità più consistenti necessarie rispetto alle altre previsioni.

Rileva notare tuttavia come l'eliminazione del margine di flessibilità legato al principio di "*comply or explain*" potrebbe determinare un forte ridimensionamento dell'autonomia di valutazione da parte delle singole banche rispetto a scelte tecnologiche e di processo a garanzia della sicurezza dei pagamenti via internet, a fronte di un'attenta e continua attività di analisi del rischio.

Permangono inoltre alcuni elementi di perplessità legati all'interpretazione puntuale della norma, riportati in appendice al presente documento, che si aggiungono alle ben note difficoltà di applicazione degli orientamenti

normativi negli ambiti in cui sono coinvolti anche soggetti terzi (quali operatori commerciali).

1.2 Impatti derivanti dalla trasformazione delle Migliori Prassi in misure obbligatorie

Con riferimento alla trasformazione delle MP in misure obbligatorie e al relativo adeguamento, le banche hanno indicato impatti di entità considerevole in termini di investimenti, logiche di *business* e *customer experience*, con tempistiche di implementazione a oggi difficilmente stimabili.

Le considerazioni espresse dalle MP, non essendo concepite come prescrittive dall'ABE, risultano spesso estremamente generiche e non dettagliate a sufficienza per essere declinate in procedure e soluzioni direttamente e autonomamente implementabili da parte delle singole banche. Diviene quindi necessario chiarire i contenuti in esse riportate e l'approccio che Banca d'Italia intende seguire ai fini del recepimento. Si ribadisce che anche l'applicazione del principio di proporzionalità sembra contrastare con la volontà espressa dalla stessa Autorità di rendere obbligatoria l'adozione delle MP, non aiutando infatti a individuare il corretto perimetro di applicazione delle nuove prescrizioni.

Gli interventi richiesti ai fini dell'adeguamento alla normativa risulterebbero infatti eccessivamente onerosi in comparti nei quali la minore esposizione al rischio ha consentito sino ad oggi l'oculata adozione di soluzioni proporzionate alle reali esigenze, con una limitazione della possibilità per il settore di individuare procedure e soluzioni di sicurezza differenziate in base al proprio *business*.

Le MP costituiscono infatti degli esempi di strumenti a supporto della sicurezza, la cui efficacia non può essere valutata fine a se stessa, ma esclusivamente nell'ambito della valutazione del *framework* complessivo di sicurezza progettato dalla banca.

Infine, risulta difficilmente praticabile in tempi brevi la revisione dei progetti e delle attività di *risk assessment* già realizzati o in corso, oltre che dei relativi *budget* e piani di investimento per il prossimo anno, già confermati.

A seguito di tali considerazioni - e fatto salvo quanto sopra detto circa l'inopportunità di rendere obbligatorie le MP poiché ciò genererebbe un ingente impatto derivante dal disallineamento normativo rispetto agli altri Stati europei e porrebbe il settore italiano in una condizione di considerevole svantaggio competitivo, anticipando l'adozione di misure di sicurezza che, secondo quanto previsto dalla PSD2, avranno un orizzonte temporale di adeguamento notevolmente più ampio - si stima che i tempi necessari per l'adeguamento non possano comunque essere inferiori ai 24

mesi, a condizione che siano chiariti i contenuti rappresentati nelle MP e queste siano declinate in precisi comportamenti e prescrizioni operative.

2. Osservazioni sui singoli Orientamenti

Orientamento 3

In riferimento all'Orientamento 3, la rimozione del principio di "*comply or explain*" avrebbe un considerevole impatto sui contratti di *acquiring* stipulati con gli esercenti *online* che conservano, elaborano o trasmettono dati sensibili relativi ai pagamenti, indipendentemente dal rischio correlato o dalle dimensioni degli esercenti stessi (Orientamento 3.4).

L'inserimento di clausole contrattuali al riguardo dovrebbe pertanto essere lasciato all'autonomia decisionale dei PSP, dato che gli interventi sui testi contrattuali comportano costi operativi considerevoli, a fronte di previsioni il cui effetto pratico potrebbe essere limitato. Considerazioni analoghe possono essere estese alle attività previste dall'Orientamento 10.

Ad oggi la gestione ed il *follow-up* degli incidenti relativi alla sicurezza rientra nel più generale processo di gestione degli incidenti aziendali e nel processo di gestione dei rischi operativi. Alla luce dell'obbligatorietà delle nuove prescrizioni, si ritiene comunque utile una rivisitazione dei processi attuali per verificare che tutti i requisiti minimi siano stati recepiti e, in caso negativo, implementare le opportune azioni correttive.

Orientamento 4

Rispetto al punto 4.8, si osserva che l'inserimento in un contratto di clausole aventi il contenuto dei 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.

Orientamento 5

L'eliminazione del principio di "*compy or explain*" determinerebbe una maggiore complessità rispetto alla tracciabilità delle transazioni, in particolare in merito all'analisi periodica di file di log per la *detection* di operazioni sospette e non più solo a seguito di violazioni o di frodi.

Orientamento 6

Si sottolinea come sarebbe preferibile lasciare al PSP la facoltà di fornire le informazioni nella sede e nel 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.

Nel dettaglio, nel punto 6.2 si intravede il rischio di fornire una tale quantità di informazioni la cui rilevanza non risulti immediatamente percepibile dalla clientela.

Altro aspetto degno di nota si individua nel punto 6.3, ove le informazioni elencate sono di regola inserite nel contratto relativo al canale o alla carta, che risulta in alcuni casi essere il corretto *repository*. La duplicazione di informazioni non pare quindi uno strumento efficace e può comportare rischi di disallineamento.

Infine risulta necessario sottolineare un aspetto relativo al punto 6.1, in particolare alla nota 10: nella normativa italiana la firma elettronica avanzata[2] consente l'identificazione del firmatario del documento, ma non costituisce un documento di identità e di riconoscimento di cui agli articoli 1 e 35 del DPR n. 445 del 2000.

Orientamento 7

L'eliminazione del principio di "*comply or explain*" produrrebbe impatti significativi sui sistemi di pagamento via internet, a fronte dell'offerta di un livello di sicurezza sistematicamente più elevato.

Non essendo più valido il principio suddetto, la reale possibilità che hanno i PSP di definire misure di sicurezza coerenti con i risultati di un'analisi dei rischi è fortemente limitata e legata ai contenuti dei singoli Orientamenti. In particolare, la possibilità di utilizzare "misure di autenticazione alternative" sulla base di un'analisi dei rischi sarebbe di fatto possibile per i servizi di *acquiring* e di *e-wallet*, per i quali, negli Orientamenti 7.5 e 7.7, si richiama tale possibilità nel caso di pagamenti a basso rischio o a basso valore, mentre non lo sarebbe per i bonifici (servizio di *Internet Banking*), per i quali l'Orientamento 7.1 definisce nel dettaglio i criteri per la determinazione di operazioni a basso rischio. Pertanto, a meno delle eccezioni definite da tali criteri, si sarebbe vincolati a utilizzare sempre e indistintamente come soglie per l'utilizzo di sistemi di *strong authentication* quelle definite dalla PSD per i pagamenti a basso valore (30 euro o 60 euro se il PSP del beneficiario fosse insediato in Italia), anche nel caso emergesse che i rischi associati all'utilizzo di soglie più alte siano accettabili. In particolare, l'utilizzo di tali soglie (previste dalla Direttiva) invece delle soglie attuali (calcolate sulla base di un'analisi dei rischi) determinerebbe un aumento del numero di interazioni dei clienti con il sistema di *strong*

[2] L'art. 1, comma 1, lett. q)-bis del D.Lgs. n. 82/2005 (CAD) definisce la firma elettronica avanzata (FEA) come "*L'insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati*".

authentication, con conseguenti impatti sulla *user experience*, sul numero di contatti del servizio di *Contact Center* e sul costo dello stesso per livelli di servizio costanti. Gli impatti sopra riportati potrebbero non essere compensati dalla minore esposizione legata all'utilizzo di soglie più basse, come quelle definite nella PSD per i pagamenti a basso valore. In particolare, in riferimento all'Orientamento 7.5, se l'intenzione è di richiedere la *strong authentication* sulla maggioranza delle transazioni, si prevedono rilevanti impatti sui servizi di *acquiring*, in quanto gli esercenti *online* saranno orientati a scegliere PSP che consentono maggiore flessibilità sulla gestione del protocollo *3D Secure*.

La clausola *comply or explain* ha permesso ad alcuni di identificare/valutare come *sensitive payment data* quei dati che, nel rispetto delle proprie valutazioni dei rischi/contromisure di sicurezza in essere, si sono ritenuti sensibili.

L'Orientamento, venendo meno il principio di "*comply or explain*", potrebbe vincolare alcune realtà a proteggere ulteriori dati tramite *strong customer authentication*.

Orientamento 10

Si riconosce che in prospettiva tale misura potrebbe risultare determinante per fronteggiare eventuali nuove modalità di frode e la prescrizione normativa potrebbe risultare utile per il superamento delle attuali resistenze aziendali, pur basate su legittime valutazioni economiche.

Tuttavia, in linea con quanto già espresso per i precedenti Orientamenti, non sembrano sussistere livelli di rischio tali da imporre requisiti di sicurezza aggiuntivi rispetto alle misure tecnologiche e di processo già adottate dalle banche in tema di *transaction monitoring*, sotto il profilo organizzativo, economico e di processo.

Viene chiesta la possibilità di definire quali sono i requisiti da adottare, esemplificando maggiormente le regole e il tipo di «azioni» che si devono intraprendere una volta individuati fenomeni di frode.

Inoltre, si ritiene opportuno valutare la possibilità di accettare soluzioni secondo il principio di proporzionalità che implica in determinate realtà l'impossibilità di essere completamente conformi al requisito.

Orientamento 11

In riferimento all'Orientamento 11, la rimozione del principio di "*comply or explain*" avrebbe un impatto in termini di revisione delle condizioni contrattuali (sezione "Doveri dell'Esercente") allo scopo di richiedere agli operatori commerciali *online* che conservano, elaborano o trasmettono i dati sensibili relativi ai pagamenti, di attuare adeguate misure di sicurezza per la protezione di tali dati, prevedendo inoltre la possibilità, da parte della

banca, di svolgere controlli periodici per verificare il rispetto di tali obblighi contrattuali.

Orientamento 12

Si prevedono rilevanti impatti sui servizi di *acquiring* nel rendere obbligatoria la separazione dei processi relativi ai pagamenti da quelli inerenti la fase di acquisto *online*: il mercato porta infatti gli esercenti a cercare di ridurre il più possibile i passaggi nel processo di acquisto, contribuendo a richiedere ai PSP specifiche soluzioni che integrino il processo di pagamento all'interno del sito *web* dell'esercente.

Le soluzioni di successo dei cosiddetti *over the top* hanno come caratteristica saliente la sempre maggiore integrazione tra i diversi processi per fornire una "esperienza senza soluzione di continuità" da parte dell'utente.

Il timore diffuso è che i clienti potrebbero rifiutarsi di adottare soluzioni che segmentano i processi e quindi a rivolgersi ad operatori che non rientrano nel perimetro di applicazione dell'Orientamento, comportando anche in questo caso una perdita di competitività del settore bancario italiano.

Inoltre, si rimarca che l'affidabilità e l'efficacia di specifici canali di comunicazione con la clientela (ad esempio e-mail) non sono da valutarsi in senso assoluto ma devono essere rapportate all'insieme delle procedure e delle soluzioni che compongono il *framework* complessivo di gestione della sicurezza dei pagamenti via internet.

3. Osservazioni sulle singole Migliori Prassi

Migliore Prassi 2

Gli impatti derivanti dall'introduzione come obbligatoria della MP2 risulterebbero essere rilevanti, in particolar modo in termini economici, organizzativi nonché di sviluppo, gestione e manutenzione delle soluzioni da fornire ai clienti. Tale approccio porterebbe inoltre la banca a uscire dal proprio ambito di competenza, sconfinando in qualche misura in un terreno di pertinenza tipica della clientela, che adotta e sceglie in autonomia i dispositivi dai quali svolgere le operazioni di *Internet Banking* secondo le proprie esigenze e necessità.

In aggiunta, un ulteriore rilevante impatto è relativo alla limitata flessibilità dei servizi di pagamento che le soluzioni e gli strumenti messi a disposizione dalle banche determinerebbero in relazione alla *user experience* dei clienti. In dettaglio, si stimano impatti considerevoli sia in relazione al singolo PSP (a titolo esemplificativo, si verrebbe a creare la situazione per cui si potrà usufruire di determinati servizi esclusivamente da specifici *device* e/o *browser*, contrapponendosi alle esigenze della clientela di fruire in mobilità

dei servizi bancari), sia in relazione all'intero settore (i c.d. clienti multi-bancarizzati si troverebbero a dover utilizzare necessariamente dispositivi e/o *browser* diversi per usufruire di servizi offerti da banche differenti, causando notevoli disagi operativi o errori dovuti a scarsa conoscenza dei molteplici strumenti offerti).

E' opportuno sottolineare che sarebbe necessaria una definizione più dettagliata degli strumenti di sicurezza volti a proteggere l'interfaccia applicativa resa disponibile all'utente, che ad oggi non appare sufficientemente esplicativa.

Rileva infine evidenziare come tutt'ora il settore bancario svolga adeguate attività di protezione delle interfacce applicative messe a disposizione del cliente attraverso diverse modalità, tra cui l'analisi del traffico applicativo o la verifica di integrità delle pagine *web* applicative: in dettaglio, tali attività vengono svolte mediante l'utilizzo di *software* e sistemi che non impattano in nessun modo sull'operatività dell'utente, non necessitando di essere installati sui dispositivi utente ma operando direttamente sui sistemi informativi della banca.

Migliore Prassi 3

Si evidenzia in primo luogo come la traduzione in italiano della MP3, fornita dalla stessa ABE, non corrisponda con quanto riportato nella versione originale delle Linee Guida. A tal proposito, si evidenzia che tale previsione appare in contrasto con quelle elencate al punto 3 dell'Orientamento 11.

A valle di tale premessa, se si considera il documento tradotto, si segnalano impatti modesti per le banche che comporterebbero adeguamenti che investirebbero soprattutto gli operatori commerciali: saranno tali soggetti che dovranno, infatti, adeguare i sistemi e i contratti con i PSP alla nuova previsione.

Per comodità si propone la traduzione corrispondente alla versione originale delle Linee Guida: "I PSP che offrono servizi di *acquiring* potrebbero richiedere contrattualmente ai *merchant online* che conservano informazioni di pagamento di disporre di adeguati processi a supporto della tracciabilità."

Migliore Prassi 4

Gli impatti maggiormente rilevanti che derivano dall'introduzione di tale MP sono riconducibili in particolar modo ai PSP la cui logica di *business* prevede una forte componente legata all'operatività online da parte dei clienti, in quanto comporterebbe un adeguamento oneroso dei contratti con la clientela, dovendo definire un contratto di servizio dedicato per lo svolgimento di operazioni di pagamento via internet invece di mantenere le attuali condizioni contrattuali incluse in un contratto di servizio generale più ampio con il prestatore di servizi di pagamento.

Migliore Prassi 6

La MP6 impatterebbe fortemente sui clienti, sulle banche e indirettamente sui circuiti, implicando accordi strategici, tecnici ed economici fra i vari attori coinvolti.

Migliore Prassi 7

Rendere obbligatorio l'utilizzo di un unico strumento di autenticazione forte degli utenti per tutti i servizi di pagamento via internet determinerebbe notevoli impatti in termini economici, organizzativi e di *user experience*. Tali impatti potrebbero non essere compensati dai minori costi legati all'implementazione di uno strumento unico di autenticazione.

Inoltre le esigenze dei clienti sono differenti, sia su base individuale sia per segmento di clientela; risulterebbe quindi opportuno proseguire con l'erogazione dei servizi bancari soddisfacendo da un lato gli elevati standard di sicurezza tutt'ora offerti e dall'altro soddisfare le necessità espresse da specifiche categorie di utenti (es. *retail* o *corporate*) in relazione allo strumento di autenticazione da adottare.

Si evidenzia infine come quanto appena riportato risulterebbe maggiormente accentuato se all'interno del perimetro di applicazione dell'MP7 venisse ricompreso anche il mondo carte.

Migliore Prassi 8

Come anticipato nella prima parte del presente documento, si evidenzia in primo luogo come l'introduzione di tale previsione di fatto anticiperebbe, senza adeguata giustificazione, di circa 30 mesi l'adeguamento ai requisiti di sicurezza stringenti previsti dalla PSD2 in via di pubblicazione. Tale anticipazione contrasterebbe inoltre con la decisione presa dalla stessa ABE - a seguito di consultazione pubblica dello scorso novembre 2014 - in relazione alle tempistiche di introduzione di tali misure stringenti.

Anticipare tali tempistiche esclusivamente a livello nazionale avrebbe altresì delle ripercussioni molto importanti sulle complessità implementative, sull'usabilità utente e sui costi di acquisizione e manutenzione.

Analizzando in dettaglio le ricadute delle intenzioni di Banca d'Italia si rileva in particolare che:

- le banche vedrebbero vanificare investimenti rilevanti fatti negli anni precedenti per l'adozione della *strong authentication* (*token* o similari), che ora dovrebbero essere dismessi in un breve arco temporale, mentre la validità e l'ammortamento di questi dispositivi sono generalmente quinquennali;
- se l'autenticazione forte dei pagamenti venisse effettuata unicamente con strumenti *hardware*, questi oggetti avrebbero un costo unitario

molto elevato, in special modo se fossero dotati di meccanismi in grado di rilevare automaticamente i dati della transazione;

- il requisito prevede che "*La soluzione tecnologica che consente il collegamento tra i dati di autenticazione forte ed i dati delle operazioni, dovrebbe essere a prova di manipolazioni*". Si ritiene necessario un chiarimento puntuale di tale richiesta;

  un'altra situazione rilevante che non trova attuale pieno riscontro nella normativa è relativa alla gestione delle distinte che raggruppano più disposizioni e nel perimetro di prodotti/servizi *online* offerti alla clientela *corporate*. L'autenticazione forte di distinte massive che comprendono più bonifici (ad esempio nel caso di pagamenti di stipendi) non presenta caratteristiche tali da poter essere conforme alla specifica normativa richiesta, non prevedendo a oggi la firma di singole disposizioni per singolo importo e singolo beneficiario; gli obblighi previsti sulla *strong transaction authentication* sarebbero inoltre di più complessa applicazione nell'ambito dei pagamenti con carte via internet.

Occorre infine anche considerare come un'eccessiva rigidità operativa potrebbe "disaffezionare" la clientela dei canali virtuali italiani, favorendo la concorrenza da parte di banche estere non sottoposte allo stesso vincolo.

Considerando quindi l'orientamento emerso a livello europeo, oltre che i considerevoli impatti che comporterebbe l'implementazione immediata di una soluzione di *strong transaction authentication* (in termini economici, organizzativi e di *user experience*), si ritiene che l'adozione di tale soluzione non debba essere resa obbligatoria ma debba essere valutata dai singoli PSP sulla base di un'analisi dei rischi, dei costi e dei benefici, con la possibilità eventualmente di includere tale modalità tra le raccomandazioni cui adempiere obbligatoriamente a valle del recepimento della nuova PSD.

Migliore Prassi 9

Si evidenzia come l'adeguata formazione del personale degli operatori commerciali *online* impiegati nella gestione delle frodi difficilmente potrebbe essere formalizzata come obbligo per il *merchant* stesso, ad esempio riportandola come un requisito contrattuale.

Inoltre si fa presente come un adeguato livello di sicurezza per l'attività di tale categoria di operatori commerciali sia garantito dai requisiti previsti dagli Orientamenti 3.4, 4.8 e 11.3.

Migliore Prassi 11

Gli impatti derivanti dalla possibilità di gestione, da parte dei clienti e in autonomia rispetto alla banca, dei limiti di operatività collegati ai servizi di *Internet Banking* sarebbero particolarmente onerosi in termini di processo, in particolare per le banche *online*, con ripercussioni soprattutto a livello di sviluppo applicativo e di coinvolgimento delle strutture della banca a diretto

contatto con la clientela (ad es. *Contact Center*, relativamente alle prevedibili numerose richieste di contatto per avere informazioni circa l'utilizzo degli strumenti o per modificare i suddetti limiti).

Si ritiene che quanto descrtitto nella MP debba essere valutato autonomamente dal singolo PSP, potendo rappresentare un elemento di concorrenzialità.

Migliore Prassi 13

Per consentire ai clienti di definire "*white list*" o "*black list*" di Paesi e specifici beneficiari occorrerebbe avviare progettualità consistenti ed effettuare adeguamenti che, anche se non considerati elevati, hanno un impatto abbastanza rilevante; al contempo, lo sviluppo di tali investimenti non determinerebbe necessariamente un maggior livello di sicurezza dei servizi offerti. Inoltre, analogamente a quanto riportato in relazione alla MP11, l'introduzione di tale previsione potrebbe determinare rilevanti impatti anche verso strutture delegate al contatto diretto con la clientela.

E' opportuno sottolineare che l'adozione di tale MP, così come la MP11, potrebbe non tradursi sempre e necessariamente in un rafforzamento della sicurezza dei pagamenti via internet: si teme infatti che in taluni casi l'adozione di tale MP potrebbe portare ad una maggiore esposizione verso il frodatore. In particolare la messa a disposizione dell'utente di un ambiente con piena autonomia di gestione di limiti e regole generali e personalizzate, potrebbe esporre maggiormente l'utente verso i frodatori: a fronte di attacco mirato, il frodatore avrebbe a disposizione un ambiente personalizzato per agire indisturbato, oltre che poter addirittura escludere l'utente dalla sua operatività (anche immediata, si pensi ad esempio all'annullo di un bonifico fraudolento). Per quanto esposto, oltre che per poter conciliare le esigenze di *customer satisfaction* con i vincoli che derivano dalle procedure anche interbancarie, sarebbe preferibile lasciare la possibilità di valutazione/modulazione al PSP.

4. Ulteriori considerazioni

Si coglie inoltre l'occasione della presente consultazione per riportare alcuni punti degli Orientamenti in merito ai quali sarebbe auspicabile un chiarimento da parte dell'Autorità, ad esempio nella forma di FAQ, al fine di garantire una piena aderenza alle previsioni richieste:

- Un applicativo *client-server* (non *web-based*) riservato alla clientela corporate, che però utilizza il canale internet, può risultare escluso dagli Orientamenti?
- È possibile avere un'esemplificazione dei dati di pagamento sensibili?
- È possibile avere un'esemplificazione delle "operazioni di pagamento effettuate da un'impresa tramite reti dedicate"?

- L'invio di una *password* dinamica può essere condizionato alla presenza di elementi di rischio (es bonifici verso IBAN non presenti in *white list* generate in base alle consuetudini operative dei clienti), anche in conformità a quanto disposto nel punto 7.1 delle Linee Guida dell'ABE in materia di sicurezza via internet, relativamente alle eccezioni per le quali è possibile adottare misure alternative di autenticazione?
- Si chiede di confermare che ai sensi dell'Orientamento 7.6. sia possibile, in presenza di *wallet*, 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 nelle condizioni espresse nel punto 7.7.
- Qualora l'*acquirer* si avvalga di sistemi di valutazione del rischio legati ai pagamenti *online*, la richiesta di *strong authentication* potrebbe essere selettiva rispetto ai soli ordini valutati a rischio?

Infine si chiede di esplicitare il rapporto tra gli Orientamenti ABE e precisazioni emanate dalla BCE nell'*Assessment Guide* del febbraio 2014, in quanto più dettagliate rispetto alle Raccomandazioni poi confluite negli Orientamenti dell'ABE.