BANCA D'ITALIA
EUROSISTEMA

La PSD2 e le nuove regole sulla sicurezza

Gino Giambelluca
Servizio Supervisione sui mercati e sul sistema dei pagamenti

Roma, 10 dicembre 2018

BANCA D'ITALIA
EUROSISTEMA

AGENDA

1 L’approccio del regolatore: innovazione vs. sicurezza

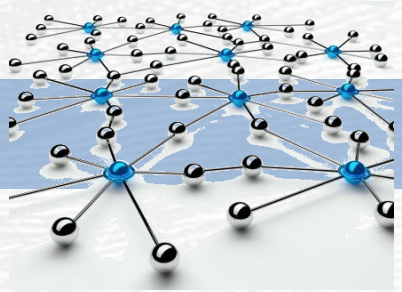
2 PSD2 e normativa attuativa della European Banking Authority (EBA)

AGENDA

1 L’approccio del regolatore: innovazione vs. sicurezza

2 PSD2 e normativa attuativa della European Banking Authority (EBA)

L'approccio del regolatore: innovazione vs. sicurezza



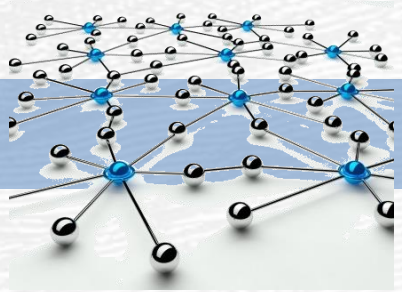
I driver del cambiamento nell'economia digitale:
L'evoluzione tecnologica e dei modelli di business

- **Ampliamento del mercato** (prodotti, canali, operatori) ➔ web platforms, mobile payments, wallet providers, virtual currencies, third party providers, instant payments,…
- **Efficienza** ➔ no vincoli di disponibilità, h24/365, né di localizzazione

+ **rischi** (complessità, decentramento, frammentazione della catena del valore , esigenze più evolute degli utenti)

Necessità di promuovere e salvaguardare la **fiducia** nelle nuove soluzioni

L'approccio del regolatore: innovazione vs. sicurezza



Adeguamento delle modalità di intervento

- **Regolamentazione** e **controllo**, che nel nuovo contesto di mercato devono essere resi più **tempestivi** e **adeguati** alle innovazioni, quindi…

  a) contatto più intenso e diretto con il **mercato**, azione di dialogo/promozione delle iniziative → valutazione – feedback (es. canale fintech)

  b) ampliamento del **perimetro di osservazione** oltre i providers tradizionali (es. fintech, fornitori di servizi e tecnologie, …)

Due livelli di intervento del regolatore in tema di sicurezza

- Dimensione sistemica (*macro*) → **presidi per rischi cyber**
- Offerta dei servizi (*micro*) → regole stringenti per **autenticazione pagamenti** e **comunicazione sicura tra PSP** (open banking) → ***PSD2***

AGENDA

1 L’approccio del regolatore: innovazione vs. sicurezza

2 PSD2 e normativa attuativa della European Banking Authority (EBA)

PSD2 e normativa attuativa della European Banking Authority (EBA)

- **La nuova Payment Service Directive - PSD2: DIR (EU) 2015/2366** del 25 novembre 2015, entrata in vigore il 13 gennaio 2016

- **Regolamento sulle carte di pagamento** (IFR): Regulation (EU) 2015/751 del 29 aprile 2015

Lo stato dei lavori: PSD2 e sua implementazione nazionale

Il recepimento della PSD2 in Italia è avvenuto con il d. lgs. 218/2017, in vigore da gennaio 2018,

EBA EUROPEAN BANKING AUTHORITY

E’ in via di completamento il set delle normative attuative (RTS e Guidelines) previste dalla PSD2

PSD2 e normativa attuativa della European Banking Authority (EBA)

PSD2 e Regolamento Carte (IFR): obiettivi comuni

- raggiungere un maggiore livello di armonizzazione nel mercato europeo dei pagamenti retail (evitando arbitraggi)
- tenere conto del rapido sviluppo tecnologico che caratterizza il mercato dei nuovi prodotti di pagamento retail
- accrescere la concorrenza tra operatori e tra prodotti/canali

La PSD2: le principali novità

- **Ambito di applicazione**: precisazione delle esclusioni già previste dalla PSD (operatori TLC, ticketing, charities, piattaforme web, circuiti limitati); estensione dell'ambito di applicazione positivo della direttiva)

- **Rapporti tra autorità di vigilanza (home e host)**: nuovo modello di coordinamento; central contact point; misure precauzionali.

- **Servizi di payment initiation e di account information (cd.** *servizi di accesso ai conti/ open banking***)** : diritto di offrire tali servizi; procedure di autorizzazione e registrazione; ripartizione di responsabilità;

- **Requisiti di sicurezza per pagamenti elettronici** : strong customer authentication; standard di comunicazione sicura tra PSP

Titolo 1

Titolo 2

Titoli 2-4

Titolo 4

L'approccio del regolatore: innovazione vs. sicurezza

***Open banking**: impulso all'innovazione e alla concorrenza*

Impatto sulla concorrenza e sull'attività bancaria tradizionale

Impatto sulla sicurezza, la responsabilità e la protezione dei dati

LICENSED THIRD PARTY PROVIDERS

L'approccio del regolatore: innovazione vs. sicurezza

Approccio olistico alla sicurezza = ***4 aree di intervento nella PSD2***

1 - **UTENTI**: autenticazione forte del cliente per l'avvio di una transazione di pagamento
2 - **PAYMENT SERVICES PROVIDERS (PSPs)**: requisiti per la gestione interna dei rischi di sicurezza
3 - **INTERBANCARIO**: comunicazione sicura tra PSPs (API)
4 - **SISTEMICO**: segnalazione degli incidenti alle autorità competenti e condivisione delle informazioni

Sicurezza e regole EBA

I mandati PSD2 all'EBA in tema di sicurezza/frodi

Mandato PSD 2	Oggetto	Stato
Art. 98	**RTS on strong customer authentication and secure communication**	Commission Delegated Regulation (EU) 2018/389, pubblicata a marzo 2018, data di applicazione 14/9/2019
Art. 96	**Guidelines on fraud data reporting**	pubblicate a luglio 2018
Art. 96	**Guidelines on major incident reporting**	pubblicate a luglio 2017
Art. 95	**Guidelines on operational and security risk management**	pubblicate a dicembre 2017

Guidelines su reporting delle frodi (art. 96 PSD2)

In vigore in Italia nel corso del 2019

Contenuti:

Criteri armonizzati (definizioni, tempistiche e schemi segnaletici) per l'invio da parte dei PSP dei dati statistici semestrali sulle frodi all'autorità competente

Obiettivi:

- *Monitoraggio sistemico da parte delle autorità competenti, utile per orientare policy e modifiche regolamentari*
- *Utile anche ai PSP per comparare i propri tassi di frode con le medie di sistema e per adottare interventi correttivi*

Lo stato dei lavori: PSD2 e regole EBA

RTS su autenticazione forte e comunicazione sicura (art. 98 PSD2)

Contenuti:

- Obbligo di **autenticazione forte** (a due fattori con elementi dinamici) del cliente e della transazione; definizione delle esenzioni
- misure di sicurezza adeguate per tutelare la **riservatezza** e **l'integrità delle credenziali di sicurezza** personalizzate degli utenti
- requisiti per la **comunicazione sicura** tra banche, terze parti e utenti

RTS su autenticazione forte e comunicazione sicura (art. 98 PSD2)

La Strong Customer Authentication (SCA)

- 2 elementi scelti fra 3 tipi: Conoscenza, Possesso, Inerenza
- tutti i pagamenti elettronici devono usare procedure di autenticazione forte a due fattori (carte su POS/ATM/e-commerce, Mobile, Internet)
- SCA genera un codice dinamico (monouso) detto Authentication Code
- dynamic Linking: solo per pagamenti remoti si aggiunge un link a importo/beneficiario (codice dinamico associato indissolubilmente al pagamento)

RTS su autenticazione forte e comunicazione sicura

Esenzioni dall'applicazione della SCA

- pagamenti verso 'trusted beneficiaries' (white lists)
- pagamenti presso 'unattended terminals' per il trasporto e il parcheggio
- pagamenti in remoto di basso importo (*fino a EUR 30; su base cumulativa EUR 100 o più di 5 transazioni consecutive, dall'ultima applicazione della SCA*)
- pagamenti contactless (*fino a EUR 50; su base cumulativa EUR 150 o più di 5 transazioni consecutive, dall'ultima applicazione della SCA*)
- pagamenti classificati a basso rischio in base a transaction risk analysis
- corporate payments

RTS su autenticazione forte e comunicazione sicura (art. 98 PSD2)

Standard aperti per la comunicazione sicura

- per il colloquio con altri operatori, l'ASPSP mette a disposizione un'interfaccia che può essere o dedicata o l'interfaccia utente (opportunamente modificata)

- se dedicata, l'ASPSP deve garantire lo stesso livello di disponibilità e di performance dell'interfaccia utente e adottare le stesse misure di contingency in caso di indisponibilità

Guidelines su reporting delle frodi (art. 96 PSD2)

In vigore in Italia da 1° luglio 2019

Contenuti:

Criteri armonizzati (definizioni, tempistiche e schemi segnaletici) per l'invio da parte dei PSP dei dati statistici semestrali sulle frodi all'autorità competente

Obiettivi:

- *Monitoraggio sistemico da parte delle autorità competenti, utile per orientare policy e modifiche regolamentari*
- *Utile anche ai PSP per comparare i propri tassi di frode con le medie di sistema e per adottare interventi correttivi*

Guidelines su management of operational and security risks (art. 95 PSD2)

Contenuti:

Requisiti per la gestione dei rischi operativi e di sicurezza nella prestazione dei servizi di pagamento (8 aree: governance, valutazione rischi, protection, detection, business continuity, testing, awareness/learning , relationship with users)

Punti di attenzione:

- *principi di alto livello*
- *proporzionalità*
- *focus su cyber risk*

Applicabili a tutti i prestatori di servizi di pagamento (Banche, IP, IMEL, Poste)

Lo stato dei lavori: PSD2 e regole EBA

Guidelines su major incident reporting (art. 96 PSD2)

Recepimento nelle disposizioni di vigilanza entro 1°sem. 2018

Contenuti:

Criteri, threshold e metodologia per valutare la rilevanza degli incidenti e le informazioni da condividere con altre autorità nazionali, prevedendo un ad hoc template per la notifica

- lower/higher impact
- dimensioni su cui valutare l'impact (# pag.ti, perdita, …)

Punti di attenzione:

- *Coordinamento con altri obblighi di reporting (es. Direttiva NIS, SSM, GDPR)*

L'approccio del regolatore: innovazione vs. sicurezza

Pagamenti non cash - trends: Italia vs EU

Source: ECB statistics

Var. su base annua (volumi)	*2009-2012*	*2012-2017*
Italia	**+ 3.0%**	**+ 7.0%**
Euro Area	**+ 3.9%**	**+ 3.3%**

*Nel 2017 effettuati in Italia **100** pagamenti pro-capite non cash vs **231** in Europa*

Grazie per l'attenzione !

Gino GIAMBELLUCA
Banca d'Italia
Dipartimento Mercati e sistemi di pagamento
Servizio Supervisione mercati e sistema dei pagamenti