CONSILIA

Business Management

La responsabilità delle Banche nella sicurezza dei pagamenti

Milano, 25 novembre 2025

Agenda

- **Innovazione, sostenibilità e stabilità del sistema finanziario**
- **Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento**

Agenda

- **Innovazione, sostenibilità e stabilità del sistema finanziario**
- **Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento**

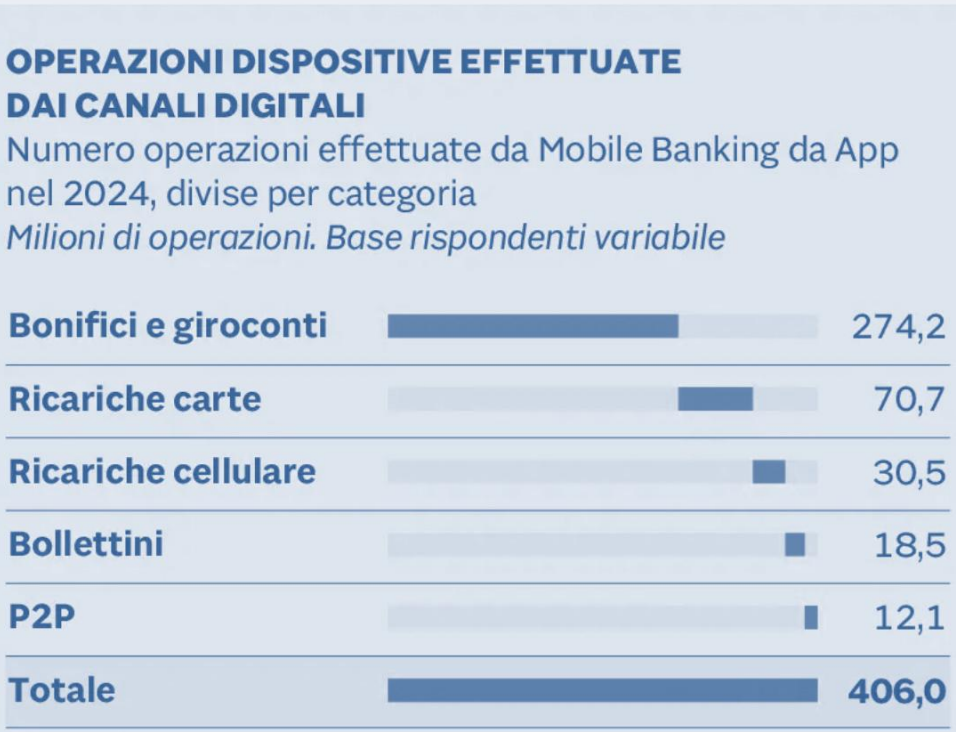
Innovazione, sostenibilità e stabilità del sistema finanziario

I trendi di mercato

OPERAZIONI DISPOSITIVE EFFETTUATE DAI CANALI DIGITALI

Numero operazioni effettuate da Mobile Banking da App nel 2024, divise per categoria

Milioni di operazioni. Base rispondenti variabile



L'avvento della tecnologia, i diversi stili di vita e le abitudini di consumo stanno contribuendo a ridisegnare fortemente i modelli di servizio, i processi interni e i presidi di sicurezza, dell'ecosistema di mercato.

Crescono le operazioni dispositive da App Mobile, che oggi sono 2,3 volte quelle da sito Web. Le banche stanno intercettando questa evoluzione, con il 61% che indica come priorità nello sviluppo dei canali digitali l'arricchimento delle funzionalità di pagamento. Quest'attenzione si riflette sull'offerta al cliente: il 77% di esse propone pagamenti con fotocamera, il 55% servizi P2P e il 36% funzionalità Nfc.

Anche i prodotti si stanno trasformando: i bonifici istantanei in digitale crescono in doppia cifra (+50,6% da app e +26,5% da sito) e rappresentano già il 10% dei bonifici totali, con una prospettiva attesa di crescita ulteriore.

Innovazione, sostenibilità e stabilità del sistema finanziario

I trendi di mercato

Numero operazioni effettuate da Sito Web da App nel 2024, divise per categoria
Milioni di operazioni. Base rispondenti variabile

Bonifici e giroconti	157,6
Ricariche carte	6,4
Ricariche cellulare	2,6
Bollette	9,8
Totale	**176,4**

I Paesi dell'area euro sono giunti il 9 ottobre scorso al traguardo fissato dal legislatore europeo per l'attuazione di tutte le misure fissate dal regolamento europeo sui bonifici istantanei.

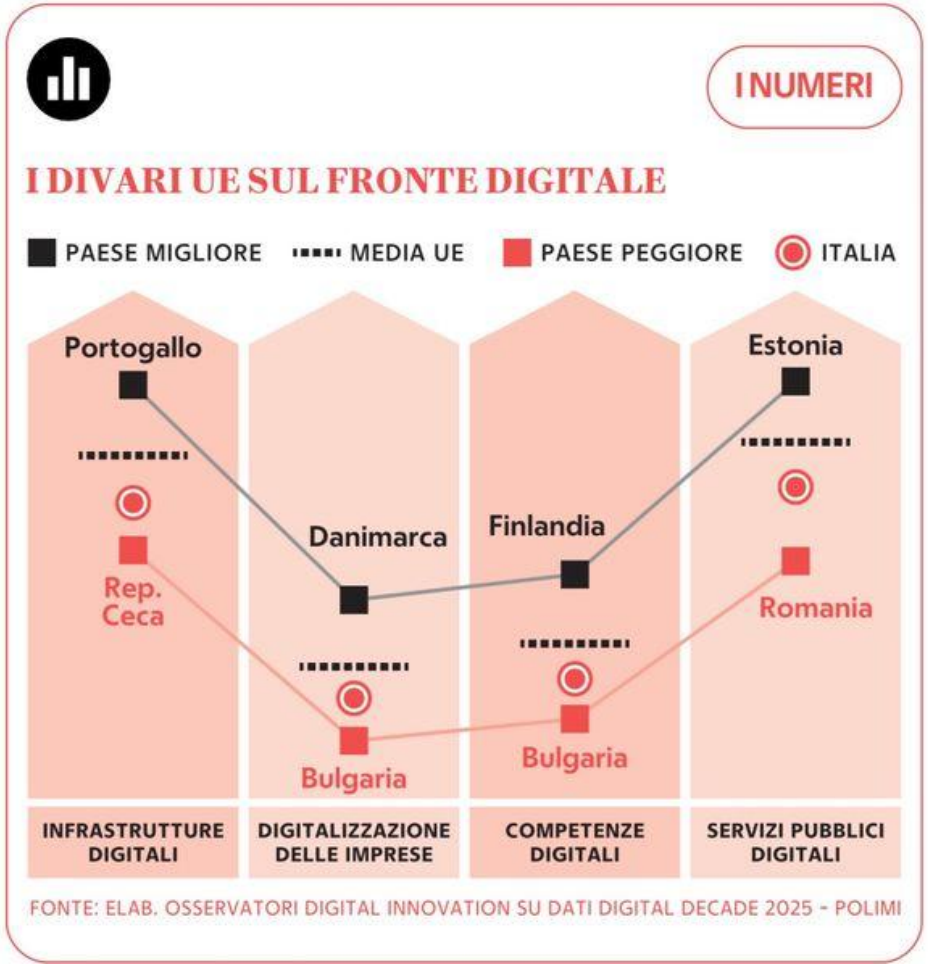
Nel 2027 le stesse previsioni saranno adottate anche dai Paesi Ue non euro. Il percorso già messo alle spalle ha visto due tappe importanti

- quella del 9 gennaio 2025, in cui le banche dell'area euro hanno reso raggiungibili tutti i conti della propria clientela per la gestione dei bonifici istantanei in ingresso e con un costo analogo ai bonifici ordinari;
- la seconda tappa il 9 ottobre scorso, ha portato le banche dell'area euro a offrire i bonifici istantanei in uscita a tutti i clienti e tramite gli stessi canali già in uso.

Altra importante novità ha riguardato l'introduzione del servizio di verifica di congruenza tra Iban e dati anagrafici del beneficiario che i prestatori di servizi di pagamento svolgono su tutte le operazioni di bonifico (istantaneo e non), a presidio della sicurezza delle transazioni.

Innovazione, sostenibilità e stabilità del sistema finanziario

I trendi di mercato



L'Europa presenta ancora divari nazionali significativi, nonostante un leggero miglioramento complessivo nella corsa alla digitalizzazione. L'Italia si posiziona nella fascia medio-bassa con un miglioramento di tre punti percentuali rispetto allo scorso anno, ma dietro i tradizionali competitor: con 52 punti su 100 si trova più vicina al fondo della classifica che alla media europea (60), staccati dai 59 della Francia e i 58 della Germania.

Guardando ai Paesi leader per ogni pilastro digitale, il Portogallo alla voce delle infrastrutture (punteggio di 96%), per le competenze la Finlandia (56%), per le imprese la Danimarca (52%) e per i servizi pubblici l'Estonia (97%).
In ogni pilastro di digitalizzazione l'Italia risulta sotto la media europea.

Innovazione, sostenibilità e stabilità del sistema finanziario

I trend di mercato

Il mercato dei pagamenti è da tempo scenario di sempre nuovi cambiamenti che si susseguono e modificano, di volta in volta, la morfologia del comparto

Innovazione, sostenibilità e stabilità del sistema finanziario

Le principali sfide

I trend in corso pongono sfide complesse

Contrastare le minacce emergenti

- Schemi di frodi più sofisticati
- Cyber criminalità
- Scala globale delle attività illecite

Sostenere la competitività nel mercato

- Visione organica della normativa dei vari settori
- Level playing field

Dare risposta alle esigenze degli utenti (persone e imprese)

- Customer experience semplice
- Pagamenti immediati
- Inclusione finanziaria

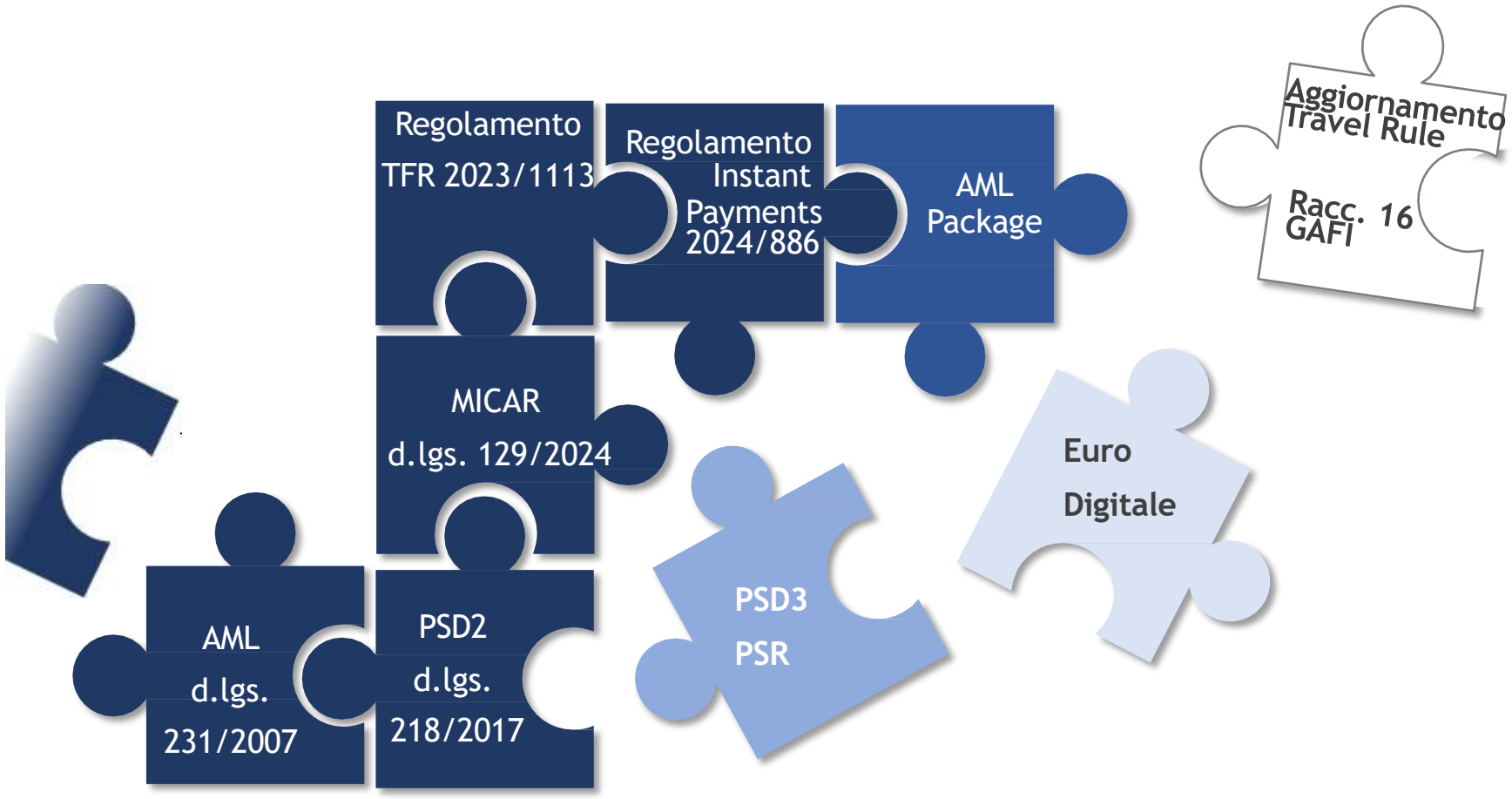
Perseguire le finalità istituzionali

- Tutela degli utenti
- Integrità del sistema finanziario
- Stabilità e sicurezza dei mercati

Innovazione, sostenibilità e stabilità del sistema finanziario

Evoluzione del quadro delle regole

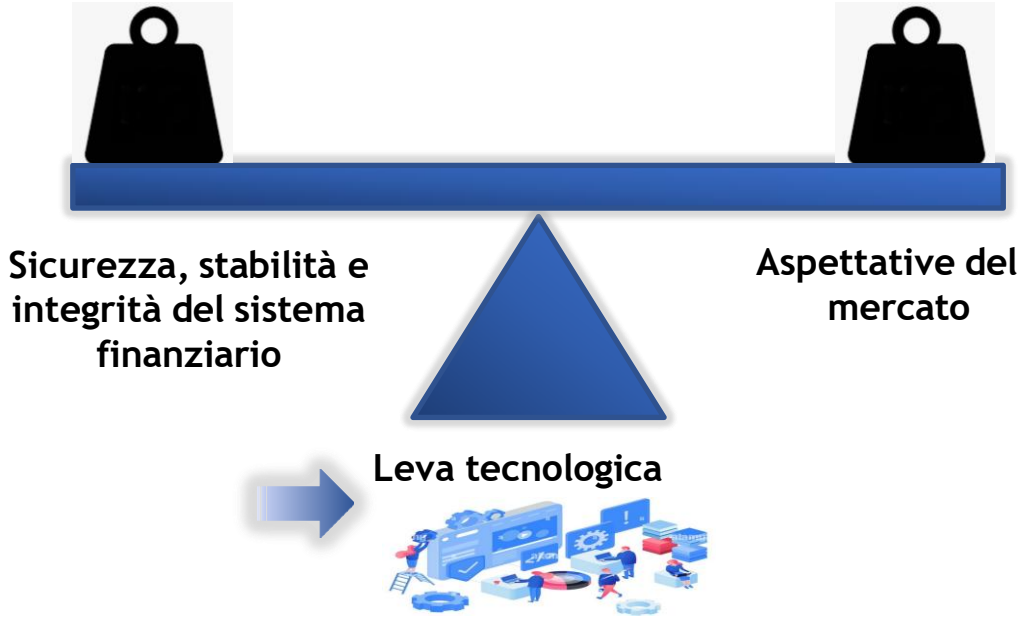
Il quadro normativo riflette i trend di mercato.



Innovazione, sostenibilità e stabilità del sistema finanziario

Evoluzione del quadro delle regole

Esigenza di definire un punto di equilibrio tra sostegno all'innovazione e aspettative del mercato e salvaguardia degli interessi degli utenti (consumatori e imprese) e dell'economia in generale



Innovazione, sostenibilità e stabilità del sistema finanziario

Verso la twin transition

I principali fattori che stanno trasformando il sistema finanziario, orientandone i nuovi modelli di business, di governance e di controllo del rischio, sono:

- la rivoluzione digitale
- la transizione verde.

Le connessioni tra questi due fattori, spesso indicati congiuntamente con il termine twin transition, sono molteplici: da un lato, la digitalizzazione può agevolare la transizione verso un'economia più sostenibile, mettendo a disposizione tecnologie in grado di ridurre l'impatto ambientale dei sistemi di produzione; dall'altro, essa potrebbe costituire un ostacolo, qualora fosse incurante della sostenibilità ambientale.

In questo contesto, il sistema dei pagamenti è il "motore" che permette gli scambi, sostenendo così l'attività economica e sospingendo la crescita. Le tecnologie digitali permettono di conseguire soluzioni di pagamento sempre più avanzate, efficienti, accessibili, inclusive. La competizione, accresciuta con il fintech, aumenta la pressione verso la modernizzazione; l'industria dei pagamenti si configura come un "incubatore di innovazione".

Innovazione, sostenibilità e stabilità del sistema finanziario

Il futuro dei pagamenti

In prospettiva futura è verosimile attendersi che famiglie e imprese potranno passare facilmente da una soluzione di pagamento all'altra; i pagamenti digitali potranno essere effettuati sia in moneta di banca centrale sia con moneta privata; i regolamenti istantanei diventeranno la norma; la velocità, la facilità d'uso e il costo dei pagamenti transfrontalieri non si discosteranno significativamente da quelli dei pagamenti domestici; anche le persone meno abbienti e meno istruite avranno accesso a soluzioni di pagamento di tipo digitale.

La situazione attuale si discosta ancora da questa visione sotto diversi profili. In particolare, molte persone hanno un accesso limitato o nullo ai pagamenti elettronici; i pagamenti transfrontalieri, che stanno vivendo un rapido trend di crescita, sono ancora relativamente costosi, lenti, poco trasparenti e con accesso limitato.

Innovazione, sostenibilità e stabilità del sistema finanziario

Il payment package

Il Payment Package è l'insieme di proposte legislative presentate dalla Commissione Europea il 28 giugno 2023 per modernizzare il quadro normativo dei servizi di pagamento nell'UE, composto da:

- PSD3 (Payment Services Directive 3) - Proposta di Direttiva
- PSR (Payment Services Regulation) - Proposta di Regolamento
- Revisione della Direttiva sulla moneta elettronica (EMD)

Motivazioni della Riforma:

- Evoluzione tecnologica del settore pagamenti
- Crescita dei pagamenti digitali
- Necessità di rafforzare la protezione consumatori
- Aumento delle frodi nei pagamenti online
- Frammentazione del mercato unico

Innovazione, sostenibilità e stabilità del sistema finanziario

Il payment package

OBIETTIVI

- Rafforzare la tutela degli utenti e il contrasto alle frodi (APP fraud, spoofing, IBAN/name check, condivisione info antifrode).
- Aggiornare l'open banking (PSD2) per favorire innovazione e concorrenza, con interfacce migliori e consensi più chiari.
- Creare un level playing field in tutta l'UE: meno frammentazione (regolamento direttamente applicabile), requisiti omogenei per banche, IP/IMEL.
- Rendere davvero "istantanei" i bonifici in euro, con costi/operatività parificati ai bonifici ordinari

DESTINATARI

- PSP: banche, istituti di pagamento (IP), istituti di moneta elettronica (IMEL), prestatori di servizi di informazione/disposizione (AIS/PIS), acquirer.
- Gestori di schemi e sistemi di pagamento, fornitori di soluzioni di sicurezza/antifrode, terze parti open banking.
- Utenti finali (consumatori e imprese), merchant e marketplace; per l'Italia, sotto la vigilanza di Banca d'Italia (competent authority per i PSP).

La pubblicazione del New Payments Package, attesa nei prossimi mesi, richiederà ai PSP di intraprendere le necessarie azioni di adeguamento, nello specifico alla PSD3 e al PSR, frutto di un riesame della PSD2 attualmente in vigore.

La nuova direttiva e il regolamento mirano a risolvere quattro questioni emerse come prioritarie dall'analisi dello stato attuale della regolamentazione del mercato:

1. migliorare la sicurezza contro le frodi per rafforzare la fiducia nei sistemi di pagamento,
2. rafforzare l'open banking,
3. armonizzare le norme tra Stati membri
4. garantire una concorrenza equa tra attori bancari e non bancari.

Innovazione, sostenibilità e stabilità del sistema finanziario

Sicurezza e fiducia nei pagamenti digitali: le novità di PSD3 e PSR

La fiducia del consumatore è il fulcro di qualsiasi modello di business di successo. La PSD2 ha fatto passi importanti in questa direzione riducendo il numero di frodi con l'introduzione della SCA (Autenticazione forte del cliente), ma l'evoluzione della tecnologia, la crescente sofisticazione delle frodi e la crescita in tutti gli Stati Membri dell'adozione dei sistemi di pagamento digitali hanno portato il regolatore a intervenire per garantire la continuità della tutela del consumatore e il mantenimento della sua fiducia.

La PSR promette di rafforzare ulteriormente la sicurezza, obbligando, ad esempio, a verificare la corrispondenza tra il nome beneficiario e IBAN (Check IBAN) prima di confermare una transazione anche nei bonifici ordinari e migliorando i meccanismi di monitoraggio delle transazioni e condivisione delle frodi tra gli operatori di settore.

Il Regolamento introduce, inoltre, specifiche relative ad obblighi di trasparenza nell'ottica di aumentare la consapevolezza del consumatore nel momento della transazione e della gestione delle controversie: il Parlamento con gli emendamenti al testo della Commissione rafforza questo punto parlando espressamente di "comunicazione trasparente e facilmente comprensibile". In particolare, il Regolatore insiste sulle disposizioni di trasparenza in 3 macro-ambiti: operazioni in valuta, operazioni di prelievo e la gestione delle controversie con comunicazioni che rendano più accessibile all'utente finale la conoscenza delle commissioni applicate dai PSP, inclusa la loro composizione, e le modalità per effettuare eventuali reclami.

Per incentivare l'adozione delle soluzioni di pagamento digitali per i consumatori più vulnerabili che ricorrono frequentemente al contate, il testo della PSR proposto dalla Commissione, rafforzato dagli emendamenti del Parlamento, propone: disposizioni circa le modalità di comunicazioni ai consumatori che devono essere "chiare e comprensibili", impegni nell'educazione al riconoscimento delle frodi per la loro prevenzione e l'obbligo di rivedere i processi di SCA per garantirne l'accessibilità anche con mezzi differenti dallo smartphone.

Innovazione, sostenibilità e stabilità del sistema finanziario

Open Banking e il rapporto con PSD3 e PSR

L'open banking è stato uno degli obiettivi più ambiziosi della PSD2, e ora con PSD3 e, soprattutto, PSR si punta a rafforzare questa trasformazione. L'idea è quella di creare un ecosistema in cui dati e servizi circolino liberamente tra banche e terze parti (AISP e PISP), offrendo agli utenti esperienze più fluide e personalizzate.

Tuttavia, i risultati degli anni successivi all'entrata in vigore della PSD2 rivelano che, sebbene l'adozione di soluzioni di open banking sia cresciuta (+1,7% nel 2024), siamo ancora lontani dal pieno potenziale. I player del settore segnalano tra le principali problematiche: barriere tecnologiche, un'offerta limitata, alti costi di investimento, lacune regolamentari, API bancarie di scarsa qualità e customer experience poco soddisfacente.

L'analisi della nuova regolamentazione rivela che l'intento del Regolatore è proprio quello di lavorare sulle principali problematiche segnalate dagli operatori di mercato: le nuove norme promettono di eliminare gli ostacoli tecnici, obbligando gli operatori del sistema a fornire interfacce standard e accessibili alle terze parti per facilitare l'innovazione e garantire equa concorrenza.

Da questo punto di vista, la cooperazione e la proposizione di soluzioni accessibili, trasparenti e in grado di offrire servizi a valore aggiunto per il consumatore finale sarà la chiave per un concreto passo avanti verso il sistema di open banking e, più in generale, di open finance auspicato dall'Unione Europea. Tale sistema è supportato anche dalla proposta del nuovo framework per l'accesso e l'utilizzo sicuro dei dati finanziari contenuto nel regolamento denominato "Financial Data Access" (FIDA).

Innovazione, sostenibilità e stabilità del sistema finanziario

L’evoluzione della normativa sui pagamenti

Ripercorrendo brevemente le principali tappe dell’evoluzione della normativa europea sui servizi di pagamento, si può rilevare che la prima direttiva europea sui servizi di pagamento (anche nota come “Payment Services Directive” o “PSD”) - emanata nel 2007 - aveva l'obiettivo fondamentale di creare un quadro giuridico armonizzato per un mercato dei pagamenti integrato all’interno dell'UE.

La seconda direttiva sui servizi di pagamento - entrata in vigore il 13 gennaio 2016 e con termine di recepimento nel 2018 - costituisce l’attuale framework normativo europeo per la regolamentazione dei pagamenti al dettaglio nell'UE, nazionali e transfrontalieri e con essa il legislatore europeo ha affrontato gli ostacoli relativi ai nuovi tipi di servizi di pagamento e ha migliorato il livello di protezione e sicurezza dei consumatori.

Più nello specifico, le principali finalità della PSD2 sono state quelle di (i) garantire parità di condizioni tra gli operatori tradizionali e i nuovi fornitori di servizi di pagamento (carte, internet e dispositivi mobili), (ii) migliorare l'efficienza, la trasparenza e la facoltà di scelta per gli utenti dei servizi di pagamento (consumatori e commercianti), (iii) agevolare la prestazione di servizi di pagamento a livello transfrontaliero, (iv) favorire l'innovazione nei servizi di pagamento e (v) garantire elevati livelli di protezione per gli utenti dei servizi di pagamento in tutti gli Stati membri.

Nell'ambito delle strategie per i pagamenti al dettaglio e la finanza digitale, nel 2022, la Commissione ha svolto una valutazione in merito all'applicazione della PSD2, al fine di valutare se la relativa disciplina fosse ancora adeguata rispetto ai mutamenti tecnologici, sociali e di mercato medio tempore intervenuti. Tale valutazione, passata anche attraverso una consultazione dell’EBA e una consultazione pubblica, ha rilevato che la direttiva ha effettivamente conseguito alcuni degli obiettivi originariamente fissati. In particolare, un rilevante impatto positivo è stato registrato nella prevenzione delle frodi, attraverso l'introduzione della autenticazione forte del cliente (Strong Customer Authentication - SCA). Inoltre, la PSD2 è stata particolarmente efficace nell’aumentare l'efficienza, la trasparenza e la scelta dei diversi tipi di strumenti di pagamento per gli utenti.

Innovazione, sostenibilità e stabilità del sistema finanziario

Alcune criticità nella PSD2

Tuttavia, dalla valutazione sono emerse anche alcune criticità, ad esempio, nel conseguimento di una effettiva condizione di parità tra prestatori di servizi di pagamento bancari e non bancari, il cui squilibrio deriva fondamentalmente dalla mancanza di un accesso diretto, da parte di questi ultimi, ai fondamentali sistemi di pagamento.

Peraltro, nonostante la comparsa di un rilevante numero di nuovi prestatori di servizi di pagamento non bancari, nel territorio dell'Unione europea si sono registrati risultati contrastanti nell'adozione di servizi di open banking, soprattutto a causa di problemi relativi alle prestazioni delle interfacce di accesso ai dati dei clienti per i prestatori di tali servizi. Inoltre, sebbene l'offerta di servizi di pagamento a livello transfrontaliero sia in aumento, molti sistemi di pagamento (in particolare i sistemi relativi alle carte di debito) continuano ad avere una portata per lo più nazionale. Infatti, le condizioni per consentire la riduzione dei costi a carico degli esercenti non si sono ancora pienamente concretizzate e, per tale ragione, non è ancora stata realizzata alcuna soluzione di pagamento interamente paneuropea.

In conclusione, la valutazione ha rilevato che, nonostante la PSD2 abbia determinato significativi miglioramenti nel settore dei pagamenti, i relativi obiettivi sono stati conseguiti soltanto in parte. Pertanto, la Commissione ha deciso di proporre gli opportuni aggiornamenti normativi attraverso un nuovo Regolamento sui Servizi di Pagamento ("PSR") e la terza Direttiva sui Servizi di Pagamento ("PSD3").

Relativamente all'iter di approvazione della suddetta regolamentazione, in data 23 aprile 2024 il Parlamento Europeo ha approvato con emendamenti rispetto alle proposte della Commissione i testi della direttiva e del regolamento, evidenziando altresì la volontà di migliorare la prestazione di servizi di pagamento in tutti gli Stati Membri. Attualmente, con riguardo ad entrambi i dossier, sono in corso le discussioni del Consiglio dell'UE; si attende l'avvio delle discussioni e dei negoziati interistituzionali che coinvolgeranno congiuntamente la Commissione Europea, il Parlamento Europeo e il Consiglio dell'Unione Europea per giungere ad un testo finale di compromesso.

Innovazione, sostenibilità e stabilità del sistema finanziario

Alcune criticità nella PSD2 (segue)

Nell'ambito della valutazione della PSD2, una delle criticità rilevate attiene al fatto che non sempre i poteri delle autorità di vigilanza sono apparsi effettivamente adeguati alle relative funzioni e, talvolta, l'applicazione della PSD2 all'interno dell'Unione Europea risulta disomogenea tra i singoli Stati membri, causando fenomeni di arbitraggio normativo.

In tale contesto, i prestatori di servizi di pagamento si trovano in una situazione di incertezza riguardo ai propri obblighi. Più nel dettaglio, si rileva che, come noto, la seconda direttiva sulla moneta elettronica (EMD2) contiene norme in materia di autorizzazione e vigilanza degli istituti di moneta elettronica ("IMEL"), mentre la PSD2 contiene norme in materia di autorizzazione e vigilanza degli istituti di pagamento ("IP") e stabilisce diritti e obblighi, anche in materia di trasparenza nei rapporti tra tutti i prestatori di servizi di pagamento (compresi gli IMEL) con i relativi utenti.

Poiché le operazioni di pagamento che utilizzano moneta elettronica sono già ampiamente disciplinate dalla PSD2, il quadro giuridico applicabile agli IMEL e agli IP è apparso già ragionevolmente coerente. Tuttavia, le prescrizioni in materia di autorizzazione, in particolare il capitale iniziale e il capitale corrente, unitamente ad alcuni concetti fondamentali che disciplinano le attività relative alla moneta elettronica, quali la relativa emissione, distribuzione e la rimborsabilità, presentano alcune differenze rispetto ai servizi forniti dagli IP. In tale contesto, le autorità di vigilanza hanno incontrato difficoltà pratiche nel definire chiaramente i due regimi applicabili e nel distinguere i prodotti/servizi di moneta elettronica dai servizi di pagamento offerti dagli IP.

Tale circostanza ha suscitato evidenti preoccupazioni in merito all'arbitraggio normativo e alla disparità di condizioni, oltre a causare problemi relativi alla possibile elusione delle prescrizioni della EMD2, approfittando della somiglianza tra servizi di pagamento e servizi di moneta elettronica.

Innovazione, sostenibilità e stabilità del sistema finanziario

La soluzione della Commissione UE

Pertanto, al fine di migliorare l'applicazione e l'attuazione negli Stati membri, la Commissione ha deciso di sostituire la maggior parte delle disposizioni della PSD2 con un regolamento direttamente applicabile, chiarendo gli aspetti della PSD2 che risultano essere attualmente poco chiari o ambigui, integrando i regimi di autorizzazione per gli IP e gli IMEL e orientandosi, inoltre, per un rafforzamento delle sanzioni.

Più nello specifico, la Commissione ha ritenuto opportuno introdurre le modifiche all'attuale framework normativo tramite due atti legislativi distinti:

- la proposta di direttiva, contenente, in particolare, norme in materia di autorizzazione e vigilanza degli istituti di pagamento e
- una proposta di regolamento contenente le norme per i prestatori di servizi di pagamento, sia che prestino servizi di pagamento che di moneta elettronica.

In particolare, è apparsa appropriata la direttiva, dal momento che l'autorizzazione e la vigilanza degli istituti finanziari in generale (compresi gli istituti di pagamento e le altre categorie di prestatori di servizi di pagamento, come gli enti creditizi) restano di competenza nazionale degli Stati membri e non è proposta alcuna autorizzazione o vigilanza a livello dell'UE.

Innovazione, sostenibilità e stabilità del sistema finanziario

Crescenti fenomeni di frode

Una delle principali innovazioni della PSD2 è stata l'introduzione della autenticazione forte del cliente (Strong Customer Authentication, SCA), la quale, come noto, richiede l'utilizzo di almeno due fattori di autenticazione basati sulla conoscenza (ad esempio, una password), sul possesso (come una carta) o sull'inerenza (come, un'impronta digitale).

Nello specifico la PSD2 prevede che i prestatori di servizi di pagamento sono tenuti ad applicare l'SCA quando il pagatore accede a un conto di pagamento on line, dispone un'operazione di pagamento elettronico o effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi.

Tuttavia, nonostante il notevole successo ottenuto dalla SCA, permangono delle problematiche significative in relazione alle frodi. Queste criticità derivano principalmente dal fatto che le tattiche utilizzate per compiere le truffe sono in continua evoluzione e, spesso, viene ingannato direttamente proprio il pagatore, il quale crede di interagire con un beneficiario autentico o addirittura un rappresentante della banca.

Le frodi come il phishing, vishing, smishing, spoofing e altre ancora, non possono essere efficacemente contrastate dalla SCA, perché, la maggior parte di queste truffe si verifica - sia dal punto di vista tecnico che legale - prima dell'applicazione della SCA.

Innovazione, sostenibilità e stabilità del sistema finanziario

Crescenti fenomeni di frode

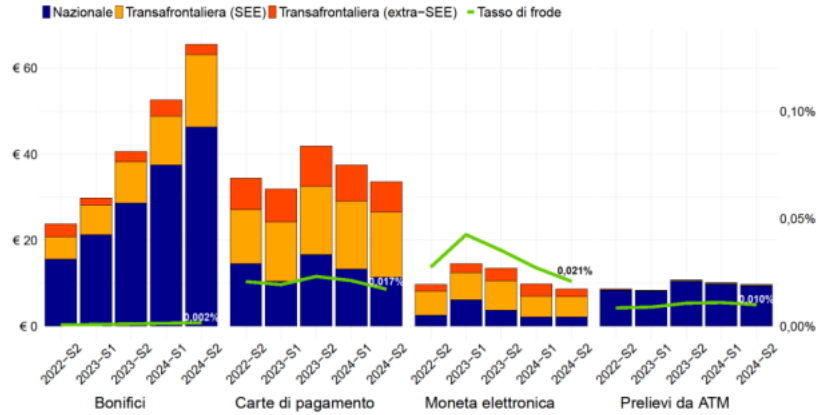
Lo strumento con l'ammontare più elevato di operazioni fraudolente è il bonifico, seguito dalle carte di pagamento. In termini di frequenza, invece, il maggior numero di operazioni fraudolente riguarda le carte di pagamento, lo strumento più utilizzato (oltre il 70% del totale delle operazioni) seguite dalla moneta elettronica.

Nel secondo semestre del 2024 il valore dei bonifici fraudolenti (esclusi quelli eseguiti allo sportello) disposti dalla clientela tramite PSP italiani ammonta a circa 65,5 milioni di euro (+61% su base annua), mentre il valore delle operazioni fraudolente con carte di pagamento (debito e credito) e quello con moneta elettronica emesse da PSP italiani si collocano, rispettivamente, a 34 milioni (-20%) e 9 milioni (-36%).

Livelli e tassi di frode delle operazioni fraudolente per strumento di pagamento e prospettiva geografica del PSP del beneficiario

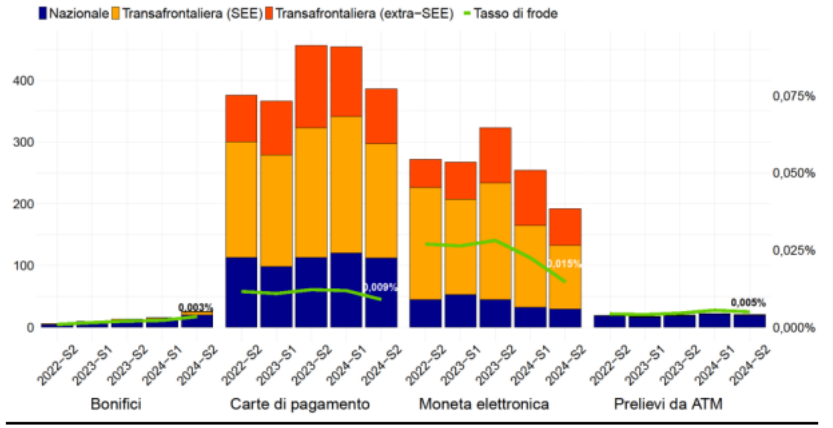
a) Valore delle operazioni fraudolente

(asse di sinistra: milioni di euro; asse di destra: in % del valore totale delle operazioni per strumento di pagamento)



b) Numero di operazioni fraudolente

(asse di sinistra: migliaia; asse di destra: in % del numero totale delle operazioni per strumento di pagamento)



Fonte: Elaborazioni su dati di matrice dei conti forniti dai PSP italiani.

Innovazione, sostenibilità e stabilità del sistema finanziario

Crescenti fenomeni di frode

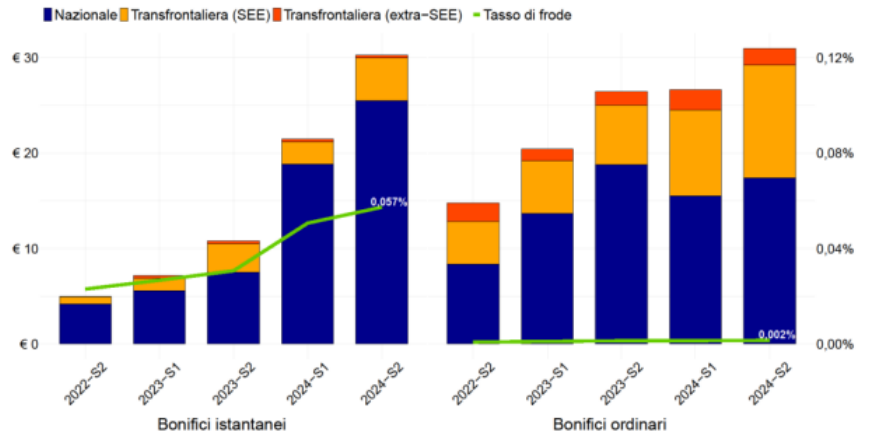
Il tasso di frode è rimasto stabile e molto contenuto (0,0015%) per i bonifici ordinari, mentre per quelli istantanei è aumentato (+90% su base annua) ed è di gran lunga più elevato (a 0,057%).

In termini di numero di operazioni, esso risulta pari allo 0,001% per i bonifici ordinari, contro lo 0,027% per i bonifici istantanei (rispettivamente 0,001% e 0,014% un anno prima)

Livelli e tassi di frode delle operazioni fraudolente: bonifici istantanei vs. bonifici ordinari per prospettiva geografica del PSP del beneficiario

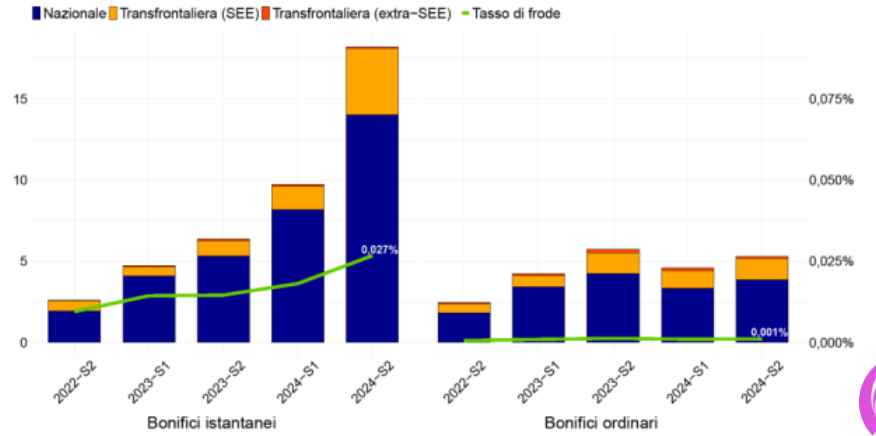
a) Valore delle operazioni fraudolente

(asse di sinistra: milioni di euro; asse di destra: in % del valore totale delle operazioni di pagamento)



b) Numero di operazioni fraudolente

(asse di sinistra: migliaia; asse di destra: in % del numero totale delle operazioni di pagamento)



Fonte: Elaborazioni su dati di matrice dei conti forniti dai PSP italiani.

Innovazione, sostenibilità e stabilità del sistema finanziario

Crescenti fenomeni di frode

Nel caso delle carte di pagamento, le operazioni “a distanza” risultano più rischiose di quelle al punto vendita. Nel secondo semestre del 2024 l’incidenza delle operazioni fraudolente nei pagamenti con carte utilizzate on line (ad esempio, sui siti e-commerce) rappresenta, infatti, il 73,5% del valore e il 76% del numero di frodi complessive, nonostante la maggior parte delle operazioni venga effettuata dagli utenti al punto vendita fisico.

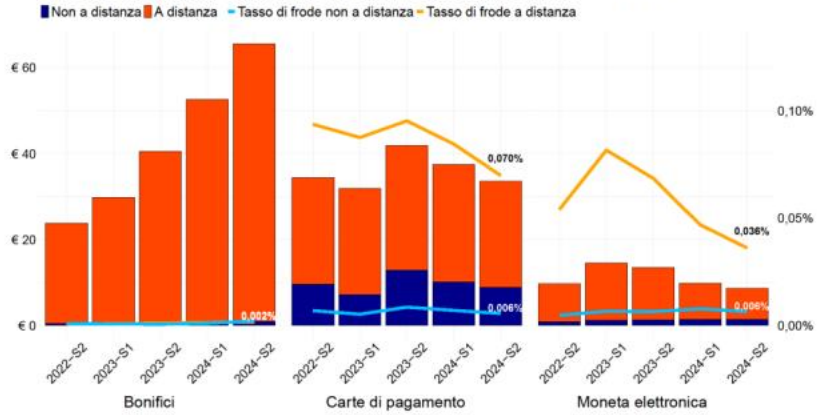
Il tasso di frode per le operazioni “a distanza” (0,07% in valore; 0,046% in numero) è dunque pari a oltre dieci volte quello per le operazioni “non a distanza” (0,006% in valore; 0,003% in numero), divario che sembra essersi ridotto nel corso del 2024.

Anche per la moneta elettronica, l’incidenza delle frodi è maggiore nelle operazioni “a distanza”, sebbene sia in riduzione. Nel secondo semestre del 2024 il 51% del valore delle operazioni risulta “non a distanza” (61% del numero), mentre l’84% del valore delle frodi riguarda le operazioni “a distanza” (88% del numero).

Livelli e tassi di frode per strumento di pagamento e canale di utilizzo “a distanza” vs. “non a distanza»

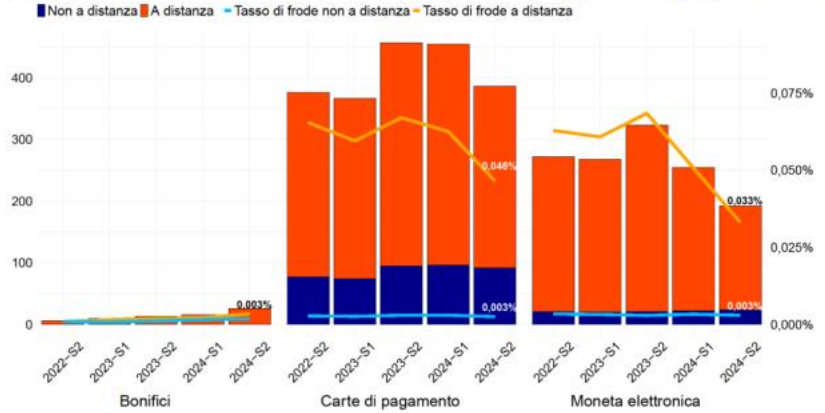
a) Valore delle operazioni fraudolente

(asse di sinistra: milioni di euro; asse di destra: in % del valore totale delle operazioni per strumento di pagamento e canale di utilizzo)



b) Numero di operazioni fraudolente

(asse di sinistra: migliaia; asse di destra: in % del numero totale delle operazioni per strumento di pagamento e canale di utilizzo)



Fonte: Elaborazioni su dati di matrice dei conti forniti dai PSP italiani.

Innovazione, sostenibilità e stabilità del sistema finanziario

Crescenti fenomeni di frode

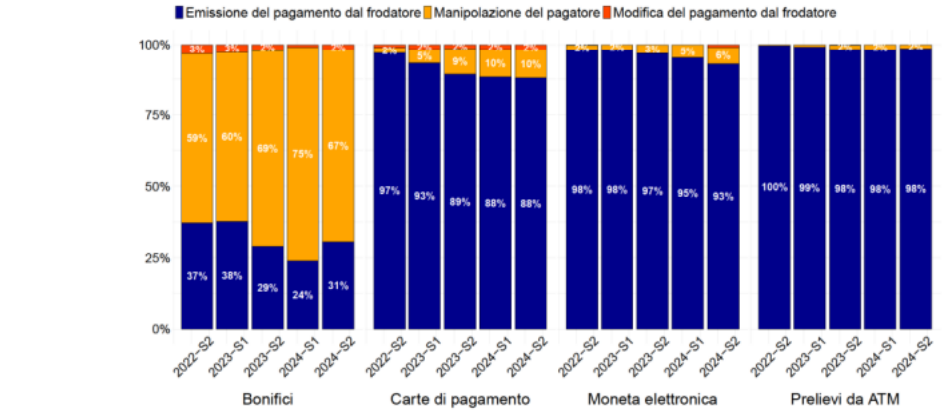
Le GL EBA sul fraud reporting ai sensi della PSD2 individuano tre principali categorie di frode:

1. Emissione di un ordine di pagamento da parte di un frodatore: tipologia di frode senza il consenso del legittimo titolare, in cui il frodatore effettua il pagamento a seguito di appropriazione indebita dello strumento stesso o di informazioni e dati confidenziali quali numeri di carta di credito, PIN e credenziali d'accesso (username, password) ai conti bancari on line.
2. Modifica di un ordine di pagamento da parte del frodatore: tipologia di frode senza il consenso del legittimo titolare, in cui il frodatore intercetta e modifica un ordine di pagamento legittimo durante la comunicazione elettronica tra il dispositivo dell'utente pagatore e il PSP (es. tramite malware o attacchi informatici), oppure interviene direttamente nel sistema del PSP prima che l'ordine sia autorizzato e liquidato.
3. Manipolazione del pagatore: tipologia di frode con il consenso del legittimo titolare, il quale, in buona fede, viene indotto dal frodatore a impartire un'istruzione di pagamento al proprio PSP a favore di un conto fraudolento. La manipolazione avviene soprattutto tramite tecniche di social engineering (phishing, vishing, spoofing), che imitano il comportamento di persone fidate (familiari, dipendenti del PSP, ecc.).

Operazioni fraudolente per tipologia di frode

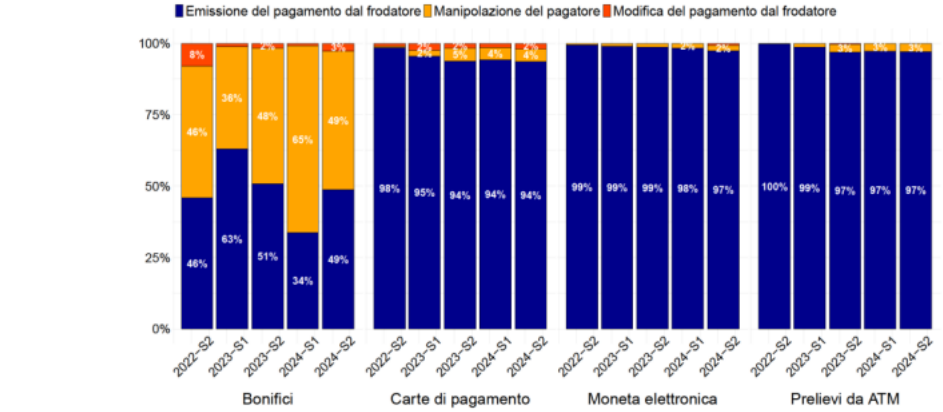
a) Valore delle operazioni fraudolente

(quote percentuali)



b) Numero di operazioni fraudolente

(quote percentuali)



Fonte: Elaborazioni su dati di matrice dei conti forniti dai PSP italiani.

Innovazione, sostenibilità e stabilità del sistema finanziario

Tentativi di frode più comuni nei pagamenti

Nell'ambito delle frodi più comune nei pagamenti rilevano le seguenti:

- il **phishing** (tipologia di frode ormai diffusa, effettuata tramite un'e-mail "civetta" con il logo contraffatto di un istituto di credito diverso da quello in cui insiste il conto corrente del pagatore o di una qualsiasi società commerciale come Poste, DHL, Expedia, Amazon, in cui il pagatore viene invitato a inserire, in appositi campi, i proprio dati riservati quali ad esempio: numero di carta di credito, password di accesso al servizio di home banking, ecc.), motivando tale richiesta con ragioni di ordine tecnico);
- Il **vishing** (deriva dall'unione fra due parole: "voice" e "phishing". Un attacco di vishing è simile al phishing, ma avviene per telefono o tramite messaggio vocale);
- lo **smishing** è una forma di phishing che utilizza i telefoni cellulari come piattaforma di attacco, inviando messaggi di testo o SMS (da cui il nome "SMiShing") con l'intento di raccogliere informazioni personali, compresi il codice fiscale e/o il numero di carta di credito e/o i codici statici e dinamici dell'home banking delle potenziali vittime. Il contenuto dei messaggi consiste nell'attirare l'attenzione della vittima su operazione sospette o anomalie nel processo di aggiornamento relativo alla sicurezza dei dati personali, invitandola a cliccare su un collegamento ipertestuale, al fine di intervenire sulle presunte anomalie. La vittima, attraverso il reindirizzamento a pagine web che copiano graficamente quelle della propria banca, è tratta in inganno e indotta a inserire le proprie credenziali (statiche e dinamiche). Lo smishing di regola può essere seguito dal vishing, ovvero da telefonate da parte del truffatore, il quale fingendosi un operatore della banca, si offre di "aiutare" il cliente nella risoluzione delle anomalie segnalate;
- lo **spoofing** si verifica quando i frodatori riescono a camuffare la provenienza della e-mail o dell'sms "civetta", facendolo comparire all'interno del thread dei messaggi, autentici e legittimi, intercorsi con il proprio intermediario. Generalmente, tali messaggi contengono un collegamento ipertestuale che rinvia a pagine di phishing dove l'utente vien e indotto ad inserire le proprie credenziali.

Innovazione, sostenibilità e stabilità del sistema finanziario

Tentativi di frode più comuni nei pagamenti

Spesso è proprio lo stesso pagatore che, in buona fede, autorizza l'operazione di pagamento attraverso la SCA. Proprio per tale ragione, la Commissione ritiene che la differenza tra operazioni autorizzate e non autorizzate sia sempre più vaga e complessa da applicare nella pratica, sollevando anche dubbi relativamente al fatto se un'operazione possa effettivamente considerarsi autorizzata solo perché è stata eseguita la SCA. Un ulteriore aspetto critico che è stato rilevato dagli operatori riguarda la scarsa consapevolezza dei consumatori riguardo alle principali tipologie di frodi. Questa circostanza ha evidenziato l'importanza dell'educazione dei consumatori e della loro alfabetizzazione in merito alle frodi e ai rischi associati a particolari strumenti di pagamento.

A questo scopo, è quindi apparso opportuno implementare campagne di sensibilizzazione più efficaci. In tale contesto, è stato anche rilevato che, nonostante i fornitori di servizi di pagamento abbiano accesso ad un rilevante patrimonio informativo, spesso non vi è alcuna condivisione delle informazioni con gli altri prestatori di servizi.

Al fine di sopperire alle criticità sopraindicate, la Commissione ha proposto:

(i) nuove misure volte a un maggiore utilizzo dell'autenticazione forte del cliente,

(ii) una base giuridica per lo scambio delle informazioni in materia di frodi tra prestatori di servizi di pagamento nel rispetto del Regolamento (UE) 2016/679 (“GDPR”),

(iii) dei sistemi di verifica della corrispondenza tra IBAN e nome del beneficiario a tutti i bonifici (attualmente prevista soltanto per i pagamenti istantanei) e

(iv) l'inversione condizionata di responsabilità (dagli utenti ai prestatori di servizi di pagamento) per le frodi nel caso in cui sussistano specifiche carenze da parte dei prestatori di servizi di pagamento (mancato funzionamento della verifica IBAN/nome e truffe con furto di identità di dipendenti della banca).

Innovazione, sostenibilità e stabilità del sistema finanziario

Nuove misure volte a un maggiore utilizzo dell'autenticazione forte del cliente

In particolare, è stata introdotta una nuova disposizione che impone ai prestatori di servizi di pagamento di disporre di meccanismi di monitoraggio delle operazioni che migliorino la prevenzione e l'individuazione delle operazioni fraudolente. Tale disposizione chiarisce ulteriormente la nozione del concetto di "inerenza" e precisa che i suddetti meccanismi di monitoraggio delle operazioni devono basarsi sulle caratteristiche tipiche di ciascun pagatore nell'usuale utilizzo delle credenziali di sicurezza (ad esempio l'ubicazione al momento dell'operazione, il dispositivo utilizzato, le abitudini di spesa, il negozio in cui è stato effettuato l'acquisto, etc.).

Per quanto riguarda l'applicazione dell'autenticazione forte del cliente nel caso di operazioni di pagamento disposte da esercenti, il Regolamento chiarisce che è necessario applicare la SCA al momento dell'istituzione del mandato, ma senza bisogno di applicarla per le successive operazioni. Inoltre, sono state introdotte alcune disposizioni volte a migliorare l'accessibilità della SCA per le persone con disabilità, persone anziane o le persone con scarse competenze digitali e coloro che non hanno accesso ai canali digitali o a uno smartphone, affinché dispongano almeno di un mezzo che le consenta di effettuare un'autenticazione forte del cliente.

Innovazione, sostenibilità e stabilità del sistema finanziario

Una base giuridica per lo scambio delle informazioni in materia di frodi tra PSP nel rispetto del GDPR

Ai fini del monitoraggio delle operazioni, sono state aggiunte alcune specifiche disposizioni che consentono ai prestatori di servizi di pagamento di scambiare, su base volontaria, dati personali quali gli identificativi unici di un beneficiario nell'ambito di accordi di condivisione delle informazioni.

Tali accordi di condivisione delle informazioni devono definire i dettagli della partecipazione e degli elementi operativi, compreso l'uso di piattaforme informatiche dedicate. Tuttavia, prima di concludere tali accordi, i prestatori di servizi di pagamento devono effettuare una valutazione d'impatto sulla protezione dei dati e, se necessario, procedere a una consultazione preliminare dell'autorità di controllo, conformemente al GDPR

Innovazione, sostenibilità e stabilità del sistema finanziario

Sistemi di verifica della corrispondenza tra IBAN e nome del beneficiario a tutti i bonifici

È stata introdotta una disposizione analoga a quanto previsto nella proposta della Commissione che modifica il regolamento SEPA per quanto riguarda i pagamenti istantanei, con la quale viene previsto l'obbligo per il prestatore di servizi di pagamento del beneficiario di fornire all'utente, su richiesta di quest'ultimo, un servizio che verifichi la corrispondenza dell'identificativo unico del beneficiario con il nome del beneficiario fornito dal pagatore e notifichi al prestatore di servizi di pagamento del pagatore qualsiasi discrepanza rilevata.

In caso di mancata corrispondenza, il prestatore di servizi di pagamento del pagatore è tenuto a notificare al pagatore tale discrepanza e la relativa portata. La notifica deve essere effettuata prima che il pagatore finalizzi l'ordine di pagamento e prima che il prestatore di servizi di pagamento esegua il bonifico.

In proposito la Commissione ritiene che, in generale, l'estensione della verifica IBAN/nome del beneficiario ai pagamenti interesserà 1.200-1.300 prestatori di servizi di pagamento, con un costo in media di alcune centinaia di migliaia di euro una tantum e di alcune decine di migliaia di euro per spese di manutenzione annue. Sarà tuttavia consentito addebitare ai clienti le spese per l'utilizzo di tale servizio permettendo un parziale recupero dei costi.

Innovazione, sostenibilità e stabilità del sistema finanziario

L’inversione della responsabilità sui PSP in caso di carenze

Nella disposizione relativa alla responsabilità del prestatore di servizi di pagamento per operazioni di pagamento non autorizzate è stato aggiunto un chiarimento secondo cui solo ragionevoli motivi per sospettare una frode da parte del pagatore possono comportare un rifiuto del rimborso da parte del prestatore di servizi di pagamento. In tal caso, il prestatore di servizi di pagamento deve motivare il rifiuto del rimborso e indicare gli organismi ai quali il pagatore può deferire la questione.

Il prestatore di servizi di pagamento del pagatore è ritenuto responsabile dell'intero importo del bonifico nel caso in cui non abbia notificato al pagatore una discrepanza rilevata tra l'identificativo unico e il nome del beneficiario fornito dal pagatore. Inoltre, è ritenuto responsabile quando un consumatore è stato indotto ad autorizzare un'operazione di pagamento da un terzo che ha finto di essere un dipendente del prestatore di servizi di pagamento del consumatore.

In tale contesto, è stato inoltre introdotto l'obbligo per i prestatori di servizi di comunicazione elettronica di cooperare con i prestatori di servizi di pagamento al fine di prevenire tali frodi. Il prestatore di servizi di pagamento del beneficiario, se la responsabilità è a lui imputabile, è tenuto a rimborsare il danno finanziario subito dal prestatore di servizi di pagamento del pagatore. Le disposizioni in materia di notifica e rettifica delle operazioni di pagamento non autorizzate o non correttamente eseguite, requisiti informativi e diritto di regresso sono state aggiornate al fine di rispecchiare la nuova disposizione in materia di responsabilità per l'applicazione non corretta del servizio di verifica della corrispondenza.

Innovazione, sostenibilità e stabilità del sistema finanziario

Misure contro i fenomeni di frode

Le istituzioni Europee hanno dimostrato che la prevenzione delle frodi è un elemento chiave della regolamentazione europea in tema di pagamenti e, a tal riguardo, sono in corso discussioni al fine di stabilire precise regole relative alla responsabilità degli utenti e dei soggetti che prestano servizi di pagamento, garantendo un alto livello di protezione dell'utente ma anche un principio di responsabilizzazione per i comportamenti tenuti dal medesimo.

In particolare, il concetto di autorizzazione della transazione è centrale nelle discussioni in corso ed infatti, al fine di disciplinare correttamente le transazioni autorizzate dagli utenti, si ritengono rilevanti tre elementi:

- l'autenticazione della transazione,
- la volontà dell'utente a predisporre la transazione. e
- la responsabilizzazione per le condotte tenute dal medesimo in relazione all'esecuzione della transazione stessa.

In ottica futura si potrebbe qualificare un'operazione di pagamento come correttamente autorizzata solo nel caso in cui sia posta correttamente in essere l'autenticazione del pagatore e sia accertata l'intenzione dell'utente di compiere tale pagamento; in tal caso non sorgerebbe alcuna responsabilità in capo al PSP. Viceversa, una transazione è considerata non autorizzata nel caso in cui non sia stata correttamente effettuata l'autenticazione da parte del pagatore e, in tal caso, il saldo del conto di pagamento dovrebbe essere ripristinato.

Infine, è stata identificata una terza casistica in cui è posta correttamente in essere l'autenticazione del pagatore ma non vi è l'intenzione del medesimo a completare la transazione e, pertanto, in tali casistiche, non potendo essere considerata l'operazione di pagamento né come autorizzata né come non autorizzata, è stata ipotizzata la possibilità di ripartire la perdita tra il prestatore di servizi di pagamento e l'utente vittima di frode.

In conclusione, alla luce di quanto sopra rappresentato, in una prospettiva futura potranno essere considerate come operazioni di pagamento autorizzate solo quelle che l'utente ha effettivamente autorizzato con cognizione di causa.

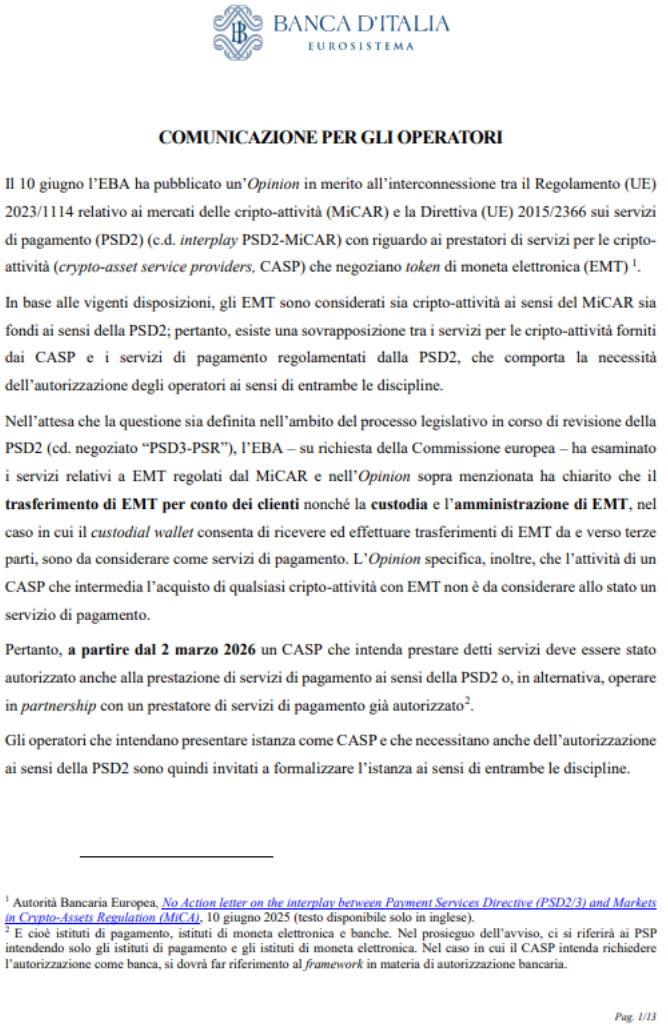
Innovazione, sostenibilità e stabilità del sistema finanziario

Banca d'Italia e il necessario coordinamento con MiCAR

Nella comunicazione di ottobre 2024, Banca d'Italia ha sottolineato la necessità di coordinare l'attività di revisione della PSD2 con il Regolamento (UE) 2023/1114 relativo ai mercati delle cripto-attività ("MiCAR"). In particolare, tale necessità di coordinamento tra le due discipline emerge dalla possibilità che le categorie di strumenti (token di moneta elettronica, token collegati ad attività, altre criptoattività) disciplinati dal MiCAR potrebbero, alla luce di una valutazione caso per caso, risultare idonei ad assolvere una funzione di pagamento.

Con particolare riferimento ai token di moneta elettronica ("EMT"), tali token sono considerati l'equivalente tokenizzato della moneta elettronica e, pertanto, gli stessi sono ricompresi sia nella nozione di cripto-attività, che in quella di moneta elettronica e fondi (anche ai sensi di PSD3/PSR e TFR), ciò in considerazione dell'utilizzabilità di tali token come mezzo di scambio con finalità di pagamento. Alla luce di ciò, la stessa Autorità segnala la possibile equivalenza tra i servizi "connessi al trasferimento" di EMT (previsti dal MiCAR) e i servizi di pagamento "tradizionali" in quanto le caratteristiche tipiche dei servizi connessi al trasferimento di token moneta elettronica potrebbero far rientrare questi ultimi all'interno dei servizi di moneta elettronica di cui alla PSD2.

Tuttavia, in tale prospettiva si pone la questione dell'applicabilità ai servizi di trasferimento di EMT – in alcuni casi equiparabili ai servizi di pagamento - delle disposizioni della PSD2, in particolare quelle riguardanti l'autenticazione forte del cliente, le operazioni non autorizzate ed i relativi riflessi sul regime di responsabilità delle parti.



BANCA D'ITALIA
EUROSISTEMA

COMUNICAZIONE PER GLI OPERATORI

Il 10 giugno l'EBA ha pubblicato un'*Opinion* in merito all'interconnessione tra il Regolamento (UE) 2023/1114 relativo ai mercati delle cripto-attività (MiCAR) e la Direttiva (UE) 2015/2366 sui servizi di pagamento (PSD2) (c.d. *interplay* PSD2-MiCAR) con riguardo ai prestatori di servizi per le cripto-attività (*crypto-asset service providers,* CASP) che negoziano *token* di moneta elettronica (EMT) [1].

In base alle vigenti disposizioni, gli EMT sono considerati sia cripto-attività ai sensi del MiCAR sia fondi ai sensi della PSD2; pertanto, esiste una sovrapposizione tra i servizi per le cripto-attività forniti dai CASP e i servizi di pagamento regolamentati dalla PSD2, che comporta la necessità dell'autorizzazione degli operatori ai sensi di entrambe le discipline.

Nell'attesa che la questione sia definita nell'ambito del processo legislativo in corso di revisione della PSD2 (cd. negoziato "PSD3-PSR"), l'EBA – su richiesta della Commissione europea – ha esaminato i servizi relativi a EMT regolati dal MiCAR e nell'*Opinion* sopra menzionata ha chiarito che il **trasferimento di EMT per conto dei clienti** nonché la **custodia** e l'**amministrazione di EMT**, nel caso in cui il *custodial wallet* consenta di ricevere ed effettuare trasferimenti di EMT da e verso terze parti, sono da considerare come servizi di pagamento. L'*Opinion* specifica, inoltre, che l'attività di un CASP che intermedia l'acquisto di qualsiasi cripto-attività con EMT non è da considerare allo stato un servizio di pagamento.

Pertanto, **a partire dal 2 marzo 2026** un CASP che intenda prestare detti servizi deve essere stato autorizzato anche alla prestazione di servizi di pagamento ai sensi della PSD2 o, in alternativa, operare in *partnership* con un prestatore di servizi di pagamento già autorizzato[2].

Gli operatori che intendano presentare istanza come CASP e che necessitano anche dell'autorizzazione ai sensi della PSD2 sono quindi invitati a formalizzare l'istanza ai sensi di entrambe le discipline.

---

[1] Autorità Bancaria Europea, *No Action letter on the interplay between Payment Services Directive (PSD2/3) and Markets in Crypto-Assets Regulation (MiCA)*, 10 giugno 2025 (testo disponibile solo in inglese).
[2] E cioè istituti di pagamento, istituti di moneta elettronica e banche. Nel prosieguo dell'avviso, ci si riferirà ai PSP intendendo solo gli istituti di pagamento e gli istituti di moneta elettronica. Nel caso in cui il CASP intenda richiedere l'autorizzazione come banca, si dovrà far riferimento al *framework* in materia di autorizzazione bancaria.

Pag. 1/13

Innovazione, sostenibilità e stabilità del sistema finanziario

Banca d'Italia e il necessario coordinamento con MiCAR (segue)

Inoltre, nella medesima Comunicazione di Banca d'Italia, si evince che, in considerazione del ruolo crescente delle imprese BigTech e Fintech nel settore dei pagamenti, è in fase di valutazione l'ampiamento del perimetro del pacchetto PSD3/PSR anche a soggetti quali i "fornitori di servizi tecnici" che, pur non propriamente e direttamente coinvolti nella prestazione di servizi di pagamento, risultano necessari alla prestazione di tali servizi.

Anche in tal caso, Banca d'Italia ha sottolineato la necessità di coordinare tale possibile estensione del perimetro applicativo con il Regolamento (UE) 2022/2554 relativo alla resilienza digitale per il settore finanziario, il c.d. DORA.

Infine, nonostante il pacchetto PSD3/PSR esclude esplicitamente i servizi di "cashin-shop" e "cashback" dal proprio campo di applicazione, l'esclusione dei servizi di "cash-in-shop" sarebbe garantita solo nel caso in cui vengano rispettate due specifiche condizioni:

(i) il servizio è offerto da un soggetto che vende beni e servizi a titolo di occupazione principale;
(ii) il prelievo massimo di contante è pari a Euro 50,00.

Tuttavia tale disciplina necessiterà di ulteriori chiarimenti e affinamenti al fine di garantire parità di trattamento ed evitare la concorrenza sleale tra gestori di ATM e dettaglianti che offrono servizi di cash-in-shop.

In tale prospettiva si innestano anche delle valutazioni circa la possibilità di estendere l'ambito di applicazione di tale framework normativo ai servizi di "Buy Now Pay Later" ("BNPL"), tuttavia la PSD3 riconosce che tali servizi hanno principalmente natura creditizia e che dunque non dovrebbero costituire un servizio di pagamento; pertanto, il servizio di BNPL sarebbe disciplinata dalla Consumer Credit Directive II ("CCD II").

Innovazione, sostenibilità e stabilità del sistema finanziario

Servizi “Open banking”

L'espressione “**open banking**” o “servizi bancari aperti” indica il processo attraverso il quale i prestatori di servizi di informazione sui conti (“Account Information Service Providers” o “AISP”) e i prestatori di servizi di disposizione di ordine di pagamento (“Payment Initiation Service Providers” o “PISP”), collettivamente noti come “prestatori terzi” o “terze parti”, erogano i servizi regolamentati dalla PSD2, mediante l'accesso, su richiesta degli utenti medesimi, ai dati dei loro conti detenuti presso i prestatori di servizi di pagamento di radicamento del conto (“Account Servicing Payment Service Providers” o “ASPSP”).

Sebbene i servizi open banking abbiano mostrato una tendenza in crescita nel corso degli ultimi anni, dalla valutazione della PSD2 sono, tuttavia, emerse alcune problematiche ricorrenti per quanto riguarda l'efficacia e l'efficienza dell'accesso da parte di prestatori terzi ai dati detenuti dagli ASPSP. Infatti, i prestatori terzi incontrano ancora notevoli ostacoli e riferiscono spesso che le interfacce progettate per agevolare il loro accesso ai dati variano in termini di qualità e prestazioni.

Da parte loro, gli ASPSP lamentano invece l’obbligo di sostenere costi di attuazione significativi per lo sviluppo delle interfacce di programmazione delle applicazioni (“application programming interface” o “API”) che, tuttavia, non sono legittimati ad addebitare, a loro volta, ai prestatori terzi. Peraltro, gli ASPSP si dichiarano prevalentemente insoddisfatti per il basso utilizzo delle loro API da parte dei prestatori terzi, i quali utilizzano in via preferenziale le interfacce cliente, anziché le API appositamente predisposte.

Innovazione, sostenibilità e stabilità del sistema finanziario

Servizi “Open banking”

In tale contesto, per la revisione della PSD2, la Commissione ha scelto di focalizzarsi su una serie di modifiche mirate a ottimizzare l'efficacia dei servizi open banking, evitando però di apportare cambiamenti radicali che potrebbero destabilizzare il mercato o generare costi di attuazione significativi. Nello specifico, le disposizioni in materia di servizi open banking contengono una serie di modifiche rispetto alla PSD2 e incorporano alcune disposizioni attualmente contenute nel Regolamento delegato (UE) 2018/389 della Commissione per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri.

In particolare, le modifiche principali prevedono l'obbligo, salvo casi eccezionali, di disporre di un'interfaccia dedicata per l'accesso ai dati e la soppressione, salvo in casi eccezionali ed espressamente autorizzati, dell'obbligo per gli ASPSP di mantenere permanentemente un'interfaccia c.d. “di riserva”.

Inoltre, al fine di consentire agli utenti di gestire comodamente le loro autorizzazioni rilasciate ai prestatori terzi per tali servizi, gli ASPSP sono tenuti a offrire un "pannello di gestione" che permetta di revocare l'accesso ai dati concesso a qualsiasi prestatore di servizi bancari aperti.

Infine, è prevista la soppressione del servizio specifico di conferma della disponibilità di fondi, previsto dall'articolo 65 della PSD2, come servizio open banking a sé stante, in ragione del fatto che pochissimi modelli di business sono stati sviluppati sulla base di questo specifico servizio, basandosi piuttosto sull'uso del sistema di identificazione automatica come alternativa per verificare la disponibilità di fondi.

Innovazione, sostenibilità e stabilità del sistema finanziario

Misure per garantire un level playing field tra operatori bancari e non bancari

Dall'entrata in vigore della PSD2, si è verificato un incremento, sia in termini numerici che di rilevanza, dei prestatori di servizi di pagamento non bancari. Nonostante essi siano in grado di fornire servizi di conto di pagamento, a differenza delle banche, non possono - tendenzialmente - concedere prestiti e devono garantire la sicurezza dei fondi dei clienti attraverso l'intermediazione di una banca.

L'art. 114-octies, del D.lgs 1° settem bre 1993, n. 385 ("TUB"), rubricato "Attività accessorie esercitabili", dispone che gli istituti di pagamento (e gli istituti di moneta elettronica, ai sensi del combinato dell'art. 114-quater, comma 3, lett. a) del TUB) possono esercitare, tra l'altro, anche l'attività di concessione di crediti in stretta relazione ai servizi di pagamento prestati e nei limiti e con le modalità stabilite dalla Banca d'Italia. Nello specifico, il finanziamento deve essere concesso nel rispetto delle seguenti condizioni:

(i) il finanziamento deve essere accessorio e concesso esclusivamente in relazione all'esecuzione di un'operazione di pagamento;
(ii) non deve essere superiore a dodici mesi;
(iii) non deve essere concesso utilizzando fondi ricevuti o detenuti ai fini dell'esecuzione di un'operazione di pagamento; e
(iv) l'istituto di pagamento dovrebbe dotarsi di una specifica dotazione minima di capitale pari al 6% dei finanziamenti erogati.

Inoltre, il processo per l'erogazione del credito deve comprendere le seguenti fasi: 1) istruttoria; 2) erogazione; 3) monitoraggio delle posizioni; 4) interventi in caso di anomalia; 5) revisione delle linee di credito.

Per poter offrire servizi di pagamento, è indispensabile avere accesso alle principali infrastrutture di pagamento che gestiscono e regolamentano le transazioni finanziarie.

Innovazione, sostenibilità e stabilità del sistema finanziario

Misure per garantire un level playing field tra operatori bancari e non bancari

In relazione all'accesso ai conti bancari da parte degli istituti, è opportuno sottolineare che, sebbene il secondo paragrafo dell'articolo 36 della PSD2 imponga agli enti creditizi di fornire una motivazione adeguata all'autorità di vigilanza competente in caso di rifiuto di concedere l'accesso ai conti di pagamento essenziali per la prestazione dei servizi di pagamento, si è notato che diverse banche non rispettano pienamente tali obblighi normativi.

Alcune di esse forniscono spiegazioni insufficientemente dettagliate o addirittura adottano prassi che comportano inizialmente l'accesso ai conti bancari, per poi revocarlo senza fornire alcuna spiegazione. Questo tipo di comportamento può avere gravi conseguenze sulle attività degli IP e degli IMEL, minando la stabilità e l'efficienza delle loro operazioni.

Inoltre, la Direttiva 98/26/CE, del 19 maggio 1998, concernente il carattere definitivo del regolamento nei sistemi di pagamento e nei sistemi di regolamento titoli, attualmente costituisce un ostacolo all'accesso alle infrastrutture di pagamento da parte dei prestatori di servizi di pagamento non bancari, in quanto non li contempla come possibili partecipanti. Ciò costringe gli IP e gli IMEL a fare ancora più affidamento sulle banche, non solo per la salvaguardia dei fondi dei clienti, ma anche per l'esecuzione dei pagamenti, creando una evidente dipendenza strutturale dalle banche.

Innovazione, sostenibilità e stabilità del sistema finanziario

Misure per garantire un level playing field tra operatori bancari e non bancari

La proposta della Commissione di revisione della PSD2 contiene pertanto misure volte a porre rimedio a tali carenze e a migliorare la parità di condizioni. Le prescrizioni imposte alle banche per quanto riguarda i servizi di conto bancario a prestatori di servizi di pagamento non bancari saranno inasprite, imponendo un obbligo più severo di spiegare il motivo dell'eventuale rifiuto e includendo tra le fattispecie soggette all'obbligo di spiegazione anche l'eventuale revoca del servizio.

Tale giustificazione potrebbe essere rappresentata, ad esempio, da violazioni della legge da parte del prestatore di servizi di pagamento.
In particolare, le relative motivazioni dovrebbero includere, tra le altre, fondato sospetto di attività illegali e di riciclaggio di denaro.

Infine, le banche centrali potrebbero, a propria discrezione, offrire servizi di custodia dei fondi detenuti dai prestatori di servizi di pagamento non bancari, fornendo così una eventuale soluzione di ripiego nel caso in cui dovessero non dovessero riuscire ad ottenere l'apertura di un conto presso una banca.

La Commissione propone, inoltre, di modificare la direttiva "concernente il carattere definitivo del regolamento" al fine di includere i prestatori di servizi di pagamento non bancari come possibili partecipanti a sistemi di pagamento designati. La nuova disciplina così modificata comprenderà norme rafforzate sull'ammissione degli IP come partecipanti ai sistemi di pagamento, con un'adeguata valutazione del rischio.

Agenda

- Innovazione, sostenibilità e stabilità del sistema finanziario
- **Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento**

Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

La sicurezza come elemento da rafforzare

La trasformazione digitale impone maggiori presidi di sicurezza a fronte di un'impennata nelle frodi. Spesso è il cliente l'obiettivo delle strategie di attacco da parte di soggetti malevoli. Non a caso, il 99% delle frodi effettive riguarda operazioni autorizzate dal cliente stesso e il 76% delle frodi effettive nasce da manipolazioni finalizzate a indurre il pagatore a disporre personalmente l'operazione.

Il contatto iniziale avviene nel 60% dei casi attraverso telefonate o Sms, ma stanno emergendo con forza anche i social media e le App di messaggistica come nuovi vettori di attacco. Le banche stanno reagendo con un duplice approccio:

- da un lato rafforzano la prossimità al cliente con campagne strutturate di sensibilizzazione e percorsi di educazione finanziaria, strumenti indispensabili per accrescere la consapevolezza e la capacità di difesa;
- dall'altro si dotano di tecnologie avanzate di monitoraggio e rilevazione.

Oggi il 96% delle banche presidia la rete per identificare siti contraffatti, il 92% monitora transazioni anomale da Internet Banking, l'88% utilizza strumenti di threat intelligence e l'84% rileva anomalie sulle transazioni da mobile.

È in corso anche una trasformazione operativa che si riflette sui processi operativi. La digitalizzazione ha ormai ridotto fortemente la componente cartacea: il 96% dei bonifici è online, l'85% delle deleghe per il pagamento dei tributi è digitale e il 95% degli effetti/documenti è dematerializzato.

Questo scenario non riguarda solo il mondo della clientela retail, basti pensare alla gestione della tesoreria per conto delle Pubbliche Amministrazioni, dove l'86% degli Enti è oggi servito con procedure telematiche.

Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

La sicurezza come elemento da rafforzare (segue)

Rafforzare la protezione degli utenti e il contrasto alle frodi, migliorare e semplificare i servizi di open banking, e garantire una maggiore armonizzazione con altre normative correlate, come il Gdpr e Micar (in particolare per gli e-money token con funzioni di pagamento). Questi gli obiettivi della nuova versione della direttiva sui servizi di pagamento (Psd), che sta raggiungendo le fasi conclusive dell'iter legislativo.

La revisione si articola in due testi distinti:

- una direttiva (Psd3), che riguarda le norme sull'autorizzazione per chi può erogare servizi di pagamento,
- un regolamento (Psr) che disciplina diritti e obblighi sia dei prestatori sia degli utenti di servizi di pagamento.

PSD3 entrerà in vigore dopo pubblicazione in GUUE; gli Stati membri avranno tipicamente 18–24 mesi per il recepimento.

Le disposizioni “di mercato” del PSR diventeranno applicabili dopo un periodo transitorio (di norma ~18 mesi dall’entrata in vigore).

Gli IMEL avranno una finestra di transizione per migrare al regime PSD3; le autorizzazioni PSD2/EMD2 esistenti saranno riallineate.

Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

La situazione attuale

Attualmente i testi dei colegislatori europei si trovano nella fase di trilogo. Sebbene la Psd2 abbia introdotto con successo la doppia autenticazione (Sca), riducendo sensibilmente le frodi online, i frodatori hanno trovato nuove vie. Secondo il recente Rapporto della Banca d'Italia sulle operazioni di pagamento fraudolente in Italia II semestre 2024, un numero crescente di operazioni fraudolente sono in realtà operazioni perfettamente autorizzate con la Sca correttamente eseguita, ma in cui il pagatore è stato raggirato, manipolato. Per affrontare questo fenomeno, le nuove norme mirano a mobilitare tutti gli attori coinvolti nell'effettuazione dei pagamenti per aggredire le frodi in fase preventiva.

In pratica il legislatore sta cercando un punto di equilibrio tra la responsabilità dei vari attori della catena di pagamento, ampliando quella dei prestatori di servizi di pagamento, ma anche responsabilizzando l'utente e coinvolgendo gli operatori di telefonia e i gestori delle piattaforme online.

Il settore bancario sostiene che le banche dovrebbero essere responsabili solo di ciò che è sotto il loro controllo, dato che molte frodi nascono in ambienti esterni alla banca.

Un elemento di grande importanza, ancora in discussione ma fondamentale, è la possibilità di sospendere un'operazione in presenza di un sospetto di frode. Questo è cruciale anche considerando la crescente diffusione dei pagamenti istantanei. Per potenziare la prevenzione, inoltre, la Psr prevede lo scambio informativo tra le banche, operazione essenziale che deve essere conciliata con gli obblighi di protezione dei dati personali, come è considerato anche l'Iban.

Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

Overview e Contesto

Nell'ambito delle innovazioni normative sulla finanza digitale, è stato introdotto il Digital Financial Package, che mira a regolamentare una serie di aspetti. All'interno di questo pacchetto normativo, è incluso il Payments Package, che comprende ulteriori proposte legislative riguardanti la protezione dei dati e la sicurezza nei pagamenti. In particolare, il Payments Package include le proposte di Payment Services Directive 3 e Payment Services Regulation relative ai pagamenti digitali.

Digital Financial Package
Comprende una strategia per la finanza digitale, proposte legislative sui cripto-asset e sulla resilienza digitale e una strategia per i pagamenti retail

Payment Package
Incluso nel Digital Financial Package, prevede proposte legislative e iniziative strategiche volte a promuovere innovazione, concorrenza, user experience, protezione dati e sicurezza nei pagamenti.

Payment Services Directive 3
Evoluzione della PSD2, progettata per rispondere alle esigenze di un mercato dei pagamenti. L'obiettivo della PSD3 è rafforzare la sicurezza dei pagamenti elettronici e migliorare la protezione dei consumatori, introducendo norme più rigorose per l'accesso ai dati di pagamento, la gestione delle frodi e la trasparenza dei servizi finanziari digitali.

Payment Services Regulation
Quadro normativo per il settore dei pagamenti, direttamente applicabile in ciascuno Stato membro.
L'obiettivo del PSR è stabilire norme che regolino i servizi di pagamento nel mercato europeo, garantendo la protezione dei consumatori, la sicurezza delle transazioni e la concorrenza leale tra i fornitori di servizi di pagamento.

Si applicano a:

- Fornitori di servizi di pagamento
- Banche
- Ist. Pagamento
- IMEL
- Società di carte di credito e debito
- Fornitori di servizi di pagamento online
- Digital Wallet «Staged»
- Servizi di trasferimento di denaro
- Gateway di pagamento

Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

I limiti della precedente normativa

PSD2 utilizzava un approccio monolitico - una sola direttiva onnicomprensiva che lasciava ampi margini di interpretazione nazionale. Questo ha generato:

- ❑ 27 implementazioni diverse nell'UE
- ❑ costi di compliance moltiplicati per operatori cross-border
- ❑ incertezza giuridica per le fintech paneuropee.

La PSD2 aveva creato le fondamenta per un mercato dei pagamenti più competitivo e innovativo, ma l'applicazione pratica ha rivelato:
- Frammentazione interpretativa: ogni Stato membro ha implementato le disposizioni con sfumature nazionali;
- Limiti tecnologici: le API previste si sono rivelate eterogenee e spesso inadeguate;
- Protezione insufficiente: l'esplosione delle frodi APP ha dimostrato lacune nella tutela dei consumatori.

PSD3+PSR introducono invece una struttura biforcata dove:
- La **Direttiva** gestisce gli aspetti che richiedono flessibilità nazionale (licensing, supervisione, sanzioni)
- Il **Regolamento** impone standard tecnici uniformi (API, sicurezza, reporting)

Questa architettura riflette la maturazione del mercato: non più solo principi da interpretare, ma regole precise da applicare uniformemente.

Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

Principali novità introdotte dalla PSD3

Per affrontare i limiti e risolvere i principali problemi rimasti irrisolti con la PSD2, riguardanti la sicurezza dei pagamenti, le frodi, la concorrenza tra entità bancarie e non, l'open banking e la disponibilità di contante, il Regolatore ha ritenuto opportuno revisionare il testo della PSD2, introducendo una nuova versione della Direttiva.

Autorizzazioni

Sono introdotte nuove procedure di autorizzazione per gli IP che includono:

- una valutazione della Governance e meccanismi interni di controllo;
- la definizione degli accordi relativi ai servizi ICT;
- l'obbligo di presentare un piano di liquidazione in caso di dissesto.

Anche per enti già autorizzati, una nuova autorizzazione è da richiedere entro 24 mesi dall'emissione della Direttiva

Servizi di fornitura del denaro contante

Gli Stati membri esentano dall'applicazione della Direttiva le persone fisiche o giuridiche che forniscono contante in negozi al dettaglio, se il servizio è offerto da chi vende beni o servizi come attività principale e l'importo non supera i 50 euro per prelievo.

Prelievo contanti da ATM

Le persone fisiche o giuridiche che offrono servizi di prelievo di contante senza gestire conti di pagamento o altri servizi di pagamento devono registrarsi presso l'autorità competente dello Stato membro di origine prima di iniziare l'attività, senza necessità di autorizzazione.

Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

Principali novità introdotte dalla PSD3

Per affrontare i limiti e risolvere i principali problemi rimasti irrisolti con la PSD2, riguardanti la sicurezza dei pagamenti, le frodi, la concorrenza tra entità bancarie e non, l'open banking e la disponibilità di contante, il Regolatore ha ritenuto opportuno revisionare il testo della PSD2, introducendo una nuova versione della Direttiva.

Moneta elettronica

La legislazione ha introdotto le categorie di moneta elettronica, che rappresenta un valore monetario memorizzato elettronicamente, e i servizi di moneta elettronica, che comprendono l'emissione, la gestione di conti e il trasferimento di moneta elettronica.

Distributori di servizi di moneta elettronica

Gli Stati membri consentiranno agli istituti di pagamento che forniscono servizi di moneta elettronica di distribuire e rimborsare la moneta elettronica attraverso distributori.

Requisiti in materia di tutela

Gli istituti di pagamento dovranno custodire i fondi dei propri utenti in conti separati di differenti istituti di credito, garantendo così un livello di protezione più elevato in caso di insolvenza.

Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

PSD3: RTS e Linee Guida attesi

Per **facilitare l'implementazione dei requisiti introdotti dalla PSD3**, la Direttiva prevede la pubblicazione di **Standard Tecnici di Regolamentazione** (RTS) e **Linee Guida**.

Questi strumenti offrono **indicazioni dettagliate** e **pratiche** per garantire una **corretta applicazione** della nuova Direttiva.

Gli **RTS** stabiliscono **requisiti tecnici specifici** che devono essere rispettati, mentre le **Linee Guida** forniscono **orientamenti e best practices** per aiutare gli Stati membri e le entità coinvolte a **conformarsi alle disposizioni della PSD3**.

Initial capital requirements

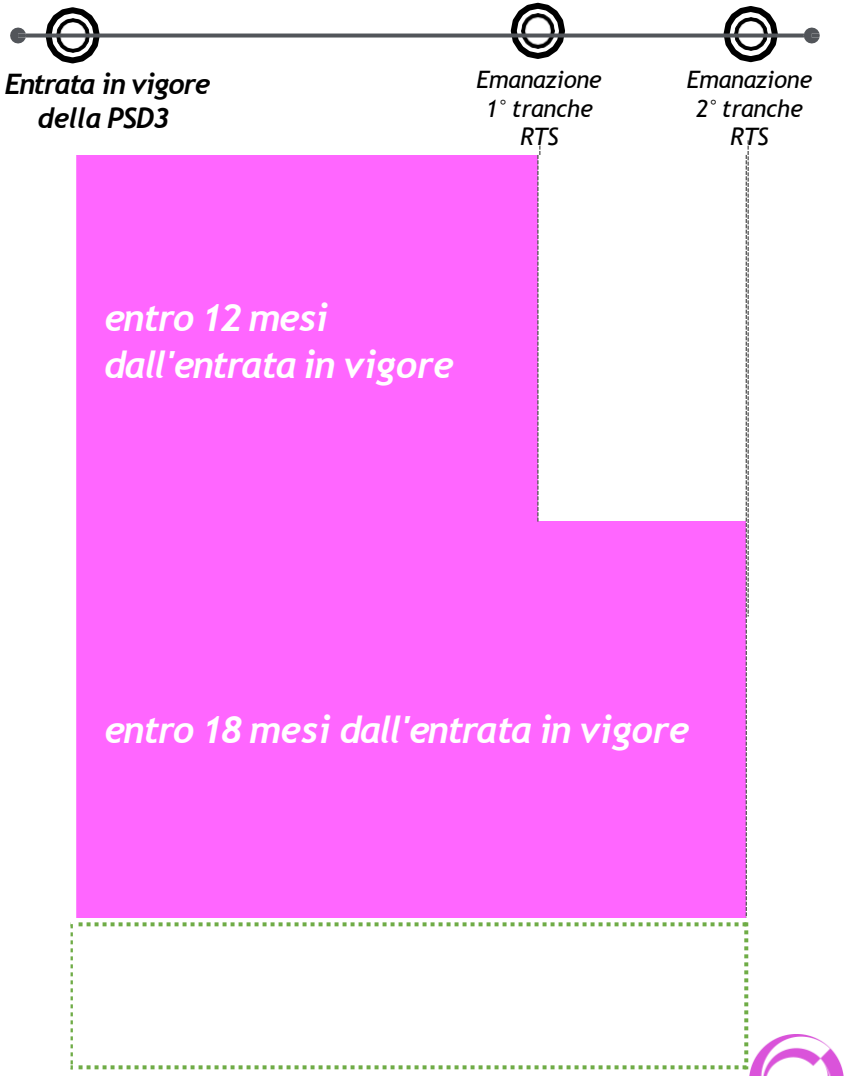
Activities	PSD3	PSD2 (EMD2)
Payment services	EUR 150,000	EUR 125,000
E-money services	EUR 400,000	EUR 350,000
Money remittance services	EUR 25,000	EUR 20,000
Payment initiation services	EUR 50,000 or professional indemnity insurance*	EUR 50,000
Account initiation services	EUR 50,000 or professional indemnity insurance*	None

La proposta PSD3 introduce l'opzione per i fornitori di servizi di avvio dei pagamenti (PISP) e i fornitori di servizi di informazione sui conti (AISP) di detenere un capitale iniziale anziché avere un'assicurazione di responsabilità professionale. Questa possibilità è stata introdotta per superare le difficoltà incontrate dai PI nell'ottenere un'assicurazione di responsabilità professionale nella fase di autorizzazione.

Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

PSD3: RTS e Linee Guida attesi

Ambito	Descrizione
Autorizzazione degli Istituti di pagamento	**RTS** contenenti le informazioni e requisiti per l'autorizzazione per diventare un istituto di pagamento, un prestatore di servizi di informazione sui conti o un operatore ATM.
Modelli di business	**RTS** contenenti i criteri per stabilire quando il modello operativo di un istituto di pagamento permette di effettuare solo un numero limitato di operazioni, caratterizzate però da un elevato valore individuale.
Requisiti di salvaguardia	**RTS** contenenti i quadri di gestione del rischio di salvaguardia per gli IP, finalizzato a garantire la protezione dei fondi degli utenti. Comprendono i requisiti di segregazione, designazione, riconciliazione e calcolo degli obblighi di salvaguardia dei fondi.
EBA Register	**RTS** contenenti le norme relative al funzionamento, alla manutenzione e alle modalità di accesso alle informazioni contenute nell'EBA Register.
Domanda di esercizio del diritto di stabilimento e di libera prestazione di servizi.	**RTS** contenenti il quadro per la cooperazione tra le autorità competenti dello Stato membro d'origine e dello Stato membro ospitante.
Vigilanza sugli istituti di pagamento che esercitano il diritto di stabilimento e di libera prestazione dei servizi.	**RTS** contenenti i criteri per determinare, in base al principio della proporzionalità, quando è necessaria la nomina di un punto di contatto centrale.
Rilascio dell'autorizzazione per IP per fornire servizi di pagamento e moneta elettronica	**Linee guida** contenenti le norme, procedure e meccanismi di autorizzazione per un istituto di pagamento che intende offrire servizi di pagamento e di moneta elettronica.



Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

Premessa

I testi della PSD3 non sono ancora definitivamente in vigore: contenuti e tempistiche potranno essere ritoccati fino alla pubblicazione in GUUE e al recepimento nazionale.

Natura	Direttiva che rifonde/aggiorna il quadro di autorizzazione e vigilanza dei prestatori di servizi di pagamento (PSP). Sposta in un regolamento separato (PSR) molte regole "di mercato" oggi in PSD2 (diritti/obblighi utenti e PSP, trasparenza, SCA, open banking
Obiettivi	Rafforzare l'assetto autorizzativo/prudenziale e di supervisione dei PSP, unificando il regime della moneta elettronica (EMD2) con quello degli istituti di pagamento, e colmando lacune emerse con PSD2.

Cosa Resta in PSD3

- ❑ Autorizzazione, requisiti di ammissione ed esercizio per: istituti di pagamento (IP) e istituti di moneta elettronica (IMEL).
- ❑ Requisiti prudenziali (capitale iniziale, fondi propri, fixed overhead), salvaguardia fondi clienti, governance e controlli interni, uso di agenti/filiali/distributori, outsourcing, partecipazioni qualificate, passaporto e vigilanza.
- ❑ Regole e cooperazione tra autorità, sanzioni e misure di enforcement, disposizioni transitorie (migrazione EMD2 → PSD3).

Cosa passa in PSR

- ❑ Diritti/obblighi nei pagamenti (trasparenza, contestazioni e rimborsi),
- ❑ SCA/CSC (Common and Secure Communication),
- ❑ accesso ai conti (open banking XS2A),
- ❑ requisiti anti frodi (name check, scambio info),
- ❑ condotta e protezione utenti,
- ❑ accesso ai sistemi di pagamento e ai conti di servizio.

Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

Contenuti di PSD3 in chiave analitica (e confronto con PSD2)

Perimetro soggettivo e definizioni	Cosa introduce PSD3: ▪ Unifica il regime di istituti di pagamento (IP) e moneta elettronica (IMEL) sotto un unico quadro autorizzativo e prudenziale. Riduce asimmetrie storiche tra PSD2 ed EMD2. ▪ Rivede e chiarisce esenzioni (limited network, operatori di telecomunicazioni, fornitori puramente tecnici) per contrastare usi estensivi/abusivi emersi con PSD2. Differenza vs PSD2: ▪ In PSD2 gli IMEL erano disciplinati da EMD2 con prassi divergenti fra Stati; PSD3 punta a un'armonizzazione maggiore (licenze, salvaguardia, vigilanza).
Autorizzaz., passaporto e vigilanza	Cosa introduce PSD3: ▪ Dossier autorizzativo più robusto: programma di attività, modello di business, assetto ICT e piani DORA ready, funzioni chiave (risk, compliance, audit) con requisiti di indipendenza e risorse, politiche AML/CFT, safeguarding e outsourcing register. ▪ Fit & proper per organi e funzioni chiave rafforzato; controllo su partecipazioni qualificate (acquisizione/cessione) più stringente. ▪ Regole più nette su uso di agenti e distributori (responsabilità del PSP, requisiti di onboarding, formazione, monitoraggio, eventuali contact point nazionali). ▪ Cooperazione home host e poteri del Paese ospitante sulle condotte locali; basi per sanzioni armonizzate. Differenza vs PSD2: ▪ PSD2 prevedeva requisiti ma con forte eterogeneità applicativa (es. controllo reti di agenti, qualità dei presidi ICT). PSD3 innalza l'asticella e rende più omogenei i criteri di vigilanza.

Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

Contenuti di PSD3 in chiave analitica (e confronto con PSD2)

Requisiti prudenziali e fondi propri	Cosa introduce PSD3: ▪ Aggiorna il capitale iniziale per tipologie di servizio e raffina i metodi di calcolo dei fondi propri (incl. fixed overhead requirement), con maggiore attenzione alla proporzionalità e alla sostenibilità del modello. ▪ Migliora l'inquadramento di test interni (ICAAP "light"), gestione concentrazioni, liquidità e rischio di controparte Differenza vs PSD2: ▪ Sotto PSD2 il calcolo dei requisiti presentava divergenze interpretative; PSD3 tende a chiarire basi e soglie, anche per la convergenza IP IMEL.
Salvaguardia dei fondi della clientela	Cosa introduce PSD3: ▪ Chiarisce i meccanismi di segregazione (conti dedicati, garanzie/assicurazioni equivalenti), frequenza delle riconciliazioni e gestione dei tempi di accreditamento; ribadisce l'"insolvency remoteness" (fondi fuori dalla massa in caso d'insolvenza del PSP). ▪ Più presidi su dove e come sono detenuti i conti di salvaguardia, verifiche periodiche e accountability del management Differenza vs PSD2: ▪ PSD2 conteneva principi, ma la pratica è stata disomogenea (contabilità, tempi di segregazione, escrow). PSD3 tende a ridurre le aree grigie e a rendere verificabili i presidi.

Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

Contenuti di PSD3 in chiave analitica (e confronto con PSD2)

Governance, controlli e outsourcing (incl. ICT/cloud)	Cosa introduce PSD3: ▪ Allineamento strutturale a DORA: registro outsourcing, clausole minime contrattuali (accesso/ispezione, sub outsourcing, data location, incident reporting, exit/portabilità), governance delle terze parti "critiche". ▪ Ruoli di risk/compliance/audit con maggiore indipendenza, reporting e piani di formazione; politiche di remunerazione coerenti con una sana gestione del rischio. Differenza vs PSD2: ▪ Con PSD2 la disciplina era meno specifica su outsourcing ICT/cloud; PSD3 (+ DORA) porta requisiti sostanzialmente più dettagliati e auditabili.
Reti di agenti, distributori e "hybrid entities"	Cosa introduce PSD3: ▪ Standard minimi per onboarding, formazione e monitoraggio degli agenti; responsabilità piena del PSP per condotte della rete; trasparenza dei punti di contatto; controllo su attività non payment di entità ibride per proteggere i fondi clienti. Differenza vs PSD2: ▪ La gestione degli agenti era fonte frequente di rilievi (qualità KYC, condotte). PSD3 alza l'asticella e rende più chiara la catena delle responsabilità.
Accesso ai sistemi di pagamento e ai conti (bank account access)	Cosa introduce PSD3: ▪ Rafforza il principio di accesso non discriminatorio per IP/IMEL ai sistemi di pagamento e ai conti presso enti creditizi, contrastando il "de risking" generalizzato. Richiede criteri oggettivi per rifiuti/chiusure e una governance documentata di tali decisioni. Differenza vs PSD2: ▪ In PSD2 il principio c'era, ma l'enforcement era debole. PSD3 spinge su motivazioni, tracciabilità e possibilità di sindacato da parte delle autorità.

Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

Contenuti di PSD3 in chiave analitica (e confronto con PSD2)

Enforcement, sanzioni e cooperazione	Cosa introduce PSD3: ▪ Poteri di ispezione e di intervento delle NCA più armonizzati; cornice sanzionatoria minima comune; scambi informativi strutturati tra NCA, BCE/SEBC, EBA e autorità AML; attenzione a “letter box entities”. Differenza vs PSD2: ▪ Maggiore convergenza e prevedibilità nell’azione di vigilanza; meno margini per arbitraggi regolatori.

Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

Impatti del passaggio da PSD2 a PSD3

Attività da svolgere in vista del passaggio alla PSD3	Licenze e status: ▪ IMEL: migrazione a regime PSD3 con requisiti più allineati agli IP; possibile revisione delle autorizzazioni esistenti. ▪ IP: verifica di continuità su requisiti patrimoniali e governance; potenziali aggiornamenti documentali per autorizzazioni/passaporto. Safeguarding e contabilità: ▪ Riconciliazioni più serrate, prove di segregazione e controlli su conti/garanzie; maggiore "auditability". Outsourcing/ICT (insieme a DORA): ▪ Contratti da aggiornare; registro outsourcing e mappatura terze parti critiche; piani di exit e test; integrazione con incident management DORA. Reti e distribuzione: ▪ Onboarding/monitoraggio agenti più rigorosi; responsabilità esplicita su training e condotte; rischi sanzionatori più tangibili. Accesso ai conti/sistemi: ▪ Maggiore possibilità di far valere il diritto di accesso; onere di prova su rifiuti/chiusure spostato sul fornitore del conto/sistema.
Invariati nella filosofia di fondo	➢ Centralità del modello basato su licenza e passaporto UE per PSP non bancari. ➢ Proporzionalità: requisiti graduati per dimensione/profilo; spazio a piccoli operatori pur con presidi minimi più chiari. ➢ Coordinamento strettissimo con AML/CFT: i presidi antiriciclaggio restano cardine del modello autorizzativo e operativo.

Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

La Rivoluzione della Strong Customer Autentication

La SCA in PSD2 era concepita come un baluardo contro le frodi ma si è trasformata in un ostacolo all'user experience. I tassi di abbandono del carrello sono aumentati fino al 30% in alcuni settori. La PSD3 ridefinisce completamente l'approccio:

Behavioral Authenticat. come IV Fattore	Non più solo "qualcosa che sai, hai o sei", ma anche "come ti comporti". Questo permette: - Autenticazione invisibile basata su pattern comportamentali - Riduzione drastica del friction per utenti legittimi - Identificazione più efficace di comportamenti anomali
Delegated Authenticat.	La possibilità di delegare la SCA a terze parti fidate (es. wallet provider, merchant di fiducia) crea un ecosistema di fiducia distribuita dove: - L'utente si autentica una volta e può operare un numero multiplo di volte - I merchant possono offrire experience seamless - I liability shift sono chiari e predefiniti

Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

Le Esenzioni: Da Eccezione a Regola Intelligente

Mentre PSD2 vedeva le esenzioni come deroghe eccezionali, PSD3 le integra come parte di un risk management dinamico:

Transaction Risk Analysis Potenziata	- Machine learning obbligatorio per PSP sopra certe soglie - Condivisione dati fraud in tempo reale tra PSP - Esenzioni dinamiche basate su risk scoring real-time
Nuove Categorie di Esenzione	Corporate payments: si riconosce che i flussi B2B transitano spesso su canali chiusi e controllati (host-to-host, EBICS, SWIFT, API dedicate, portali treasury) con controlli di sicurezza equivalenti alla SCA. L'Account Service Payment Provider può non richiedere SCA se il pagamento è disposto tramite un processo/protocollo aziendale "sicuro" e certificato, che: ➢ è riservato a clientela non consumer (società/enti), ➢ usa autenticazioni forti equivalenti (certificati client/mTLS, token HSM, chiavi EBICS, firma digitale server-to-server), ➢ è incardinato in controlli organizzativi B2B (entitlements, segregazione ruoli, four-eyes, log/audit).
Subscription evolution	Il pagatore presta consenso una tantum con SCA alla creazione di un mandato che definisce: ▪ beneficiario, conto addebitato, durata/validità, ▪ limiti: cap per singola operazione e/o per periodo, frequenza massima. I singoli addebiti successivi, effettuati dal beneficiario (merchant-initiated) entro i parametri del mandato, non richiedono nuova SCA; restano soggetti a monitoraggio e diritti di revoca/disputa.
Trusted merchant programs	Un'evoluzione combinata di tre leve esistenti sotto PSD2: "trusted beneficiaries" (lista beneficiari fidati), esenzione TRA (transaction risk analysis, soglie basate su tasso frodi) e "delegated authentication". L'idea è istituzionalizzare programmi in cui merchant/acquirer certificati, con performance di rischio comprovate e controlli di sicurezza elevati, possono beneficiare di percorsi frizionless più ampi.

Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

Il Nuovo Framework di Protezione

Il rimborso non è un «diritto assoluto» del cliente, diventa un obbligo del PSP quando ricorrono determinate condizioni:

Comportam. della vittima ragionevole	Il rimborso diventa un obbligo del PSP quando ricorrono determinate condizioni che qualificano il comportamento della vittima come "ragionevole" (secondo standard EBA oggettivi). In concreto: ➢ non ha condiviso credenziali/OTP/PIN con terzi, né ha consegnato il dispositivo a sconosciuti; ➢ ha letto e considerato i warning mostrati dal PSP (es. "IBAN-Nome non coincidono", "attenzione: rischio truffa/impersonation") e non li ha ignorati sistematicamente; ➢ non ha disattivato/aggirato misure di sicurezza (MFA, biometria, limiti) e non ha installato app di controllo remoto su richiesta di sedicenti operatori; ➢ ha usato canali ufficiali e ha segnalato senza indugio il sospetto di frode appena resosi conto dell'errore.
Implement. di warning system adeguati da parte del PSP	Il PSP deve dimostrare di aver messo in campo misure preventive efficaci (se mancano o sono inadeguate, il rimborso è dovuto di default): ➢ Verifica IBAN-Nome (confirmation of payee) con messaggi chiari e ben visibili in caso di mismatch, prima della conferma del pagamento. ➢ Avvisi specifici per pattern di rischio (importo/frequenza anomali, nuovi beneficiari, geografie a rischio, transazioni fuori abitudini) con spiegazioni comprensibili e call-to-action ("verifica direttamente col beneficiario", "contatta la banca"). ➢ Meccanismi di "attrito" sui pagamenti ad alto rischio: doppia conferma, cooling-off, blocco temporaneo e sblocco mediato da canali sicuri. ➢ Logging completo: prova che l'avviso è stato mostrato, quando, con quale testo, e quale scelta ha compiuto l'utente.

Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

Il Nuovo Framework di Protezione

il rimborso non è un «diritto assoluto» del cliente, diventa un obbligo del PSP quando ricorrono determinate condizioni:

Assenza di colpa grave	Il cliente mantiene il diritto al rimborso salvo che abbia agito con colpa grave o dolo. Spetta al PSP dimostrare la colpa grave del cliente, portando evidenze oggettive (log, warning ignorati, condotte vietate). Esempi indicativi: ➢ Probabile colpa grave: consegna deliberata di OTP a un "finto operatore" dopo warning espliciti; installazione di app di controllo remoto nonostante avvisi; ripetuto override di name-check mismatch e warning antifrode in brevi minuti; ritardi ingiustificati nella segnalazione che aggravano la perdita. ➢ Tipicamente non colpa grave: truffe particolarmente sofisticate (spoofing del numero della banca, deepfake voce), con assenza di warning efficaci; un singolo override in un contesto non palesemente anomalo; condotte conformi alle istruzioni del PSP; segnalazione tempestiva.

Per negare il rimborso, il PSP deve poter dimostrare insieme:

- di aver fornito warning adeguati (condizione 2),
- e che l'utente, nonostante ciò, ha agito con colpa grave o fuori dallo standard "ragionevole" (condizioni 1 e 3).

Se il PSP non prova l'una o l'altra (warning carenti; assenza di colpa grave provata), scatta l'obbligo di rimborso.

Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

Il Nuovo Framework di Protezione

Liability sharing 50-50	Si parla di frodi "authorised push payment" (APP), cioè bonifici autorizzati dall'utente ma indotto in errore (impersonation, invoice fraud, social engineering). L'obiettivo è quello di ridurre perdite e frodi incentivando sia il PSP mittente (sending) sia il PSP del beneficiario (receiving) a prevenire, intercettare e cooperare ex-ante ed ex-post. Regola base: quando scatta l'obbligo di rimborso APP (ferme le condizioni: comportamento "ragionevole" del cliente, warning adeguati, assenza di colpa grave), il costo netto è ripartito di default al 50% tra sending PSP e receiving PSP: il sending PSP rimborsa il cliente entro i termini di legge e poi "recupera" il 50% dal receiving PSP tramite regole di schema/clearing (chargeback/inter-PSP claim) oppure la piattaforma di dispute. Il riparto può essere "dinamico" in base a condotte/adempimenti (vedi sotto), ma la baseline è 50-50.

La divisione paritaria tra sending e receiving PSP crea incentivi per:

- Receiving PSP a fare KYC più stringenti;
- Sending PSP a implementare warning migliori;
- Collaborazione nel fraud detection.

Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

Il Nuovo Framework di Protezione

Il cd "Timeline Accelerate" nel pacchetto PSD3/PSR, riferito alla gestione delle frodi "authorised push payment" (APP) e, più in generale, delle contestazioni su operazioni di pagamento, consiste nel sostituire formule elastiche tipo "senza indebito ritardo" con SLA numerici stringenti, così da proteggere l'utente e creare pressione operativa sui PSP.

- **24 ore per il primo feedback (prima: indefinito)**: entro 24 ore dal reclamo/contestazione, il PSP del pagatore deve confermare al cliente la presa in carico ("acknowledgement"), assegnare un ID pratica e comunicare i prossimi passi e le misure cautelative adottate (es. richiesta di recall fondi, blocco prevenzionale su pagamenti simili, canale di contatto dedicato). In questo modo si eliminano le "zone grigie" sul quando il caso è stato aperto, si fanno partire i clock interni e si favorisce la cooperazione con il PSP del beneficiario. Nota operativa: l'ack è 24/7 (automatizzabile), anche se il reclamo arriva fuori orario; fa fede la ricezione documentata (timestamp).

- **5 giorni per la decisione finale (prima: fino a 35)**. Entro 5 giorni il PSP deve chiudere l'istruttoria e comunicare un esito motivato (positivo/negativo/parziale) sulla base dei criteri previsti dal PSR/RTS EBA (ragionevolezza del cliente, warning adeguati mostrati, assenza di colpa grave, v. oltre). La PSD2 dava 15 giorni lavorativi per rispondere ai reclami, estendibili eccezionalmente a 35; qui la finestra viene compressa a 5 (giorni in via generale; la qualificazione "lavorativi vs. di calendario" sarà chiarita nei testi attuativi) per i casi APP/frodi rilevanti. Implicazioni: il PSP mittente non può "attendere" oltre per la mancanza di risposte dal PSP ricevente; deve decidere sui fatti ed eventualmente rimborsare, rivalendosi poi nella sede inter-PSP (liability sharing).

- **Rimborso immediato se l'esito è positivo (prima: entro il giorno successivo)**: se il caso è fondato, l'accredito al cliente deve essere eseguito nella stessa giornata in cui è stata assunta la decisione, con valuta che neutralizza il precedente addebito (stessa data di addebito o migliore, secondo le regole di valore). Tale previsione riduce l'esposizione finanziaria del cliente e allinea la prassi alle aspettative di "remedy" rapido per vittime di APP fraud.

Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

Accesso al contante

La PSD3 introduce per la prima volta obblighi sociali espliciti nel framework dei pagamenti. L'accesso al contante diventa un diritto garantito, alla luce del fatto che:

- il 13% degli adulti UE usa principalmente cash;
- le aree rurali perdono 5% di ATM all'anno;
- l'esclusione digitale colpisce 40+ milioni di cittadini nell'eurozona.

A fronte dell'obiettivo di far crescere i pagamenti digitali senza escludere chi dipende dal contante viene previsto quanto segue:

- **Cashback in negozio senza acquisto**. Più negozi potranno offrire "cash services" come canale aggiuntivo di prelievo, specie nei comuni senza filiali/ATM;
- **ATM "indipendenti"** (IAD) e trasparenza delle commissioni: riconosce e disciplina in modo uniforme i servizi di prelievo cash erogati da IAD come "servizi di pagamento"; introduce obblighi di informativa chiara e preventiva sull'eventuale surcharge applicato all'utente e sulle condizioni del prelievo; allinea i diritti di rimborso in caso di malfunzionamenti;
- **Versamenti/prelievi di contante tramite PSP non bancari e reti di agenti**: viene chiarito che istituti di pagamento e di moneta elettronica possono offrire servizi di cash-in/cash-out per i propri clienti, con regole omogenee di salvaguardia fondi, trasparenza e antiriciclaggio.

Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

Inclusione finanziaria

- **Accesso a conti bancari e sistemi di pagamento per PSP non bancari (anti de-risking):** obbligo delle banche di garantire accesso non discriminatorio ai conti di servizio (per salvaguardia fondi, operatività) e ai sistemi di pagamento a istituti di pagamento/e-money, con motivazioni scritte in caso di rifiuto/chiusura e possibilità di ricorso presso le autorità.

- **Salvaguardia fondi più sicura (anche presso banche centrali)**: consente ai PSP non bancari opzioni più sicure per la salvaguardia dei fondi dei clienti (es. possibilità di detenere fondi salvaguardati presso banche centrali, dove disponibile), riducendo il rischio percepito, rafforzando la fiducia e favorendo la sostenibilità e contenendo i costi.

- **Stop a discriminazioni IBAN e frizioni transfrontaliere**: rafforzamento del divieto di "IBAN discrimination" (rifiuto di IBAN esteri nell'area SEPA) e introduce strumenti pratici per l'allineamento tra nome beneficiario e IBAN (c.d. "match del beneficiario") per ridurre errori/frodi. In tal modo si facilita la mobilità dei consumatori e l'uso di conti "pan-UE", utili a lavoratori transfrontalieri e studenti.

- **Unificazione del perimetro "pagamenti" e "moneta elettronica"**: integrazione della normativa e-money dentro PSD3/PSR, livellando diritti/obblighi tra conti di pagamento e conti di moneta elettronica (informativa, rimborsi, sicurezza).

- **Miglior tutela consumatori nei pagamenti digitali**: rafforzamento dei diritti di rimborso in alcuni scenari di frode e di errore, maggiore trasparenza delle commissioni, requisiti più chiari per l'autenticazione forte, nell'ottica di favorire una maggior fiducia nei pagamenti digitali e ridurre la dipendenza "forzata" dal contante per motivi di sicurezza percepita.

Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

Principali novità introdotte dal PSR

Il Payment Services Regulation (PSR) è un regolamento UE, quindi direttamente applicabile in tutti gli Stati membri senza necessità di recepimento. È il "pilastro di condotta" del pacchetto: stabilisce regole su trasparenza, diritti/obblighi, sicurezza, accesso ai conti (open banking), antifrode.

E' complementare con PSD3. Quest'ultima (direttiva) si occupa soprattutto di licenze, vigilanza prudenziale e accesso alle infrastrutture da parte di banche e non-banche; la PSR disciplina l'operatività, le interazioni con gli utenti e gli standard tecnici (via RTS/ITS EBA).

La PSR prevede l'Integrazione dell'e-money: i diritti/obblighi per le operazioni con moneta elettronica vengono allineati a quelli dei servizi di pagamento "classici", superando la frammentazione tra PSD2 ed EMD2.

Ambito soggettivo	Banche, istituti di pagamento, istituti di moneta elettronica (EMI), AISP (account information), PISP (payment initiation), CBPII (Card-Based Payment Instrument Issuer). Questi ultimi sono emittenti di strumenti di pagamento basati su carte che, tramite l'API "Confirmation of Funds" (COF), possono verificare se un conto bancario contiene fondi sufficienti per una transazione, con il consenso esplicito del cliente.
Operazioni impattate	Bonifici (inclusi istantanei, regolati a parte quanto a obblighi di offerta), addebiti diretti SEPA, carte, rimesse, e money, servizi che si basano su accesso a conto.

Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

Principali novità introdotte dal PSR

Il Payment Services Regulation (PSR) è stato introdotto insieme alla PSD3 e stabilisce una serie di requisiti normativi che sono direttamente applicabili agli Stati membri dell'Unione Europea, senza la necessità di essere recepiti nelle legislazioni nazionali.

Dashboard per la gestione delle autorizzazioni

Obbligo per gli Account-Servicing Payment Service Provider (ASPSPs) di implementare una dashboard che permetta agli utenti di visualizzare e gestire i consensi concessi ai Third Party Providers (TPP), inclusi dettagli su accesso, dati condivisi e durata, con la possibilità di revocare l'accesso in tempo reale.

Interfacce d’accesso dedicate

Obbligo per gli Account-Servicing Payment Service Provider (ASPSPs) di fornire ai Third Party Providers (TPP), interfacce dedicate, prive di ostacoli, per l’accesso ai dati dei conti di pagamento.

Maggiore trasparenza e sicurezza

Obbligo per il beneficiario di informare il Payment Service Provider (PSP) dell'importo esatto subito dopo la consegna del servizio o bene.
Verifica gratuita del PSP del beneficiario sulla coerenza tra nome e identificativo unico prima della finalizzazione del pagamento.

Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

Principali novità introdotte dal PSR

Il Regolamento mira a uniformare e introdurre requisiti in materia di gestione delle autorizzazioni, interfacce d'accesso dedicate ai Third Party Providers per agevolare l'accesso ai dati dei conti, ulteriori strumenti per la Strong Customer Authentication. Infine, sono previste maggiori tutele per evitare le frodi, prevedendo nuove disposizioni sul monitoraggio dei dati e delle transazioni.

Frodi

- Nuove disposizioni su monitoraggio delle transazioni e condivisione dei dati, inclusa la condivisione delle statistiche sulle frodi con i regolatori.
- Maggiore responsabilità dei PSP, i quali dovranno prevenire e contrastare fenomeni come lo "spoofing", tramite misure preventive e collaborazioni con i gestori di reti mobili e piattaforme online.

Strong Customer Authentication (SCA)

- Nuove responsabilità dei fornitori tecnici e operatori di pagamento in caso di fallimento.
- Definizione di accordi di esternalizzazione per i servizi di SCA offerti.
- Nuovi requisiti per l'elemento di inerenza della SCA.

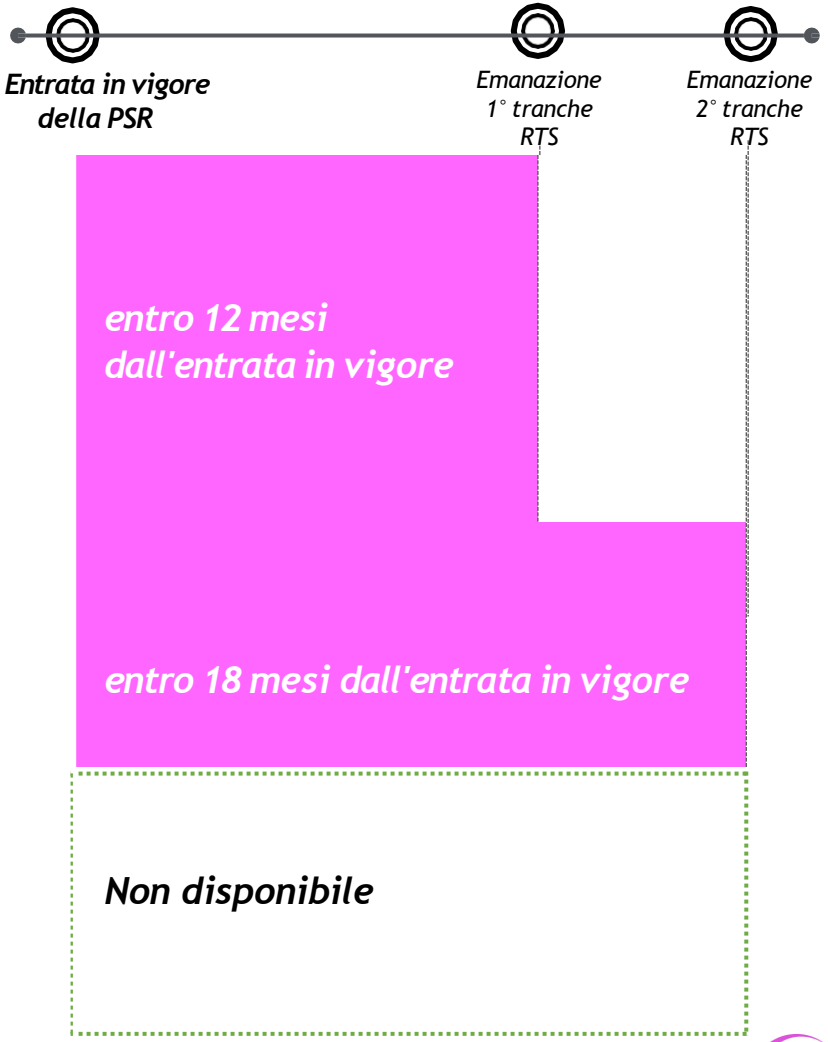
Gestione e monitoraggio dei dati

Possibilità per i Payment Service Provider (PSP) di condividere le informazioni relative alle frodi utili per il monitoraggio del rischio legato alle transazioni.

Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

PSR: RTS e Linee Guida attesi

Ambito	Descrizione
Esercizio per specifici strumenti di pagamento	RTS contenenti le condizioni specifiche per determinare le esenzioni relative ai servizi che utilizzano specifici strumenti di pagamento.
Fornitura da parte delle Banche di conti di pagamento per l'accesso ai Dati	RTS contenenti le norme che definiscono il formato standardizz e le informazioni da includere nella notifica e nella motivazione per il rifiuto di apertura o chiusura di un conto di pagamento.
Deroga all'obbligo di avere un'interfaccia dedicata per l'accesso ai Dati	RTS contenenti i criteri per esentare un prestatore di servizi di pagamento dall'obbligo di fornire un'interfaccia per le TPP.
Ruolo delle Autorità Competenti	RTS contenenti i criteri per stabilire i dati da fornire alle autorità competenti, nonché le modalità e la frequenza di invio.
Fraud reporting	RTS contenenti i criteri per determinare i dati statistici da fornire in merito agli obblighi di segnalaz. delle frodi di diversi mezzi di pagam.
Autenticazione, comunicazione e monitoraggio delle transazioni	RTS contenenti le norme relative ai requisiti, alle esenzioni, alle misure di sicurezza delle credenziali e all'esternalizzazione delle SCA; agli standard di comunicazione aperti e sicuri e ai meccanismi di controllo.
Esenzione per operaz di pagamento	GL contenenti le esenzioni specifiche per le operazioni di pagam effettuate dal pagatore al beneficiario tramite un agente.
Rischi e tendenze delle frodi nei pagamenti	GL contenenti le modalità e le tempistiche di comunicazione che i prestatori di servizi di pagamento devono adottare in merito ai rischi di frode nei pagamenti.
Autorità Competenti e poteri investigativi	GL contenenti le informazioni sulle procedure di reclamo, inclusi i canali per la presentazione di reclami, le informazioni richieste ai denuncianti e la pubblicazione delle analisi aggregate ai reclami.



Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

PSR – Trasparenza e Informativa

Il PSR prevede che le informazioni debbano essere chiare, in linguaggio comprensibile, disponibili su supporto durevole (anche digitale), fornite prima del contratto e durante il rapporto. Le informazioni devono dare anche evidenza di canali reclamo/Alternative Dispute Resolution (ADR).

Info da fornire prima della conclusione	▪ **Descrizione servizi e canali**: tipologie di operazioni (bonifici, addebiti, carte, e-money, AIS/PIS/CBPII), limiti di uso, orari di cut-off. ▪ **Costi e commissioni**: tariffario completo (fisso/percentuale; per canale; istantanei vs ordinari), eventuali fee di ATM "non proprietari", costi di carte, sostituzione, notifiche SMS, ecc. ▪ **Valute e tassi di cambio**: valuta/e di conto, tasso di riferimento usato (es. BCE), frequenza di aggiornamento, metodo di calcolo del mark-up/spread. ▪ **Tempi di esecuzione**: D+1 per bonifici elettronici intra-UE; policy per istantanei (prezzi e disponibilità). ▪ **SCA e sicurezza**: fattori usati, dynamic linking, esenzioni tipiche, canali alternativi se il dispositivo non è disponibile. ▪ **Reclami e ADR**: tempi di risposta (15 giorni lavorativi, 35 in casi eccezionali), organismi ADR competenti. ▪ **Dati personali**: finalità, basi giuridiche (incluso il trattamento dati anti-frode), retention, diritti GDPR. ▪ **Per Account Information Service (AIS)/ Payment Initiation Service (PIS)**: finalità, set minimo di dati, durata del consenso, come revocare da dashboard, contatti del TPP. ▪ **Modifiche unilaterali e recesso**: preavviso standard di 2 mesi per modifiche al framework contract, con diritto del cliente di recedere senza penali prima dell'entrata in vigore. ▪ **Forma**: documento riepilogativo chiaro (es. scheda di trasparenza + termini e condizioni). Accessibilità: linguaggio semplice, layout leggibile, opzioni per utenti con disabilità

Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

PSR – Trasparenza e Informativa

Trasparenza su costi e commissioni	▪ **Struttura prezzi**: evidenziare parte fissa e %; per canale (filiale, online, API), per valuta e tipo (ordinario vs istantaneo). ▪ **Divieti/limiti**: Surcharging vietato sui pagamenti con carte regolamentate (come carte consumer a quattro parti: l'emittente della carta, l'esercente, l'acquirer (la banca dell'esercente) e il circuito di pagamento (es. Visa, Mastercard) ▪ **One-leg-out**: informare su possibili costi di corrispondenti/intermediari.
Valute, tassi di cambio e DCC (Dynamic Currency Conversion)	▪ Tasso di cambio applicato o mark-up sul tasso di riferimento (es. BCE) espresso in percentuale, Importo stimato nella valuta del cliente e nella valuta del beneficiario. ▪ Eventuali commissioni fisse aggiuntive. ▪ DCC su POS/ATM/online: confronto chiaro "Affidati alla conversione della tua banca/emittente" vs "Accetta la conversione del commerciante/ATM (DCC)", con pari evidenza. Indicare il mark-up DCC rispetto al tasso di riferimento e l'importo risultante nella valuta del cliente. Nessuna opzione preselezionata; pulsanti di scelta equivalenti; messaggi neutrali.
Rendicontaz. e ricevute (ex post)	▪ Per ogni operazione, il PSP del pagatore e/o del beneficiario deve fornire su supporto durevole: Identificativo univoco dell'operazione, importo e valuta addebitata/accreditata; se c'è conversione, entrambe le valute, Tasso FX e mark-up, data/ora del tasso, commissioni applicate separate, Beneficiario/pagatore: nome e identificatore (es. IBAN o alias), Data valuta e data di esecuzione, Canale (POS, online, ATM, API/PIS), Esito e, se negata, motivo sintetico. Per addebiti diretti: mandato, Riferimetnio Unico Mandato (RUM)/identificativi SEPA, diritti di rimborso. ▪ Estratti conto periodici: frequenza, almeno mensile se ci sono movimenti; sempre disponibili in area riservata, Contenuti: elenco operazioni; saldo iniziale/finale; commissioni totali per periodo; indicatori su spese ricorrenti; ▪ Notifiche in tempo reale: spiegazione degli alert configurabili per operazioni, limiti superati, nuovi beneficiari, operazioni transfrontaliere/FX, con indicazione chiara se a pagamento e relativo costo.

Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

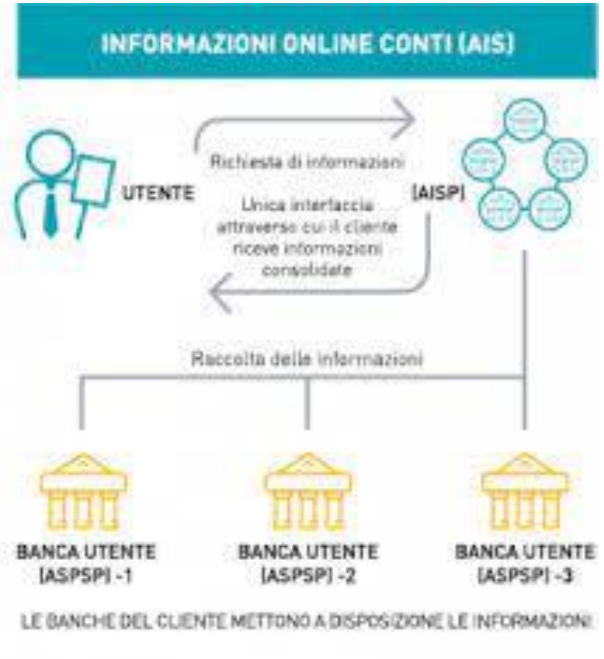
PSR – Trasparenza e Informativa

One-leg-out" (fuori dallo SEE)	▪ **Ex ante**: spiegare tempi indicativi, possibili fee di banche corrispondenti, rischi di ripartizione spese, e se l'importo al beneficiario può subire riduzioni non controllate dal PSP UE. ▪ **Ex post**: indicare quanto è stato detratto da intermediari, se comunicato al PSP; altrimenti, avvertenza che potrebbero esserci state deduzioni esterne.
Requisiti di forma, lingua accessibilità	▪ Lingua: nella lingua del paese dell'utente o in una lingua concordata. Evitare gergo; glossario semplice. ▪ Accessibilità: canali e documenti compatibili con assistive technologies; ▪ Conservazione: documenti archiviati e accessibili per un periodo congruo, di facile download.
Specificità per TPP (AIS/PIS/CBPII)	▪ PIS: ➢ Prima dell'avvio: informare che il pagamento sarà avviato tramite PISP dal conto presso l'ASPSP; eventuali costi del PISP; dati scambiati; stato/riscontro dell'ordine. ➢ Dopo: conferma esito e identificativo operazione. ▪ AIS: ▪ Prima: finalità, dataset minimo, frequenza di accesso, durata del consenso (es. fino a 180 giorni se/come previsto nei RTS), come revocare via dashboard ASPSP. ▪ Durante: indicare quando avviene la re-autenticazione; notificare accessi periodici rilevanti se l'utente lo desidera. ▪ CBPII: Informare che la risposta è solo "sì/no" alla disponibilità fondi entro un tetto, senza condividere saldo o dettagli di transazione.

Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

PSR – Trasparenza e Informativa

- PISP (Payment Initiation Service Provider) avvia pagamenti per conto del cliente, previa sua autorizzazione, agendo da intermediario tra cliente e banca;
- AISP (Account Information Service Provider) Aggrega informazioni da più conti bancari e fornisce una visione consolidata della situazione finanziaria del cliente,
- ASPSP (Account Servicing Payment Service Provider) è l'istituto bancario che gestisce il conto,
- CBPII il prestatore di servizi che emette strumenti di pagamento "basati su carta" (carte fisiche o virtuali) e che, grazie al servizio di "confirmation of funds", può chiedere alla banca che detiene il conto del pagatore se ci sono fondi sufficienti per una certa operazione.



Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

PSR – Diritti e obblighi nelle operazioni

Consenso, ricezione e revoca degli ordini	▪ **Consenso**: un'operazione è valida solo se il pagatore ha dato consenso con i canali e le procedure concordate (spesso con SCA e dynamic linking a importo/beneficiario). ▪ **Momento di ricezione** ("time of receipt"): coincide con il momento in cui il PSP del pagatore riceve l'ordine; se oltre il cut-off concordato, si considera ricevuto il giorno lavorativo successivo; se è programmato per una data futura (standing order), il momento di ricezione è quel giorno (o il primo lavorativo utile se cade in giorno non lavorativo); con PIS: l'ordine è considerato ricevuto dall'ASPSP quando il PISP lo trasmette all'ASPSP. ▪ **Revoca**: in linea generale, il pagatore può revocare fino al momento di ricezione; per i pagamenti avviati dal beneficiario o tramite beneficiario (es. addebiti diretti) la revoca possibile fino alla fine del giorno lavorativo precedente la data di addebito concordata; le revoche successive sono possibili solo se previsto dal contratto e con accordo del PSP/beneficiario.
Rifiuto di un ordine	▪ Il PSP può rifiutare se l'ordine non rispetta i requisiti (fondi insufficienti, IBAN non valido, limiti, sospetti di frode/AML). ▪ In tal caso deve dare informativa "immediata" o entro la fine del giorno lavorativo successivo, indicando il motivo e come rimediare, salvo divieti di legge (es. indagini AML).
Tempi di esecuzione	▪ **Pagamenti elettronici intra-UE** in valuta UE/SEE: addebito/accredito entro il giorno lavorativo successivo (D+1). Ordini cartacei: D+2. ▪ **Pagamenti programmati**: eseguiti il giorno concordato. ▪ **Instant payments**: regole specifiche nel regolamento dedicato (prezzo non superiore all'ordinario). ▪ **One-leg-out**: i tempi possono variare per infrastrutture extra-SEE; resta l'obbligo di trasparenza ex ante.
Data valuta e disponibilità fondi	▪ **Sul conto del pagatore**: la data valuta dell'addebito non può essere anteriore al momento dell'addebito. ▪ **Sul conto del beneficiario**: la data valuta del credito non può essere posteriore al giorno in cui i fondi sono accreditati al PSP del beneficiario; i fondi devono essere messi a disposizione senza ritardi ingiustificati. ▪ **Divieti di retrodatazioni penalizzanti** e di "parcheggi" non motivati dei fondi.

Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

PSR – Diritti e obblighi nelle operazioni

Operazioni non autorizzate: rimborsi e responsab.	▪ **Rimborso al pagatore**: il PSP del pagatore deve rimborsare senza indugio l'importo e ripristinare il conto allo stato pre-addebito (inclusi interessi/commissioni collegate). ▪ **Franchigia a carico dell'utente**: fino a 50 EUR per perdite derivanti da uso indebito dello strumento di pagamento prima della notifica di smarrimento/furto/misappropriazione. ▪ **Nessuna franchigia quando**: l'operazione è avvenuta senza SCA a causa del PSP; l'utente non ha agito con frode o colpa grave; si tratta di operazioni successive alla notifica di blocco. ▪ **Onere della prova**: sul PSP, che deve dimostrare SCA, registrazione corretta e assenza di malfunzionamenti. ▪ **Sospensione del rimborso**: possibile solo se il PSP ha fondati motivi di sospettare frode del cliente, da documentare; in tal caso deve informare l'utente (salvo limiti di legge). ▪ **Social engineering/impersonation**: sono rafforzati gli obblighi di warning e misure antifrode; il riparto di responsabilità in questi casi sarà precisato da EBA/ADR. In generale, più robuste le misure del PSP, minore il rischio di contenzioso.
Non esecuzione, esecuzione tardiva o difettosa	▪ **Se responsabile è il PSP del pagatore**: deve rimborsare senza indugio il pagatore, ripristinando il saldo come se l'operazione non fosse avvenuta o fosse avvenuta correttamente; su richiesta, tracciare/indagare l'operazione e comunicare l'esito. ▪ **Se responsabile è il PSP del beneficiario**: deve accreditare senza indugio il beneficiario e sistemare date valuta/interessi; cooperare con il PSP del pagatore per rintracciare i fondi. ▪ **Funzionamento**: il PSP del pagatore rimborsa l'utente e poi, se il danno è imputabile al PISP, può rivalersi sul PISP.

Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

PSR – Diritti e obblighi nelle operazioni

IBAN errato e pagamenti "misdirected"	▪ **Esecuzione "sull'identificativo unico"**: se il pagatore ha indicato un IBAN sbagliato, il PSP che ha eseguito correttamente su quell'IBAN non è responsabile. ▪ **Obbligo di cooperazione nel recupero fondi**: il PSP del pagatore deve attivarsi "senza indugio" per richiedere il riaccredito; può addebitare costi "ragionevoli" se l'errore è del cliente (come da ctr); se il recupero fallisce, il PSP deve fornire informazioni utili (nei limiti di legge) per permettere al pagatore di agire contro il beneficiario indebito. ▪ **Verifica IBAN-nome** (confirmation of payee): obbligo di avviso pre-esecuzione in caso di mismatch, per ridurre i misdirected payments.
Strumenti di pagamento: uso, sicurezza e blocco	▪ **Obblighi dell'utente**: conservare con diligenza lo strumento e le credenziali; non condividere PIN/OTP/password; separare carta e PIN; notificare "senza indugio" smarrimento/furto/misuso e qualsiasi anomalia. ▪ **Obblighi del PSP**: mettere a disposizione canali 24/7 gratuiti per blocco e segnalazioni; informare l'utente sulle misure di sicurezza e su come gestire le emergenze; bloccare o limitare l'uso in caso di sospetti fondati di frode/compromissione e informarne l'utente, salvo restrizioni legali. ▪ **Responsabilità post-blocco**: il cliente non risponde delle operazioni successive alla notifica di blocco, salvo frode.
Addebiti diretti e rimborsi	▪ **SEPA Core**: diritto di rimborso "senza domande" entro 8 settimane dalla data di addebito per operazioni autorizzate; 13 mesi per non autorizzate. ▪ **Altri casi con importo non noto** al momento del consenso (pagamenti "initiated by payee"): diritto al rimborso entro 8 settimane se l'importo addebitato eccedeva quanto ragionevolmente atteso (spesa storica, condizioni del mandato, circostanze); il PSP può chiedere prove e, se rifiuta, deve motivare per iscritto. ▪ **Schema SEPA B2B**: niente rimborso "8 settimane" per addebiti autorizzati (tutela risiede nei controlli pre-addebito); resta il diritto per addebiti non autorizzati.

Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

PSR – Diritti e obblighi nelle operazioni

Operazioni a importo non determinato (pre-autorizzazioni)	▪ E' il caso degli addebiti per carburanti self-service, depositi hotel/noleggi. In questi casi: ➢ il PSP/merchant può porre un "blocco" di fondi proporzionato all'importo stimato; ➢ una volta noto l'importo finale, il blocco residuo va rilasciato senza indugio; ➢ è vietato mantenere blocchi eccedenti o prolungati ingiustificatamente; durate massime e altre regole saranno precisate da EBA. ▪ Trasparenza: informare l'utente ex ante che l'importo finale è variabile e che ci sarà un blocco temporaneo.
Commissioni collegate a errori /recuperi	▪ Indagini su operazioni non autorizzate o difettose dovute al PSP: nessun costo per il cliente. ▪ Recupero fondi per IBAN errato imputabile al cliente: il PSP può applicare costi ragionevoli se previsto. ▪ Copertura danni ulteriori: il cliente può chiedere il risarcimento di danni conseguenti (es. interessi, penali) se imputabili all'inadempimento del PSP, secondo diritto nazionale.
Termini per contestare e prova	▪ Notifica "senza indugio" appena l'utente rileva il problema. ▪ Termine lungo: fino a 13 mesi dalla data di addebito/accredito per contestare operazioni non autorizzate o eseguite in modo difettoso (se il PSP ha rispettato gli obblighi informativi). ▪ Onere della prova: in capo al PSP (autenticazione, registrazione, funzionamento sistemi).
Reclami e ADR	▪ Tempi: risposta entro 15 giorni lavorativi (eccezionalmente 35, con motivazione). ▪ Se insoddisfatti: accesso ad organismi Alternative Dispute Resolution (ADR) e ulteriori vie di ricorso; cooperazione cross-border tra autorità/ADR.

Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

PSR – Sicurezza, SCA e prevenzione frodi

Strong Customer Authenticat. (SCA)

- Cosa resta **invariato**: SCA a 2 fattori da categorie diverse (conoscenza/possesso/inerenza) e indipendenti. Dynamic linking per pagamenti elettronici a distanza: l'autenticazione deve essere "legata" a importo e beneficiario.
  Si ricorda che il Dynamic Linking è un fattore di sicurezza, introdotto da PSD2 a tutela di chi effettua operazioni di pagamento online, che permette di collegare la transazione in modo dinamico e univoco all'importo e al beneficiario specificati dall'utente al momento in cui dispone il pagamento.

- **Chiarimenti** in ambito
  - Out-of-scope o regimi particolari confermati: Direct debit (non richiede SCA del pagatore), MOTO (mail order/telephone order) e terminali unattended per trasporti/parcheggi. Merchant-Initiated Transactions (MIT): niente SCA al momento dell'addebito se esiste un mandato/consenso iniziale SCA. "Secure corporate payment processes": processi aziendali certificati possono costituire alternativa alla SCA classica.
  - One-leg transactions: rafforzata la facoltà/aspettativa di applicare controlli di rischio anche quando una sola delle parti è in UE.
- **Esenzioni** e soglie SCA
  - Rimane l'impianto di esenzioni (pagamenti low-value, contactless, trusted beneficiaries, recurring/fixed-amount, corporate).
  - Armonizzazione/aggiornamento soglie: la Commissione/EBA potranno riallineare soglie/condizioni via RTS per ridurre attriti mantenendo il livello di rischio sotto controllo.

Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

PSR – Sicurezza, SCA e prevenzione frodi

Prevenzione frodi: misure strutturali	▪ **Verifica beneficiario** (name/IBAN check): obbligo di offrire un servizio di "match nome-IBAN" al momento dell'ordine di bonifico per avvisare l'utente in caso di discrepanze rilevanti; coordinamento con il Regolamento sui bonifici istantanei; ▪ **Transaction Risk Analysis** (TRA) **rafforzata**: dataset minimo e metriche più uniformi per le esenzioni basate sul rischio; estensione della TRA a scenari finora eterogenei (es. istantanei) con criteri comparabili intra-UE. ▪ **Condivisione dati antifrode tra PSP**: Base giuridica esplicita per condividere indicatori di rischio/frode (es. IBAN/conti "mule", device fingerprint, pattern) nel rispetto del GDPR. Reporting armonizzato verso autorità nazionali/EBA con tassonomia comune delle tipologie di frode e pubblicazione di statistiche per benchmark; ▪ **Controlli lato beneficiario** (payee PSP): Obblighi più chiari per screening e monitoraggio dei conti beneficiari ad alto rischio (nuove relazioni, comportamenti anomali, flussi tipici dei mule account). Cooperazione "time-critical" nei casi di recall/freeze su fondi ricevuti da frode, nel rispetto della normativa privacy/AML. ▪ **Messaggi di avviso e "friction intelligente"**: Obbligo di fornire avvisi chiari e tempestivi per pagamenti ad alto rischio (nuovo beneficiario, discrepanza nome-IBAN, importi anomali), con frizioni proporzionate (ad es. riconferma, rafforzamento SCA, eventuale breve ritardo) dove giustificato dal rischio.

Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

PSR – Sicurezza, SCA e prevenzione frodi

Responsabilità, rimborsi e diritti dell'utente	▪ Transazioni non autorizzate ➢ Rimborso "immediato" (al più tardi entro il giorno lavorativo successivo) salvo sospetto di frode del cliente; onere della prova in capo al PSP. ➢ Conferma della franchigia a carico del cliente in caso di strumenti smarriti/sottratti fino al blocco; eventuali modifiche puntuali alla franchigia e ai casi di esonero sono oggetto di negoziato e di prossimi RTS. ➢ "SCA effettuata" non basta a provare negligenza grave dell'utente: servono elementi concreti sul comportamento. ▪ Social engineering e APP fraud (authorized push payments) ➢ Introduzione (a livello di proposta) di tutele addizionali per alcune fattispecie di impersonation/scam, specie quando l'utente è indotto in errore nonostante controlli ragionevoli messi in atto; riparto di responsabilità tra PSP del pagatore e del beneficiario se uno dei due non ha adottato le misure richieste (es. mancati avvisi, mancata cooperazione, controlli carenti sul conto del beneficiario). Dettagli e criteri di applicazione saranno precisati in norme secondarie/linee guida. ▪ Bonifici verso IBAN errato e recupero fondi ➢ Processo di recall più efficace e vincolante: obbligo per il PSP del beneficiario di cooperare entro tempi stretti, inclusa la possibilità di bloccare i fondi ancora disponibili e di facilitare il rientro. ➢ Rafforzate le informazioni rese all'utente sullo stato del recupero e sulle opzioni successive (es. denuncia, ADR).

Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

Open banking: AIS, PIS, CBPII nel pacchetto PSD3/PSR

Responsabilità, rimborsi e diritti dell'utente	▪ **Dedicated API obbligatoria**: Accesso solo tramite interfacce dedicate sicure. L'uso dell'interfaccia "PSU" come fallback resta eccezionale e condizionato a KPI non rispettati. ▪ Funzionalità minime e dataset ➢ La Commissione/EBA definiranno, via atti di esecuzione/RTS, un set minimo uniforme di: Endpoints (es. bilancio, storico transazioni, lista conti, stato pagamento, revoca, conferma fondi). Campi dati (IBAN, nome intestatario, saldo disponibile/contabile, dettagli transazione incl. remittance info, data valuta, identificativi univoci). Formati e semantica coerenti (allineamento atteso a ISO 20022/JSON). ▪ Performance e disponibilità: Obiettivo di equivalenza con i canali usati dal cliente (no throttling ingiustificato). KPI/monitoraggio pubblici e reporting alle Autorità; procedure di remediation e perdita dell'esenzione fallback in caso di degradazione persistente. ▪ Stop agli "ostacoli": Espliciti divieti di pratiche che degradano l'esperienza TPP: re-SCA non necessaria, redirection ridondante, dati incompleti, ritardi artificiali, limiti di frequenza non motivati, impossibilità di pre-popolare dati, ecc. ▪ Onboarding e supporto TPP: Ambiente di test/sandbox, documentazione aggiornata, canale incidenti e change management obbligatori.
Consenso e controllo dell'utente	▪ Permission dashboard: Ogni ASPSP deve offrire al cliente una vista centralizzata dei consensi attivi (AIS/PIS/CBPII) con revoca/limitazione granulari (per account, per TPP, per durata/scope), audit trail e timestamp. ▪ Fine del "re-SCA 90 giorni" per AIS: eliminazione dell'obbligo per i Prestatori di Servizi di Informazione sui Conti (AISPs) di richiedere una nuova SCA ogni 90 giorni, dopo SCA iniziale e consenso esplicito, l'accesso AIS può proseguire in modo continuativo fino alla scadenza/ revoca del consenso, senza re-autenticazioni cicliche imposte. ▪ Granularità del consenso: Perimetro dati (es. solo saldo vs saldo+transazioni), periodo storico, frequenza di accesso, conti inclusi; obbligo di principi di minimizzazione (GDPR). ▪ Identificazione TPP: Confermata l'identificazione tramite certificati qualificati (eIDAS); allineamento all'eIDAS aggiornato verrà precisato in atti secondari.

Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

Open banking: AIS, PIS, CBPII nel pacchetto PSD3/PSR

AIS (Account Information Services)	▪ Scope dei conti: Chiarito che rientrano tutti i "conti di pagamento" accessibili online presso banche e PSP non bancari (incl. conti e-money); chiarimenti attesi su carte a saldo/ revolving con funzionalità di pagamento. ▪ Dati accessibili: Dataset minimo armonizzato con identificativo conto (IBAN/BIC), intestatario, tipo/currency, saldo disponibile e contabile, elenco transazioni con causali, controparti e riferimenti; potenziale accesso a standing orders/mandati SEPA ove tecnicamente disponibili (da definire in RTS). ▪ Frequenza e modalità: Vietati limiti arbitrari; consentite chiamate periodiche coerenti col consenso e con la sicurezza. Possibile supporto a notifiche/event-driven (webhook) come "funzionalità premium". ▪ Esperienza utente: Niente re-SCA periodica obbligatoria; maggiore trasparenza sul TPP (chi è, cosa vede, per quanto tempo); revoca istantanea via dashboard. ▪ Privacy: consenso esplicito del cliente; obbligo di data minimization e retention limitata; TPP tenuti a DPIA ove necessario.

Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

Open banking: AIS, PIS, CBPII nel pacchetto PSD3/PSR

PIS (Payment Initiation Services)	▪ Accesso non discriminatorio ai "rails"(infrastrutture, protocolli, sistemi e regole): gli ASPSP non possono ostacolare PIS né applicare condizioni peggiorative rispetto ai canali propri; PIS deve poter usare SCT/SCT Inst a condizioni eque, incluse le nuove verifiche nome–IBAN. ▪ Flussi SCA e UX: supporto a redirection, app-to-app e canali decoupled; vietate frizioni non necessarie. Dynamic linking obbligatorio; possibilità di esenzioni (es. pagamenti ricorrenti di importo fisso) secondo RTS aggiornati. ▪ Stati e conferme del pagamento: API di stato più granulari e tempestive (ordine ricevuto, accettato, in esecuzione, eseguito/valuta, rifiutato), con identificativi univoci utili alla riconciliazione del merchant. Obiettivo: dare ai PIS un "signal" affidabile paragonabile all'autorizzazione carte. ▪ Revoca/annullo: chiarezza su tempi e modalità di revoca del bonifico prima dell'esecuzione; cooperazione PIS–ASPSP per evitare doppi addebiti/duplicazioni. ▪ Ricorrenti e "mandati": possibilità di instaurare consensi ricorrenti (pagamenti fissi o "sweeping" verso conto proprio) con SCA iniziale e successivo uso di esenzioni; gli scenari "variabili" richiederanno parametri e guardrail da definire in RTS. ▪ Responsabilità e rimborsi: Confermata la ripartizione PSD2 con chiarimenti: ➢ L'ASPSP del pagatore resta responsabile dell'esecuzione corretta del bonifico ricevuto. ➢ Il PISP risponde verso ASPSP e utente per errori nell'iniziazione (doppio invio, importo errato, dati alterati) e deve provare la corretta autenticazione/trasmissione. ▪ Coordinamento con nuove tutele anti-frodi (avvisi rischio, verifica nome–IBAN, recall più efficace).

Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

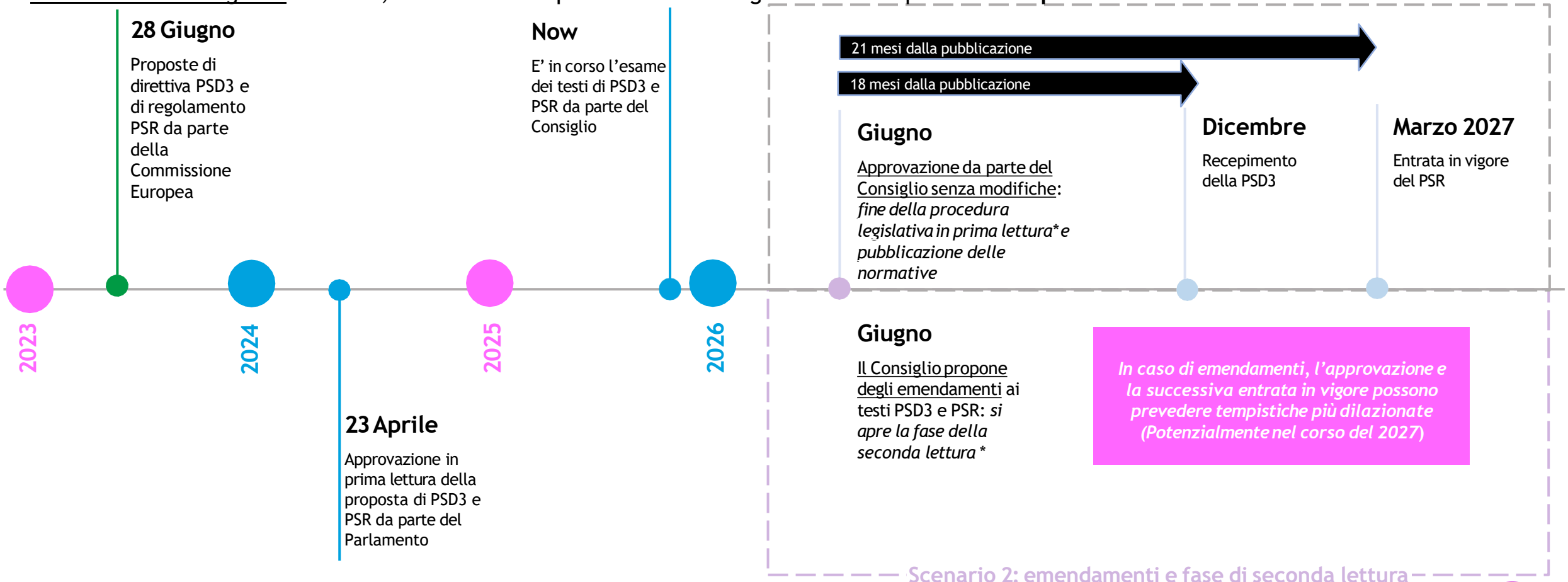
Open banking: AIS, PIS, CBPII nel pacchetto PSD3/PSR

CBPII (Conferma disponibilità fondi)	▪ Scopo e perimetro ➢ Il soggetto che emette uno strumento di pagamento "card-based" può chiedere all'ASPSP del pagatore una conferma "sì/no" sulla sufficienza dei fondi su un conto di pagamento del cliente, previa autorizzazione del cliente stesso. ➢ Chiarito l'accesso anche ai conti presso PSP non bancari (grazie alla convergenza con e-money). ▪ Dati e minimizzazione: Risposta limitata al necessario (boolean e, dove previsto, importo massimo garantibile); esclusa la trasmissione di bilanci o dettagli transazioni. ▪ Frequenza e performance: Divieto di limiti arbitrari; requisiti di latenza per casi real-time (es. pre-autorizzazione carte). Rate limiting ammesso solo per ragioni tecniche/sicurezza documentate. ▪ Consenso e sicurezza: Consenso esplicito, revocabile via dashboard; log di accesso e tracciabilità; autenticazione/identificazione TPP conforme eIDAS.
Prezzi e "premium APIs"	▪ Accesso "base" gratuito: Come in PSD2, l'accesso alle funzionalità obbligatorie AIS/PIS/CBPII non può essere a pagamento per i TPP autorizzati. ▪ Premium a contratto: Ammesso offrire, su base commerciale, funzionalità oltre il minimo (es. webhooks, arricchimento dati, alias, bulk, instant status avanzati), a patto che il canale "base" resti pienamente funzionale e non degradato.

Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

Timeline dell'iter legislativo

Secondo l'iter legislativo, a seguito dell'entrata in vigore dei testi, sono previsti **18 mesi per il recepimento della PSD3** all'interno del **diritto nazionale** e **21 mesi per l'applicazione del PSR**. Attualmente è **in corso l'analisi da parte del Consiglio dell'UE** al fine di adottare una posizione in prima lettura su entrambi gli atti. Pertanto, a seconda della posizione del Consiglio sono stati ipotizzati **due possibili scenari.**



Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

Conclusioni

Alla luce dei risultati della valutazione sulla PSD2, la Commissione ha tratto due conclusioni fondamentali:

- da un lato, ha riconosciuto la necessità di apportare modifiche mirate e tempestive al quadro normativo dei pagamenti dell'Unione europea;
- dall'altro lato, ha ritenuto opportuno che tali modifiche rappresentino una graduale e fisiologica evoluzione, piuttosto che una rivoluzione.

In questo senso, infatti, in alcuni ambiti, non sono emerse criticità tali da richiedere modifiche sostanziali. In altri ambiti, invece (ad esempio, in materia di open banking), la Commissione ha tenuto conto delle esperienze acquisite dall'entrata in vigore della PSD2 e degli investimenti già effettuati per conformarsi a queste norme. Ha anche valutato i potenziali costi associati ad una eventuale revisione totale delle disposizioni, ritenendo opportuno evitare di adottare scelte legislative che comportino nuovi oneri di attuazione significativi e risultati incerti. Le proposte di revisione della PSD2 costituiscono un pacchetto di modifiche finalizzate a migliorare il funzionamento del mercato dei pagamenti nell'Unione europea e a rafforzare la tutela dei consumatori. Tali modifiche sono allineate agli obiettivi della strategia della Commissione per i pagamenti al dettaglio e si integrano con le iniziative in corso, la proposta relativa alla "finanza aperta" (FIDA), che la Commissione ha presentato congiuntamente alla revisione della PSD2.

Per quanto concerne il processo di recepimento e attuazione della terza direttiva e del regolamento sui servizi di pagamento, è da notare che, a seguito della presentazione da parte della Commissione europea in data 28 giugno 2023, il processo legislativo procede attraverso la fase di discussione e negoziazione presso il Parlamento europeo e il Consiglio dell'Unione europea. Durante questa fase, le proposte iniziali possono essere soggette a modifiche e integrazioni, e solamente dopo aver raggiunto un accordo sull'approvazione delle proposte, tali testi divengono legge europea. Tuttavia, dopo l'adozione a livello europeo, gli Stati membri dell'Unione europea sono responsabili del recepimento e dell'implementazione delle relative disposizioni all'interno delle rispettive legislazioni nazionali, generalmente entro un termine massimo di due anni. Il termine effettivo per l'implementazione e il recepimento di tali nuove norme in Italia sarà condizionato dalla celerità e dall'efficacia con cui il Parlamento italiano e le autorità nazionali completeranno il processo di recepimento e attuazione.

Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

Conclusioni

La PSD3 non è un aggiornamento incrementale ma una ridefinizione fondamentale di cosa significa operare nel settore dei pagamenti europei. Dove PSD2 ha aperto le porte, PSD3 costruisce l'infrastruttura per i prossimi decenni.

Il successo dipenderà dalla capacità del mercato di vedere oltre i costi di compliance e cogliere le opportunità di trasformazione. I vincitori saranno coloro che comprenderanno che PSD3 non riguarda solo i pagamenti, ma la costruzione di un ecosistema finanziario digitale inclusivo, sicuro e innovativo per tutti i cittadini europei.

La vera sfida non è tecnica o normativa, ma culturale: trasformare un settore tradizionalmente conservativo in un motore di innovazione sociale ed economica. PSD3 fornisce gli strumenti; sta al mercato utilizzarli con saggezza e visione.

Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento

Conclusioni

La doppia transizione, digitale e climatica, comporta una sfida difficile, ma rappresenta anche un'opportunità unica, per il settore finanziario e per l'intera economia.

In futuro, l'evoluzione normativa e quella infrastrutturale dovranno essere continui; ma sarà altrettanto importante la collaborazione tra diverse organizzazioni, pubbliche e private, coinvolte a vario titolo nelle trasformazioni in atto.

Solo attraverso un impegno comune e una visione lungimirante sarà possibile cogliere appieno i benefici della twin transition, favorendo una crescita inclusiva e sostenibile, in grado di rispondere alle sfide globali e promuovere la competitività delle nostre imprese.

CONSILIA
Business Management

CONTACTS

Corso Europa, 13 – 20122 Milano

+39 02 873 89 370 | Fax: +39 02 873 89 371

segreteria@consiliabm.com | info@consiliabm.com