

CONSILIA

Business Management

La responsabilità delle Banche nella sicurezza dei pagamenti

Milano, martedì 25 novembre 2025

- **Il Regolamento FiDA – la condivisione dei dati finanziari**
- **Operazioni di pagamento non autorizzate: le aspettative di vigilanza della Banca d'Italia**

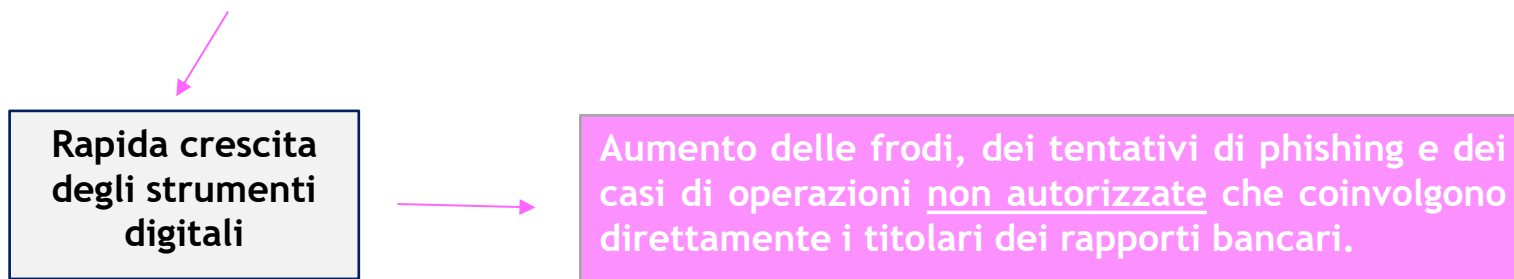
- **Il Regolamento FiDA – la condivisione dei dati finanziari**
- Operazioni di pagamento non autorizzate: le aspettative di vigilanza della Banca d'Italia

Premessa

Inquadramento normativo e contesto attuale

Negli ultimi anni il settore dei servizi finanziari e dei pagamenti ha attraversato una trasformazione molto profonda.

La crescente digitalizzazione, l'espansione dell'e-commerce e l'evoluzione dei comportamenti dei clienti hanno reso i pagamenti sempre più veloci, più integrati e più esposti ai rischi informatici.



L'innovazione nei pagamenti porta con sé enormi opportunità, ma richiede anche meccanismi di sicurezza più robusti, una maggiore trasparenza e una gestione più consapevole dei dati finanziari.

Ed è proprio in questo quadro che si collocano gli interventi regolamentari degli ultimi anni - prima con la PSD2, che ha aperto la strada all'open banking, e oggi con il Regolamento FiDA, che rappresenta l'evoluzione naturale verso un' ecosistema di open finance pienamente integrato.



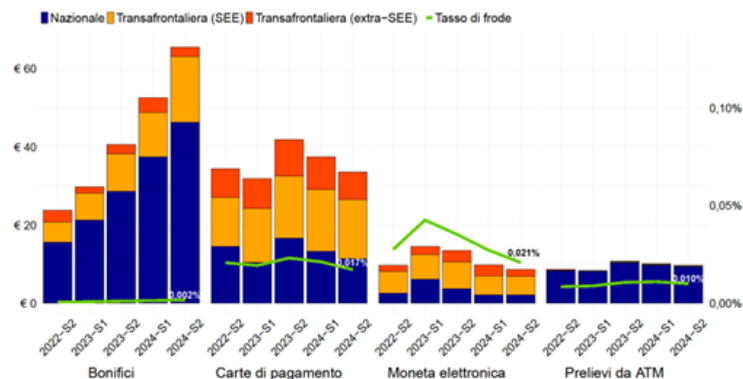
Premessa

Inquadramento normativo e contesto attuale

Figura 1. 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)

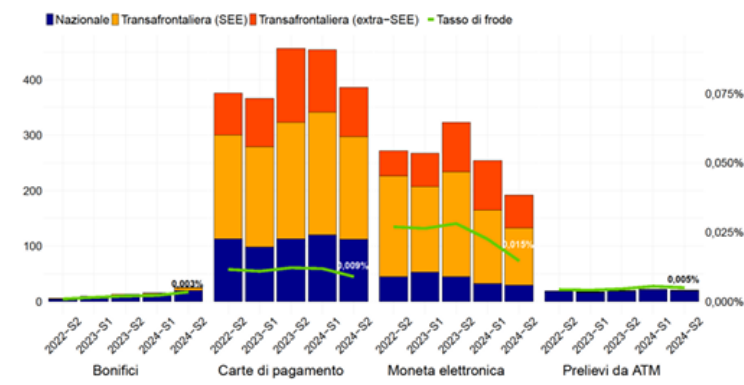


Il valore economico delle frodi mostra un peso maggiore sulle carte di pagamento, con un contributo rilevante delle operazioni transfrontaliere.

I bonifici presentano valori inferiori, ma una tendenza crescente negli episodi di phishing e social engineering. Il tasso di frode, pur restando basso in termini percentuali, evidenzia che il rischio è distribuito in modo diverso tra i vari strumenti.

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.

Note: l'insieme dei bonifici non considera quelli effettuati con modalità tradizionali, ovvero allo sportello.

Il numero delle operazioni fraudolente conferma che le carte sono lo strumento più colpito, soprattutto online e nelle transazioni cross-border.

Moneta elettronica e prelievi ATM presentano un'incidenza molto più contenuta, mentre i bonifici, pur con un numero limitato di casi, stanno diventando sempre più rilevanti per gravità degli importi.

Dai grafici emerge che le carte di pagamento sono lo strumento più esposto alle frodi, sia per valore sia per numero, soprattutto nelle operazioni transfrontaliere. Tuttavia, i tassi di frode rimangono complessivamente bassi su tutti gli strumenti, grazie al rafforzamento dei presidi di sicurezza.



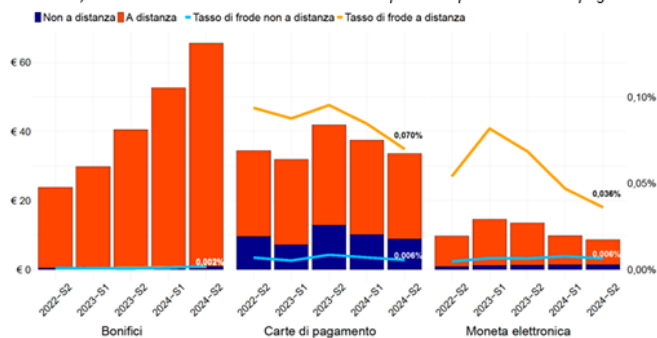
Premessa

Inquadramento normativo e contesto attuale

Figura 6. Livelli e tassi di frode per strumento di pagamento e canale di utilizzo “a distanza” vs. “non a distanza”

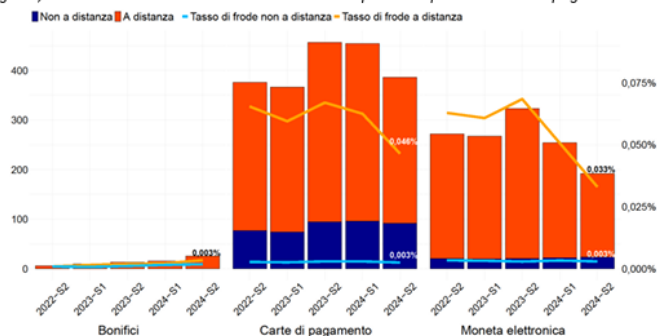
a) Valore delle operazioni fraudolente

(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.

Note: L'insieme dei bonifici non considera quelli effettuati con modalità tradizionali, ovvero allo sportello.

Mentre i dati della Banca d'Italia mostrano chiaramente **dove e come le frodi si verificano**, FIDA rappresenta lo strumento normativo e tecnico per **migliorare l'accesso ai dati, aumentare la trasparenza e prevenire frodi**, garantendo sicurezza e innovazione nello stesso tempo.

Accesso sicuro e regolamentato ai dati finanziari

Maggiore trasparenza e tracciabilità dei flussi di pagamento

Protezione del cliente e delle sue informazioni



FiDA: Financial Data Access Regulation

Contesto normativo di applicazione

Per comprendere il Regolamento FIDA (*Financial Data Access*), è utile collocarlo nel contesto evolutivo della normativa europea in materia di dati finanziari.

La prima tappa fondamentale è stata la PSD2 (Direttiva 2015/2366/UE sui servizi di pagamento), recepita in Italia con il **D.Lgs. 218/2017**, entrata in vigore il 13 gennaio 2018. La PSD2 ha introdotto il meccanismo dell'**Open Banking**, imponendo alle banche l'obbligo di rendere disponibili, tramite API, i dati di conto e di pagamento a soggetti terzi autorizzati (TPP - Third Party Providers), previo consenso del cliente. L'obiettivo era favorire la concorrenza e l'innovazione nei servizi di pagamento digitali.

Tuttavia, la PSD2 riguarda **principalmente dati relativi ai conti di pagamento**, escludendo categorie come investimenti, prodotti assicurativi, pensioni, crypto-attività e altri strumenti finanziari.

ESTENDERE LA LOGICA DELL'OPEN-BANKING A TUTTI I SERVIZI FINANZIARI

Nell'ambito della strategia europea dei servizi finanziari digitali, avviata nel 2020, nasce **FiDA**, con la proposta di regolamento della Commissione europea del **28 giugno 2023**.

Tale regolamento mira a estendere il principio di condivisione dei dati dall'open banking a un vero e proprio open finance, includendo tutte le tipologie di dati finanziari sopra menzionate.



FiDA: Financial Data Access Regulation

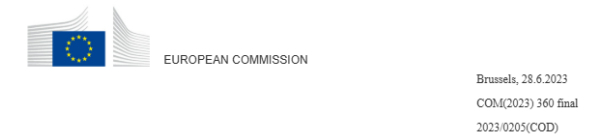
Contesto normativo di applicazione

FIDA si inserisce nella più ampia cornice della European Data Strategy (febbraio 2020) e della Strategia per la finanza digitale, confermando l'obiettivo dell'UE di creare un ecosistema dei dati finanziari sicuro, interoperabile e competitivo a livello europeo.

Il **28 giugno 2023**, la Commissione Europea ha presentato la proposta di un regolamento volto a potenziare l'accesso e la condivisione dei dati finanziari all'interno dell'Unione Europea, denominato **FiDA (Financial Data Access Regulation)**.

Questo framework si inserisce in una strategia più ampia dell'UE per la creazione di un **ecosistema di open finance**, finalizzato a consentire la condivisione sicura dei dati degli utenti tra soggetti operanti nei settori bancario, assicurativo, degli investimenti, dei pagamenti e finanziario in generale.

FiDA si fonda sui principi dell'**open banking** introdotti dalla **PSD2** - la Direttiva europea pensata per rendere i servizi di pagamento più sicuri ed efficienti negli Stati membri - e ne rappresenta un'evoluzione, anche in vista delle innovazioni normative introdotte dalla **PSD3**.



Brussels, 28.6.2023
COM(2023) 360 final
2023-0205(COD)

Proposal for a
REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
on a framework for Financial Data Access and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010, (EU) No 1095/2010 and (EU) 2022/2554

(Text with EEA relevance)

(SEC(2023) 255 final) - (SWD(2023) 224 final) - (SWD(2023) 230 final)

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

To be successful in a data driven economy that works for the people and businesses, Europe must strike a balance between the flow and wide use of data and preserving high privacy, security, safety and ethical standards. In the communication on a European strategy for data,¹ the Commission set out how the EU should create an attractive policy environment so that, by 2030, its share of the data economy at least corresponds to its economic weight.

In finance, the Commission identified the promotion of data-driven finance as one of the priorities in its 2020 digital finance strategy² and announced its intention to put forward a legislative proposal on a framework for financial data access. The 2021 Communication on a Capital Markets Union³ confirmed the Commission's ambition to accelerate its work on promoting data-driven financial services. It announced the establishment of the Expert Group on the European Financial Data Space to provide input on a first set of use cases. More recently, Commission President von der Leyen confirmed in her 2022 State of the Union letter of intent that data access in financial services is among the key new initiatives for 2023.

Customers of the EU financial sector currently cannot efficiently control access and sharing of their data beyond payment accounts. Data users, i.e. firms that want to access customer data to provide innovative services, have problems accessing data held by data holders, i.e. financial institutions that collect, store and process that customer data. As a result even where customers so wish, they do not have widespread access to data-driven financial services and financial products. A set of inter-related problems explain the limited access to data. First, in the absence of rules and tools to manage data sharing permissions, customers do not trust that potential risks of sharing data are addressed. Therefore, they are often reluctant to share their data. Second, even if they want to share data, the rules governing such sharing are either absent or unclear. As a result, data holders such as credit institutions, insurers and other financial institutions holding customer data are not always required to enable the access of data users, like for example, FinTech companies, i.e. companies using technology to support or provide financial services, or financial institutions that provide financial services and develop financial products on the basis of data sharing to their data. Third, data sharing is made more costly as both the data itself and the technical infrastructure are not standardised and therefore differ significantly.



FiDA: Financial Data Access Regulation

Definizioni utili

Il regolamento FiDA introduce una serie di definizioni fondamentali per comprendere appieno il nuovo quadro normativo. Queste esplicitazioni aiutano a chiarire i ruoli e le responsabilità degli attori coinvolti, così come la natura dei dati trattati.

CONSUMATORE E CLIENTE

Il regolamento distingue chiaramente tra “consumatore” e “cliente”. Il “consumatore” è una persona fisica che utilizza servizi finanziari per scopi non legati alla propria attività commerciale o professionale. Invece, il “cliente” può essere sia una persona fisica che giuridica che utilizza prodotti e servizi finanziari.

TITOLARE DEI DATI (DATA HOLDER)

Il “Data Holder” è un ente finanziario che raccoglie, conserva e tratta i dati inclusi nel regolamento FiDA, ma che non è un prestatore di servizi di informazione sui conti (l’AISP previsto dalla PSD2).

UTENTE DEI DATI (DATA USER)

Il “Data User”, invece, è un’entità autorizzata che, previa autorizzazione del cliente, ha accesso ai dati finanziari per fornire servizi specifici.

DATI DEL CLIENTE

Includono sia dati personali che non personali raccolti e trattati da un ente finanziario nell’ambito della propria attività. I dati del cliente comprendono le informazioni fornite direttamente dal cliente e quelle generate dalle interazioni tra il cliente e l’ente finanziario.

FISP

Prestatore di servizi di informazione finanziaria. Si tratta di un’autentica novità prevista dal regolamento, destinata (all’avviso di chi scrive) a incidere significativamente nelle strategie di sviluppo dell’Open Finance dei prossimi dieci anni. Un FISP è un soggetto “Data User” autorizzato a accedere ai dati dei clienti per fornire servizi di informazione finanziaria. Questi servizi possono variare dal monitoraggio delle transazioni alla consulenza finanziaria.



FiDA: Financial Data Access Regulation

Timeline - entrata in vigore del regolamento FiDA

PROPOSTA E
ACCORDO
POLITICO

ENTRATA IN
VIGORE

- **28 giugno 2023** - La Commissione Europea presenta la proposta di **FiDA (Financial Data Access Regulation)**. Obiettivo: migliorare l'accesso e la condivisione dei dati finanziari tra banche, assicurazioni, investitori e altri operatori finanziari, estendendo il concetto di **open banking** della PSD2.
- **4 dicembre 2024** - Il Consiglio UE raggiunge un **accordo politico** sul regolamento. La normativa è stata approvata a livello politico, pronta per l'entrata in vigore e la successiva implementazione.
- **Fine 2025/inizio 2026** - FiDA diventa **legalmente applicabile**.

Le banche e gli operatori devono iniziare a prepararsi, anche se alcune disposizioni richiedono ulteriori mesi per essere implementate concretamente.

Dopo l'entrata in vigore, FiDA prevede una **implementazione graduale in più fasi**:

- **+ 18 mesi**: vengono definiti e attivati gli schemi di condivisione dati tra banche e terze parti, per stabilire le regole comuni di accesso sicuro ai dati dei clienti.
- **+ 24 mesi - Fase 1**: inizia la condivisione dei dati base dei clienti, come conti correnti, risparmi, prestiti al consumo e assicurazioni non vita.
- **+ 36 mesi - Fase 2**: si estende la condivisione a dati più complessi, come mutui, investimenti, crypto-asset e prodotti pensionistici individuali.
- **+ 48 mesi - Fase 3**: entrano in gioco i dati business e prodotti complessi, come crediti alle imprese, rating creditizi, assicurazioni IBIPs e pensioni occupazionali.

Circa 5 anni dopo l'entrata in vigore: la Commissione UE effettua una **valutazione dell'impatto** della normativa, per verificarne l'efficacia e introdurre eventuali aggiustamenti.



FiDA: Financial Data Access Regulation

Ambito di applicazione del Regolamento FiDA

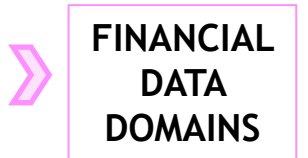
Il Regolamento FiDA definisce un quadro uniforme per la **condivisione dei dati dei clienti** (*customer data*), includendo sia **dati personali** sia **dati non personali**, purché tali informazioni siano fornite dal cliente oppure generate dall'interazione tra il cliente e l'intermediario.

Rientrano quindi nel perimetro tutti i dati che l'intermediario raccoglie, conserva o tratta nello svolgimento ordinario delle proprie attività.

Il Regolamento individua specifiche categorie di prodotti e servizi per le quali tali dati devono essere resi accessibili, nel rispetto dei requisiti tecnici e delle norme sul consenso.

In particolare, rientrano nel perimetro FiDA:

- Crediti ipotecari, finanziamenti e conti bancari, con esclusione dei conti di pagamento già disciplinati dalla PSD2.
- **Risparmi e investimenti**, includendo strumenti finanziari, prodotti di investimento assicurativi (IBIPs), crypto-attività, immobili e altre attività finanziarie, nonché i dati necessari per valutazioni di adeguatezza e appropriatezza.
- Prodotti pensionistici, in qualsiasi forma siano strutturati.
- **Prodotti assicurativi del ramo danni**, ad eccezione delle coperture relative a salute e malattia; rientrano anche le informazioni utilizzate per il demands and needs test e per le valutazioni di appropriatezza/adeguatezza del prodotto.
- **Dati utilizzati per la valutazione del merito creditizio delle imprese**, raccolti nell'ambito di richieste di finanziamento o nell'ambito dei processi di assegnazione del rating.



FiDA: Financial Data Access Regulation

Ambito soggettivo di applicazione di FiDA

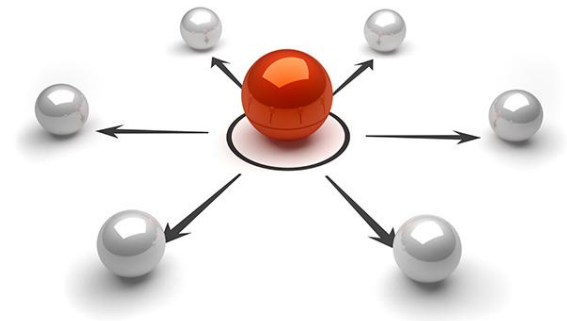
Il regolamento FiDA si applica a diverse entità che operano nel settore finanziario, stabilendo chi può agire come Data Holder o Data User.

Nel novero di tali soggetti viene inclusa una vasta gamma di istituzioni finanziarie e altri fornitori di servizi correlati. Di seguito, alcuni esempi di entità incluse nell'ambito soggettivo del regolamento:

- **Istituti di credito:** banche e altre istituzioni che offrono servizi di credito.
- **Istituti di Pagamento:** comprende i prestatori di servizi di pagamento (PSP), inclusi gli Account Information Service Providers (AISP) e gli istituti di pagamento esentati ai sensi della PSD2.
- **Istituti di Moneta Elettronica:** include gli istituti di moneta elettronica, anche quelli esentati ai sensi della Direttiva 2009/110/CE (EMD2).
- **Imprese di investimento:** aziende che offrono servizi di investimento in vari strumenti finanziari.
- **Fornitori di servizi di crypto-attività:** comprende i Crypto-asset Services Providers (CASP) come definiti dal MiCAR e gli emittenti di crypto-asset definiti come "ART Asset-referenced Token".
- **Imprese di assicurazione e riassicurazione:** compagnie che offrono prodotti assicurativi e riassicurativi.
- **Agenzie di rating del credito:** organizzazioni che forniscono valutazioni di credito.
- **Fornitori di servizi di crowdfunding:** piattaforme che facilitano il crowdfunding.
- **Fornitori di Servizi di Informazioni Finanziarie (FISP):** entità autorizzate a fornire servizi di informazione finanziaria, anche non necessariamente istituti di credito o altri soggetti inclusi nell'ambito soggettivo del FiDA.

Il Regolamento FiDA si applica anche alle branch stabilite nell'UE, poiché queste operano come estensioni della rispettiva istituzione finanziaria.

Quando detengono o utilizzano dati dei clienti nell'ambito dei servizi regolati, rientrano automaticamente nel perimetro dei soggetti obbligati in qualità di data holder e/o data user.



FiDA: Financial Data Access Regulation

La nuova figura dei Financial Information Service Providers (FISP)

Il Regolamento FiDA prevede l'introduzione di una nuova categoria di operatori: i **Financial Information Service Providers (FISP)**.

Si tratta di soggetti che, in modo analogo agli **Account Information Service Providers (AISP)** introdotti con la PSD2, possono accedere ai dati finanziari dei clienti sulla base del loro consenso.

Per poter svolgere questa attività, i FISP devono ottenere una **specifica autorizzazione** rilasciata dall'autorità di vigilanza dello Stato membro in cui hanno sede.

Il regolamento contempla inoltre la possibilità che anche operatori con sede in paesi terzi possano essere autorizzati a operare come FISP all'interno dell'Unione. In questo caso, pur non essendo richiesto l'insediamento di una società o di una succursale nell'UE, è comunque obbligatoria la **nomina di un rappresentante legale** in uno Stato membro.

Tale rappresentante diventa l'interlocutore responsabile del rispetto del quadro normativo europeo e delle obbligazioni derivanti da FiDA.

Requisiti per operare come FISP

- richiedere l'autorizzazione alla **competent authority** dello Stato membro d'origine;
- dimostrare adeguati **requisiti organizzativi, di governance e di sicurezza informatica**;
- garantire politiche trasparenti di uso, conservazione e accesso ai dati;
- disporre di procedure per la gestione dei consensi dei clienti e per la protezione dei dati personali (in coerenza con GDPR e Data Act).

Le autorità dovranno sviluppare **specifici registri pubblici** degli FISP autorizzati, analoghi all'EBA register per la PSD2.

Obblighi di condotta

I FISP non possono utilizzare i dati a cui accedono in modo illimitato:

- l'uso è strettamente limitato ai **servizi richiesti dal cliente**;
- è vietata qualsiasi forma di **riutilizzo non autorizzato** o sfruttamento commerciale dei dati;
- devono garantire **auditability**, tracciabilità delle richieste e prove documentali dell'ottenimento del consenso.

Sono inoltre soggetti a obblighi simili agli intermediari tradizionali in materia di:

- cybersecurity,
- gestione del rischio,
- continuità operativa,
- segnalazioni alle autorità.



FiDA: Financial Data Access Regulation

Gli obblighi dei data holders e dei data users

Il progetto di Regolamento FiDA definisce in modo puntuale i doveri degli **operatori che detengono i dati** (*data holders*) e di quelli che invece li **utilizzano** per erogare servizi ai clienti (*data users*). L'obiettivo è delineare un processo di accesso, trasmissione e gestione dei dati finanziari coerente con i principi di sicurezza, trasparenza e controllo da parte dell'utente.

OBBLIGHI DEI «DATA HOLDERS»

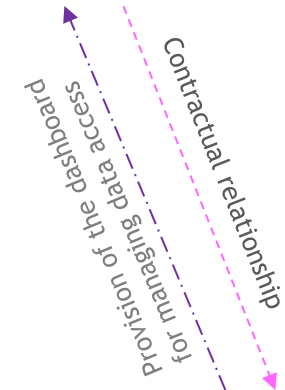


I soggetti che conservano o generano i dati finanziari del cliente devono, tra le altre cose:

- garantire la messa a disposizione dei dati senza ritardi, in modalità **continuativa** e preferibilmente **in tempo reale**;
- fornire le informazioni in un formato standardizzato, basato su schemi riconosciuti e con un livello qualitativo almeno equivalente a quello dei dati “interni”;
- assicurare con i data users una comunicazione protetta, che tuteli integrità, riservatezza e sicurezza durante tutto il processo di trasmissione;
- richiedere al data user una prova valida del **consenso che il cliente** ha espresso per autorizzare l'accesso ai propri dati;
- predisporre, a favore del cliente, un sistema di gestione delle autorizzazioni (permission dashboard) che consenta di monitorare e revocare i permessi concessi.



**Data Holders
(Data Owner)**



Customer



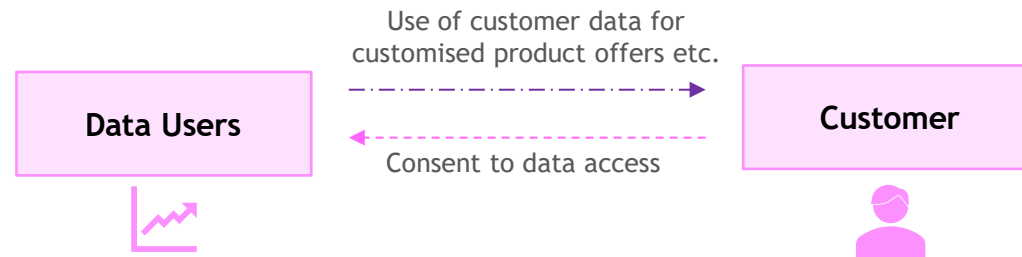
FiDA: Financial Data Access Regulation

Gli obblighi dei data holders e dei data users

OBBLIGHI DEI «DATA USERS»

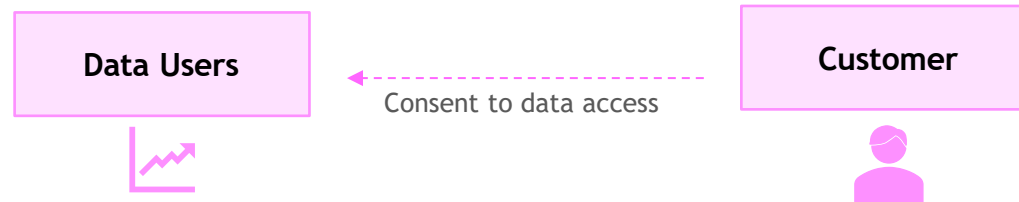
Gli operatori che accedono ai dati, invece, devono rispettare una serie di vincoli, tra cui:

- utilizzare i dati esclusivamente per le finalità connesse al servizio richiesto dal cliente, evitando impieghi ulteriori o incompatibili;
- proteggere segreti commerciali e diritti di proprietà intellettuale quando accedono a informazioni sensibili detenute dai data holders;
- adottare adeguate misure organizzative e tecniche per garantire elevati standard di sicurezza nella conservazione, nel trattamento e nella trasmissione dei dati non personali;
- evitare l'uso dei dati per attività di marketing non autorizzate, potendoli impiegare a tali fini solo nei limiti espressamente consentiti dal cliente.



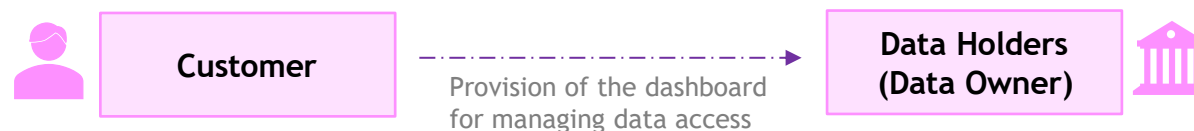
FiDA: Financial Data Access Regulation

Consenso del cliente e permission dashboard



Il Regolamento FiDA prevede che, i ***data users*** potranno avere accesso ai dati finanziari del cliente soltanto con il consenso espresso di quest'ultimo; i dati stessi potranno essere utilizzati soltanto per le finalità e alle condizioni per le quali il consenso è stato concesso e dovranno essere cancellati qualora non più necessari per le suddette finalità, fermo restando che il cliente potrà, sempre e in ogni caso, revocare il proprio consenso originariamente prestato.

I ***data holders*** dovranno mettere a disposizione del cliente la c.d. ***permission dashboard***, una particolare interfaccia informatica da utilizzare per monitorare e gestire i consensi dati dal cliente al ***data user***.



Con la ***permission dashboard*** si potrà fornire al cliente una panoramica su ciascun consenso attivo che è stato dato ai ***data users*** e consentire la revoca o la ri-attivazione del consenso, oltre che fornire un registro dei consensi revocati o scaduti in un termine massimo di due anni.



FiDA: Financial Data Access Regulation

I Financial Data Sharing Schemes (FDSS)

Il FiDA stabilisce che lo scambio dei dati avvenga all'interno dei **Financial Data Sharing Schemes (FDSS)**, ossia strutture di autoregolamentazione costituite dai soggetti che detengono i dati (data holders), da quelli che li utilizzano (data users) e dalle associazioni che rappresentano gli interessi di clienti e consumatori.

A questi organismi è affidato il compito di **definire e governare** una parte significativa degli aspetti operativi necessari per rendere effettivo il modello di open finance.

- Ogni data holder e ogni data user **è tenuto ad aderire ad almeno uno schema di condivisione**, impegnandosi a rispettarne le regole tecniche, procedurali e organizzative relative all'accesso e alla trasmissione dei dati dei clienti.

Nel caso in cui per una specifica tipologia di dati non venga istituito alcun FDSS, la Commissione europea conserva il potere di intervenire direttamente, adottando atti delegati per disciplinare gli elementi essenziali relativi alla condivisione dei dati in quello specifico ambito.

I FDSS dovranno utilizzare **standard tecnici comuni**, come formati dati uniformi (JSON, ISO 20022) e **API standardizzate** per facilitare l'interoperabilità tra data holder e data user. Inoltre, dovranno implementare **protocolli di autenticazione forti** (multi-fattore, token sicuri) e procedure di crittografia avanzata, in linea con i requisiti di sicurezza europei come quelli previsti da DORA, garantendo così accesso sicuro, tracciabile e controllato ai dati finanziari dei clienti.



FiDA: Financial Data Access Regulation

Ulteriori aspetti

- I data users potranno avere accesso ai dati finanziari del cliente anche in regime **transfrontaliero**, sia tramite libera prestazione di servizi sia per stabilimento. In particolare, i **Financial Information Service Providers (FISP)** che intendono operare in Stati membri diversi dal proprio devono notificare alle autorità competenti il loro intento, attraverso una procedura simile al “passaporto” finanziario già previsto in altri settori regolamentati.

La notifica deve includere informazioni dettagliate, come dati identificativi del FISP, numero di autorizzazione, Stati membri di interesse, tipologia di dati richiesti, eventuale appartenenza a FDSS e informazioni su eventuali attività di outsourcing.

- L'EBA è incaricata di istituire e gestire un **registro elettronico centrale**, consultabile pubblicamente per alcune informazioni, che contenga:
 - i FISP autorizzati dalle autorità nazionali;
 - i FISP che hanno notificato l'intenzione di operare cross-border;
 - i FDSS costituiti.

- Il registro sarà aggiornato tempestivamente dalle autorità nazionali competenti in caso di modifiche, revoche di autorizzazioni o cessazione di schemi FDSS, e sarà strutturato per garantire trasparenza e interoperabilità tecnica.

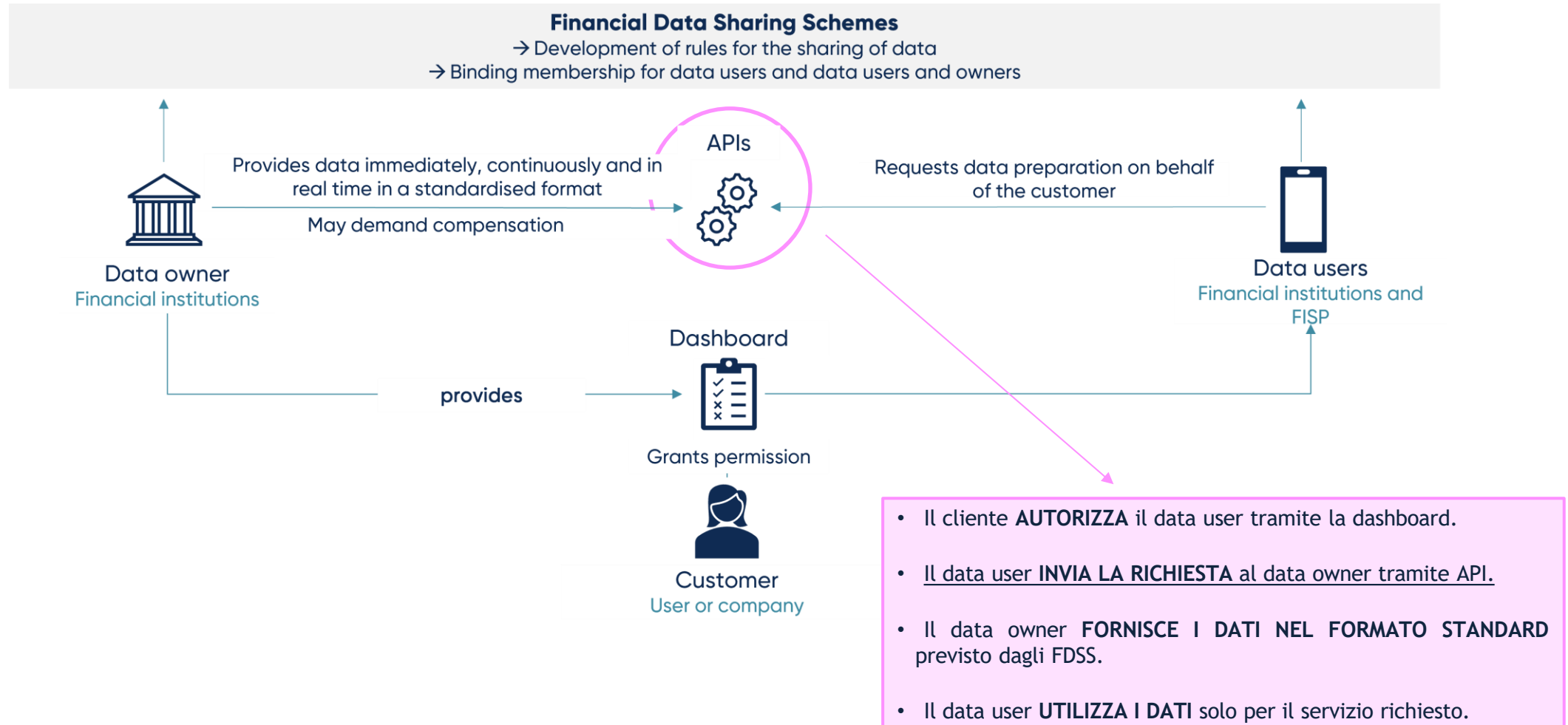
I FISP rientrano inoltre nel perimetro di DORA, dovendo rispettare requisiti stringenti di **cyber-resilienza e sicurezza informatica**, compresi controlli sui sistemi di elaborazione dei dati, autenticazione sicura e protezione contro incidenti informatici. I FDSS definiscono regole tecniche uniformi, modelli di accesso tramite **API standardizzate**, formati dati armonizzati, protocolli di autenticazione robusti e **modelli di compensazione FRAND** per i data holder. Inoltre, i clienti mantengono il controllo sui propri dati tramite una **permission dashboard**, che permette di concedere, limitare o revocare l'accesso anche in contesti transfrontalieri.

- Infine, le autorità nazionali competenti sono abilitate a comminare **sanzioni significative** in caso di violazioni da parte dei FISP o di mancato rispetto delle regole operative dei FDSS.



FiDA: Financial Data Access Regulation

Gli obblighi dei data holders e dei data users



FiDA: Financial Data Access Regulation

Ulteriori aspetti

Task	Dettaglio	Responsabile
ANALISI IMPATTO REGOLATORIO	Verificare se la filiale è “data holder” e il suo ruolo nella condivisione dati transfrontaliera	Compliance / Legale
AFFILIAZIONE FDSS	Adesione a uno schema FDSS e partecipazione ai tavoli tecnici	Compliance / Business Dev
SICUREZZA E RESILIENZA	Adeguamento ai requisiti DORA: multi-factor auth, crittografia, monitoraggio accessi	IT / Security
GESTIONE CONSENSI CLIENTI	Implementare o collegarsi a una <i>permission dashboard</i> per concedere/revocare accesso ai dati	IT / Customer Service
NOTIFICA CROSS-BORDER FISP	Preparare documentazione necessaria per notificare alle autorità competenti l'intenzione di operare in altri Stati membri	Compliance / Legale
TEST API E FLUSSI	Test dei sistemi di condivisione dati con FDSS / data users esterni	IT / Operations
COMUNICAZIONE AI CLIENTI	Informare i clienti sulle nuove modalità di gestione dei dati e sul loro controllo tramite dashboard	Marketing / Customer Service



Alcuni esempi concreti di ciò che si può fare **ORA (in attesa dell'entrata in vigore)**:

- **Analisi dell'impatto regolatorio:** Mappare il ruolo della filiale come data holder e capire quali dati gestisce; Valutare eventuali rischi legali e operativi.
- **Inventario e qualità dei dati:** Catalogare i dati dei clienti e verificare se sono digitalizzati e pronti per l'accesso via API; Identificare eventuali gap di qualità o formati non standard.
- **Preparazione tecnica preliminare:** Valutare infrastrutture IT per gestione dati, sicurezza e logging; Iniziare a familiarizzare con standard API e formati dati comuni.
- **Formazione interna:** Sensibilizzare il personale su FiDA, open finance e gestione consensi clienti.
- **Valutare schemi FDSS disponibili:** Contattare gli FDSS attivi e capire modalità di adesione e requisiti tecnici.
- **Pianificazione della permission dashboard:** Progettare un prototipo o flussi UX per permettere ai clienti di controllare i loro dati.



FiDA: Financial Data Access Regulation

Un futuro incerto: lo stato dell'arte (novembre 2025)

Negli ultimi anni, FiDA è stato presentato come il tassello mancante per completare il passaggio dall'open banking all'open finance: un ecosistema in cui tutti i dati finanziari - non solo quelli dei conti di pagamento - possono essere condivisi in modo sicuro, standardizzato e controllato dal cliente.

L'obiettivo ambizioso è chiaro: **abilitare servizi più efficienti, più personalizzati e più competitivi**, mettendo i dati realmente nelle mani degli utenti.

Tuttavia, al 2025, il percorso di FiDA non è affatto lineare.

Dopo un iniziale entusiasmo regolamentare e politico, il regolamento ha iniziato a generare dibattito, resistenze e richieste di modifica da parte di molte categorie di operatori.

Il sistema FiDA, così come originariamente proposto, richiede agli operatori:

- sistemi avanzati di sicurezza informatica;
- infrastrutture API robuste e standardizzate;
- capacità di garantire un controllo granulare dei consensi;
- processi di auditing e tracciamento di ogni accesso ai dati;
- adesione ai Financial Data Sharing Schemes con regole tecniche onerose.

Questo quadro ha immediatamente sollevato due grandi preoccupazioni.

- Protezione dei dati e rischio di perdita di dati
 - Onere economico e operativo sproporzionato



FiDA: Financial Data Access Regulation

Un futuro incerto: lo stato dell'arte (novembre 2025)

PROTEZIONE DEI DATI E RISCHIO DI LEAKAGE INFORMATIVO

Con la condivisione massiva di dati altamente sensibili (investimenti, assicurazioni, rating, pensioni), il rischio percepito è:

- ☐ fuga di dati ad alto impatto economico;
- ☐ utilizzi secondari non autorizzati;
- ☐ difficoltà di revocare efficacemente i consensi;
- ☐ aumento dei vettori di attacco informatico.

Gli operatori hanno evidenziato come FiDA, nella versione iniziale, rischiasse di diventare un fronte di vulnerabilità sistemica.

ONERE ECONOMICO E OPERATIVO SPROPORZIONATO

Più volte gli operatori hanno segnalato che:

- ☐ i costi delle API;
- ☐ l'adeguamento ai futuri FDSS;
- ☐ gli investimenti in cybersecurity avanzata;
- ☐ la costruzione delle permission dashboard;
- ☐ gli obblighi di rendicontazione;
- ☐ avrebbero avuto un peso particolarmente gravoso su operatori non giganti: banche di medie dimensioni, assicurazioni territoriali, IMEL, fintech emergenti, fondi pensione di taglia ridotta.

Molti hanno quindi parlato apertamente di **ASIMMETRIA**: l'open finance rischiava di favorire gli attori più grandi e tecnologicamente pronti, a scapito dei più piccoli.



FiDA: Financial Data Access Regulation

Un futuro incerto: lo stato dell'arte (novembre 2025)

Queste criticità hanno portato a una progressiva frenata del progetto.

Se a inizio 2024 sembrava avviato verso una rapida approvazione — il Parlamento Europeo aveva già approvato il testo in ECON — le fasi successive hanno rivelato una mancanza di consenso sufficiente a portare il regolamento in plenaria. Il dossier è rimasto in stallo per mesi, fino a uscire di fatto dalla lista delle priorità più immediate della Commissione.



È proprio in questo contesto che, negli ultimi mesi, è emersa una **PROPOSTA DI SEMPLIFICAZIONE DEL FIDA**, pensata per renderlo più snello, meno oneroso e più facilmente applicabile dagli operatori.

La proposta di semplificazione introduce alcuni elementi di forte novità.

- La prima, probabilmente la più significativa, riguarda l'esclusione delle grandi imprese dal perimetro soggettivo del regolamento. Questo significa che l'obbligo di condivisione dei dati si concentrerebbe su clienti retail e PMI, limitando così sia l'impatto operativo sui data holder sia il volume di dati da gestire in termini di sicurezza. È un cambiamento importante, che riflette la consapevolezza che le imprese di grandi dimensioni hanno già oggi capacità tecnologiche e contrattuali tali da dialogare direttamente con gli operatori, senza necessità di un framework normativo obbligatorio.
- La seconda grande novità riguarda la limitazione temporale dei dati condivisi.

Non verrebbe più richiesto di rendere disponibili dati molto remoti nel tempo o relativi a rapporti non più attivi. Anche questo è un segnale concreto di attenzione alla privacy, alla proporzionalità e alla riduzione dei costi di implementazione.



FiDA: Financial Data Access Regulation

Un futuro incerto: lo stato dell'arte (novembre 2025)

Altro elemento chiave è rappresentato dall' esclusione dei *gatekeeper* digitali, cioè i grandi operatori tecnologici designati come tali dal Digital Markets Act, dalla possibilità di diventare FISP.

Questa misura ha un significato strategico evidente: evitare che pochi player extra-settore – con risorse finanziarie enormi e capacità di scala – possano dominare il nuovo mercato dei dati finanziari.

Infine, la Commissione propone un approccio più graduale per standardizzazione e interoperabilità, prevedendo un quadro tecnico più leggero e più tempi di valutazione prima di un'eventuale estensione del perimetro.

Nel complesso, questa proposta nasce con un duplice obiettivo:

da un lato rilanciare il processo legislativo, che si era arenato; dall'altro ridurre i rischi e i costi che avevano frenato l'adozione del regolamento nella sua forma originaria.



Nel 2026 ci aspettiamo un'accelerazione decisiva sull'iter del regolamento FiDA: il nuovo testo semplificato riduce le resistenze politiche ed economiche e potrebbe consentire alla Commissione, al Parlamento e al Consiglio di trovare un accordo entro fine anno.

Se questo scenario si confermerà, FiDA potrebbe entrare formalmente in vigore già entro la fine del 2025 o nei primi mesi del 2026, avviando poi una fase di transizione che porterà alle prime applicazioni operative nel biennio successivo.



- Il Regolamento FiDA – la condivisione dei dati finanziari
- **Operazioni di pagamento non autorizzate: le aspettative di vigilanza della Banca d'Italia**

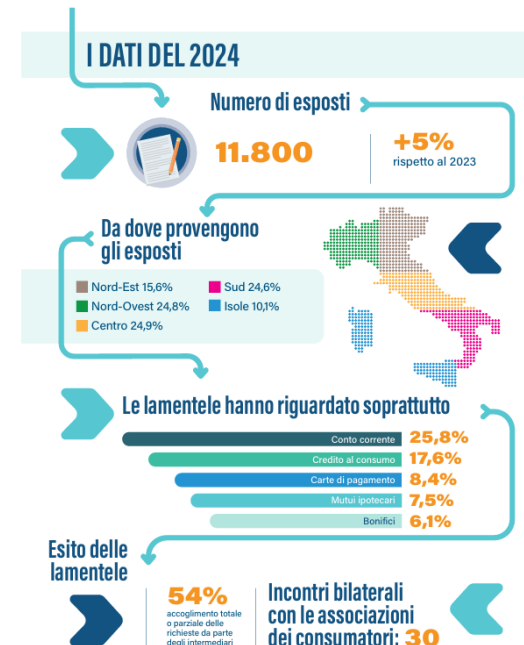
Disconoscimento operazioni non autorizzate

Relazione sugli esposti dei clienti delle banche e delle finanziarie

Nel 2024 la Banca d'Italia ha ricevuto oltre 11.800 esposti (5 per cento in più rispetto al 2023) relativi a lamentele della clientela nei confronti di banche e finanziarie.

L'aumento è riconducibile principalmente a blocchi dell'operatività di carte e servizi di pagamento disponibili mediante home banking (gli esposti in materia sono più che triplicati) e a **problemi in fase di esecuzione di bonifici** (ad es. non corretta esecuzione delle disposizioni impartite dalla clientela e transazioni non autorizzate).

Nella «Relazione sugli esposti dei clienti delle banche e delle finanziarie» presentata a Giugno 2025 (con i dati riferiti al 2024) la Banca d'Italia ha precisato, con riferimento alle truffe, che **«sono spesso volte a catturare le credenziali di accesso ai servizi bancari online per effettuare operazioni di pagamento non autorizzate dal cliente»**.



Relazione sugli esposti
dei clienti delle banche
e delle finanziarie

anno 2024

Numero 5 - giugno 2025

«[...] in caso di pagamenti non autorizzati dal cliente, è possibile disconoscere le operazioni addebitate senza autorizzazione e chiederne il rimborso, ferma la possibilità di denunciare l'accaduto alle forze dell'ordine. L'intermediario è di regola tenuto a rimborsare l'importo disconosciuto al più tardi entro la fine della giornata operativa successiva a quella in cui riceve il disconoscimento. Il rimborso non è dovuto se l'intermediario prova: (a) che l'operazione è stata autenticata, correttamente registrata e contabilizzata, senza subire conseguenze a seguito del malfunzionamento delle procedure; (b) che il cliente ha agito in modo fraudolento oppure, con dolo o colpa grave, non ha adempiuto ai propri obblighi».



Disconoscimento operazioni non autorizzate

Le aspettative di Banca d'Italia



Disconoscimenti di operazioni di pagamento non autorizzate. Comunicazione al sistema.

Negli ultimi anni il comparto dei servizi di pagamento è stato interessato da rilevanti cambiamenti, legati al recepimento di importanti normative europee (tra cui la Direttiva PSD2) e alla diffusione di nuove tecnologie, che hanno contribuito a un profondo mutamento delle abitudini di pagamento della clientela (caratterizzate dalla progressiva riduzione dell'uso del contante), alla digitalizzazione dei servizi e alla diffusione dell'e-commerce, anche per effetto dell'emergenza pandemica.

In tale contesto, assume maggiore importanza l'esigenza di garantire alla clientela il diritto di disconoscere le operazioni non autorizzate e di ottenere i dovuti rimborsi.

Il D.lgs. 11/2010 individua i presupposti in base ai quali l'utente ha diritto a essere rimborsato dal prestatore di servizi di pagamento (PSP) dell'importo dell'operazione disconosciuta¹ e definisce le tempistiche e le modalità di tale rimborso; ciò, con l'obiettivo di sterilizzare gli effetti negativi per il cliente dell'addebito legato all'operazione non autorizzata², contribuendo a rafforzare la tutela della clientela e favorire la fiducia verso i servizi di pagamento.

Il rispetto di questa disciplina è essenziale ai fini di tutela della clientela, oltre a rilevare anche per i profili di rischio operativo degli intermediari e per il regolare funzionamento, l'affidabilità e l'efficienza del sistema dei pagamenti.

La Banca d'Italia ha quindi condotto approfondimenti sui presidi approntati dai PSP in materia, con iniziative di vigilanza ispettiva e cartolare. All'esito delle analisi svolte, è emersa l'opportunità di fornire indicazioni per garantire l'omogeneità delle condotte tenute dagli operatori e il loro allineamento al dato normativo nonché per favorire la convergenza verso prassi più attente alla qualità delle relazioni con la clientela. Gli approfondimenti hanno tenuto conto anche del contenzioso affluito all'Arbitro Bancario Finanziario (ABF) e degli esposti alla Banca d'Italia, oltre che delle segnalazioni delle associazioni dei consumatori.

In particolare, sono state riscontrate le seguenti problematiche:

- **rifiuto non fondato del rimborso**, da ricondurre principalmente a criteri di valutazione dei disconoscimenti non in linea con le regole che definiscono il regime di responsabilità dei PSP e dei clienti nell'uso degli strumenti di pagamento;
- **carenze nell'esecuzione dei rimborsi**, in relazione sia ai tempi di evasione del disconoscimento – spesso appesantiti da adempimenti a carico dei clienti non richiesti dalla disciplina di settore – sia al ripristino dello stato del conto di pagamento a fronte di un'operazione non autorizzata;
- **lacune nell'informativa alla clientela**, tanto con riferimento alla rappresentazione delle modalità con cui il cliente è tenuto a notificare il disconoscimento del pagamento non autorizzato al PSP, quanto alla comunicazione del motivo del diniego del rimborso;

¹ Ai sensi degli artt. 10 e 12 del D.lgs. 11/2010, il PSP deve di norma assicurare il rimborso quando l'operazione di pagamento disconosciuta non è stata autorizzata con i più elevati standard di sicurezza previsti dalla regolamentazione, rappresentati dalla cd. "autenticazione forte" (*strong customer authentication* - SCA). Quando quest'ultima è invece prevista, il PSP ha facoltà di non rimborsare l'utente se ha accertato che l'operazione disconosciuta è stata causata dal mancato rispetto degli obblighi posti a carico dell'utente stesso (per esempio, la custodia dello strumento di pagamento) in ragione di suoi comportamenti caratterizzati da dolo o colpa grave. In ogni caso, il PSP ha sempre il diritto di non rimborsare ove presuma che la richiesta di disconoscimento del cliente derivi da un suo tentativo di frode ai danni del PSP stesso. Su tale ultimo aspetto, cfr. la [comunicazione al sistema di questo Istituto del 30 ottobre 2023](#).

² Ai sensi dell'art. 11 del D.lgs. 11/2010, il rimborso delle operazioni disconosciute va effettuato al più tardi entro la giornata lavorativa successiva alla richiesta e, laddove l'operazione abbia comportato l'addebito di un conto di pagamento, in maniera tale da riportare quest'ultimo nello stato in cui si sarebbe trovato se il pagamento non avesse avuto luogo, assicurando che la data valuta dell'accredito non sia successiva a quella dell'addebito dell'importo.

Richiamo di attenzione della Banca d'Italia sulla necessità di rispettare le norme relative al disconoscimento di operazioni di pagamento non autorizzate

Con la comunicazione del 17 giugno 2024, la Banca d'Italia richiama l'attenzione degli operatori sulla necessità di rispettare le norme relative al disconoscimento di operazioni di pagamento non autorizzate.

L'obiettivo è garantire **trasparenza e correttezza nei rapporti con la clientela**, prevenendo abusi e tutelando sia gli utenti sia la stabilità del sistema dei pagamenti.

La comunicazione nasce in un contesto di **profondo cambiamento del settore dei servizi di pagamento**, determinato da diversi fattori:

- il **recepimento di normative europee rilevanti**, tra cui la **Direttiva PSD2**, che ha introdotto regole più rigorose sulla sicurezza delle transazioni e sulla protezione dei consumatori;
- **l'adozione di nuove tecnologie**, che hanno reso i pagamenti più rapidi e digitalizzati, modificando le modalità con cui la clientela effettua transazioni;
- **la diffusione dell'e-commerce** e la **riduzione dell'uso del contante**, fenomeni accelerati anche dall'emergenza pandemica.

Tali trasformazioni hanno aumentato la complessità della gestione delle operazioni di pagamento e reso più urgente l'esigenza di procedure chiare ed efficaci per il disconoscimento delle transazioni non autorizzate, così da tutelare la clientela e rafforzare la fiducia nel sistema finanziario.



Disconoscimento operazioni non autorizzate

Tutela della clientela nelle operazioni non autorizzate

In questo contesto, risulta fondamentale tutelare il diritto della clientela a disconoscere operazioni di pagamento non autorizzate e a ricevere i rimborsi spettanti. Il D.lgs. 11/2010 definisce in modo chiaro i presupposti secondo cui l'utente può richiedere il rimborso al prestatore di servizi di pagamento (PSP) dell'importo relativo all'operazione contestata, stabilendo al contempo le **modalità e le tempistiche** entro cui tale rimborso deve essere effettuato.

Per verificare l'effettiva applicazione di queste disposizioni, la **Banca d'Italia** ha condotto approfondimenti sui sistemi di controllo e sui presidi operativi messi in atto dai PSP, attraverso **attività di vigilanza ispettiva e cartolare**.

Dall'analisi è emersa la necessità di fornire indicazioni operative e linee guida, al fine di:

- garantire **coerenza e uniformità** nelle condotte degli operatori;
- assicurare il pieno rispetto del quadro normativo vigente;
- promuovere pratiche più attente alla **qualità delle relazioni con la clientela**, rafforzando la trasparenza e la fiducia nei servizi di pagamento.

In sostanza, l'iniziativa dell'Autorità mira a **armonizzare i comportamenti dei PSP**, prevenendo discrepanze e ritardi nei rimborsi, e a favorire una gestione più efficace e responsabile delle operazioni contestate.

- Definisce i presupposti che legittimano l'utente a contestare un'operazione (ad esempio quando non l'ha autorizzata o non ne è responsabile).
- Attribuisce al PSP l'obbligo di rimborsare immediatamente l'importo dell'operazione non riconosciuta, salvo che dimostri la corretta autenticazione e l'assenza di anomalie.
- Specifica le tempistiche per la gestione della contestazione, stabilendo che il rimborso deve avvenire senza ritardi ingiustificati e, in ogni caso, entro la fine della giornata operativa successiva.
- Disciplina le modalità di valutazione della contestazione, chiarendo che l'onere della prova ricade sul PSP, non sul cliente.



Disconoscimento operazioni non autorizzate

Tutela della clientela nelle operazioni non autorizzate

Mancanza di consenso

- Un'operazione può essere considerata **non autorizzata** se l'utente non ha dato il **consenso** (ossia non ha accettato l'operazione nel modo concordato con il PSP). Il consenso deve essere prestato secondo le modalità stabilite nel contratto quadro con il prestatore di servizi di pagamento.

Prova a carico del prestatore di servizi di pagamento (PSP)

- Se l'utente dichiara che un'operazione non è stata da lui autorizzata, **l'onere della prova** ricade sul PSP. Deve dimostrare che l'operazione è stata effettivamente autorizzata, correttamente registrata e contabilizzata. In particolare, il PSP può dover dimostrare che non ci sono stati malfunzionamenti nelle sue procedure.

Autenticazione debole o carente

- Se il prestatore non ha utilizzato un sistema di autenticazione forte (strong customer authentication, SCA), può risultare più difficile per il PSP dimostrare che l'utente ha autorizzato l'operazione.
- L'autenticazione forte richiede almeno due elementi indipendenti fra "conoscenza" (es. password), "pos-sesso" (es. telefono) e "inerenza" (es. impronta).

Comportamento fraudolento o colpa grave dell'utente

- Il rimborso può essere sospeso **solo in presenza di un "motivato sospetto di frode"** da parte dell'utente.
- Ma non qualsiasi comportamento è considerato "frode": la Banca d'Italia chiarisce che non basta la semplice negligenza o colpa nell'uso (ad esempio, non aver custodito correttamente le credenziali). Serve un comportamento con elementi che manifestino intenzione di ingannare il PSP. Se il PSP sospetta frode, deve informare **immediatamente per iscritto** la Banca d'Italia.

Tempistica di contestazione da parte dell'utente

- L'utente deve notificare il disconoscimento "senza indugio" al PSP secondo modalità e tempistiche previste dal contratto o dalla normativa. C'è un termine massimo: di solito il disconoscimento deve essere fatto entro **13 mesi** dall'addebito, salvo casi particolari.

PRESUPPOSTI
PER
CONTESTARE
UN'OPERAZIONE
DI PAGAMENTO



Disconoscimento operazioni non autorizzate

Risultati delle verifiche della Banca d'Italia sui PSP

La Banca d'Italia ha svolto un'approfondita attività di analisi sui presidi adottati dai prestatori di servizi di pagamento (PSP), attraverso interventi di vigilanza sia ispettiva sia cartolare.

Dalle verifiche effettuate è emersa l'esigenza di fornire indicazioni operative volte a uniformare i comportamenti degli operatori, assicurare la piena aderenza al quadro normativo e promuovere prassi maggiormente orientate alla tutela e alla qualità del rapporto con la clientela.

L'Autorità ha rilevato alcune criticità nelle procedure interne relative alla gestione dei disconoscimenti di operazioni non autorizzate, tra cui:

- **Rifiuti di rimborso non adeguatamente motivati o privi di fondamento;**
- **Carenze nell'esecuzione dei rimborsi**, sia in termini di rapidità nella lavorazione dei disconoscimenti, sia nel tempestivo ripristino della situazione contabile del cliente;
- **Informativa carente o non sufficientemente chiara**, che può ostacolare la comprensione da parte della clientela delle tutele a loro disposizione;
- **Inadeguatezza dei sistemi di tokenizzazione delle carte**, soprattutto quando utilizzati tramite applicazioni di provider esterni (wallet digitali), con potenziali impatti sulla sicurezza dei pagamenti sia in presenza fisica sia online.



Disconoscimento operazioni non autorizzate

Aspettative di Vigilanza sulla Gestione dei Disconoscimenti

La Banca d'Italia invita i prestatori di servizi di pagamento a effettuare una valutazione autonoma e approfondita dell'adeguatezza dei propri processi, delle procedure interne e delle prassi operative, verificandone la coerenza sia con il quadro normativo vigente sia con le aspettative dell'Autorità.

In tale prospettiva, l'Autorità si attende che gli operatori assicurino:

- ❑ l'adozione di una policy interna dedicata alla gestione dei disconoscimenti, pienamente conforme alle disposizioni del D.lgs. 11/2010: la banca o il PSP deve avere regole interne chiare e formalizzate per gestire le operazioni contestate dai clienti;
- ❑ lo svolgimento dell'istruttoria sulle contestazioni nel rispetto dei criteri normativi che disciplinano la ripartizione delle responsabilità tra PSP e cliente: l'istruttoria deve rispettare le regole che stabiliscono chi è responsabile: ad esempio, se l'operazione è stata realmente non autorizzata o se ci sono responsabilità del cliente. L'obiettivo è garantire che il rimborso o il rifiuto sia giustificato e conforme alla legge, evitando decisioni arbitrarie;
- ❑ l'utilizzo di strumenti valutativi non meccanici, basati su parametri sufficientemente dettagliati da consentire una verifica concreta dell'eventuale dolo o colpa grave dell'utente;
- ❑ la predisposizione di iniziative formative e di sensibilizzazione rivolte al personale, in particolare quello a diretto contatto con la clientela, così da rafforzare la cultura interna e supportare una corretta gestione delle richieste e dei reclami;
- ❑ la definizione di tempistiche chiare e compatibili con gli obblighi di rimborso previsti dall'art. 11, comma 1, del D.lgs. 11/2010: le procedure interne devono prevedere **tempi di gestione certi** per la valutazione delle contestazioni.

REGOLE
INTERNE E
TEMPI DI
GESTIONE
CERTI !



Disconoscimento operazioni non autorizzate

Risultati delle verifiche della Banca d'Italia sui PSP

- ❑ ove sia stato addebitato un conto di pagamento, siano previsti meccanismi che tengano conto dell'esigenza di riportare quest'ultimo nello stato in cui si sarebbe trovato se l'operazione non avesse avuto luogo e che, in particolare, la data valuta dell'accredito non sia successiva a quella dell'addebito (art. 11, c. 1, D.lgs. n. 11/2010);
- ❑ la documentazione di trasparenza contenga un'informativa adeguata ad assicurare una piena consapevolezza della clientela in merito al riconoscimento dei propri diritti e alle modalità di adempimento dei propri doveri;
- ❑ sia rafforzata la trasparenza verso il cliente circa il diritto dei PSP di recuperare le somme inizialmente rimborsate qualora, all'esito di un'eventuale successiva istruttoria, emerga l'autorizzazione dell'operazione;
- ❑ le comunicazioni al cliente successive al disconoscimento siano redatte in un linguaggio chiaro e comprensibile e rechino informazioni esaustive con riguardo alle motivazioni inerenti al rigetto delle richieste di rimborso e alla possibilità di far valere i propri diritti nelle sedi competenti;
- ❑ le procedure di tokenizzazione delle carte della clientela siano disegnate in linea con le modalità di autenticazione previste dal Regolamento delegato (UE) 2018/389;
- ❑ i PSP valutino i reclami anche alla luce delle posizioni dell'Arbitro Bancario Finanziario, verificando se la questione sottoposta dal cliente rientri in fattispecie analoghe a quelle già decise e considerando le soluzioni adottate in tali casi anche in **relazione alla gestione delle segnalazioni della clientela** (reclami, esposti, ricorsi ABF) in materia di **operazioni non autorizzate**.



Disconoscimento operazioni non autorizzate

Iter di adeguamento

Nel paragrafo finale della **Comunicazione**, la Banca d'Italia introduce un aspetto centrale: le tempistiche entro cui i prestatori di servizi di pagamento devono adeguarsi alle indicazioni fornite.

Questo punto, apparentemente breve, in realtà racchiude **implicazioni operative molto importanti.**

AUTOVALUTAZIONE IMMEDIATA

La Banca d'Italia richiede ai PSP di avviare **subito** un processo di autovalutazione, che deve:

- analizzare l'intero sistema di gestione dei disconoscimenti;
- verificare policy, procedure, tempi operativi e sistemi informatici;
- controllare la coerenza tra prassi operative e quanto richiesto dal D.lgs. 11/2010 e dalla stessa Comunicazione.

Questa autovalutazione non deve essere superficiale: deve essere formale, documentata, completa.
La banca deve cioè essere in grado di mostrare, in caso di richiesta, la mappatura delle aree analizzate, le criticità emerse e la valutazione dei rischi collegati.

PIANO DI INTERVENTI CORRETTIVI

Se dall'autovalutazione emergono lacune o non conformità, la Banca d'Italia si aspetta che il PSP:

- identifichi con precisione gli ambiti in cui intervenire,
- definisca un *piano di azione*,
- stabilisca responsabilità, scadenze e modalità di attuazione.

Non si tratta quindi di una semplice "intenzione" di adeguamento, ma di un piano strutturato che coinvolge tutte le Funzioni.

Secondo la Comunicazione, questi interventi devono essere sviluppati con il *contributo delle funzioni di controllo*, che diventano garanti della corretta impostazione del processo.



Disconoscimento operazioni non autorizzate

Iter di adeguamento

La Banca d'Italia fissa una scadenza chiara: tutte le azioni correttive devono essere completate entro 12 mesi dalla pubblicazione della Comunicazione.

Ciò significa che entro un anno:

- il PSP deve aver concluso l'autovalutazione;
- deve aver progettato e implementato tutti gli interventi necessari;
- deve aver aggiornato policy, procedure, sistemi informativi e formazione del personale;
- deve aver introdotto canali di comunicazione con il cliente più efficaci;
- deve garantire la piena conformità a tutte le aspettative dell'Autorità.

Questa scadenza è molto significativa perché la Comunicazione non è una semplice “raccomandazione”: è un documento di richiamo formale, che richiede interventi concreti e verificabili.



Il periodo attuale (novembre 2025) è quello in cui l'Autorità potrebbe già aver iniziato richieste di chiarimento, controlli o follow-up verso chi non si è adeguato.



Disconoscimento operazioni non autorizzate

Conclusioni

A distanza di oltre cinque mesi dalla scadenza del 17 giugno 2025, il quadro che emerge è chiaro: la gestione dei disconoscimenti di operazioni non autorizzate rappresenta ormai un ambito **strategico**, osservato con estrema attenzione dalla Banca d'Italia.

La Comunicazione del 17 giugno 2024, pur non configurando nuove norme, ha fissato un insieme di **aspettative operative e comportamentali** a cui tutti i PSP sono tenuti a conformarsi. Oggi, la Vigilanza considera tali aspettative come standard minimi di riferimento, verificandone l'applicazione concreta nelle attività quotidiane degli intermediari.

Per le branch estere che operano sul mercato italiano, questo significa garantire che procedure, controlli, formazione del personale e qualità del servizio siano pienamente allineati al contesto regolamentare nazionale.

Particolare attenzione è richiesta sulla tempestività dei rimborsi, sulla chiarezza delle comunicazioni ai clienti e sulla capacità di gestire le richieste in modo uniforme e trasparente.

Nel panorama attuale, l'adeguamento non è più solo un esercizio formale, ma un **elemento essenziale** per ridurre il rischio operativo, prevenire contenziosi con l'ABF e preservare la fiducia dei consumatori nei servizi di pagamento. *La sfida che si apre per il 2026 è continuare a consolidare processi, presidiare l'evoluzione tecnologica e garantire una tutela sempre più efficace, in coerenza con le aspettative dell'Autorità e con le migliori pratiche del mercato.*

La Banca d'Italia punta a:

- uniformare il comportamento degli intermediari;
- garantire tempi certi per i clienti;
- limitare i contenziosi con l'Arbitro Bancario Finanziario;
- ridurre il rischio operativo e reputazionale delle banche;
- rafforzare l'affidabilità e la sicurezza del sistema dei pagamenti.





CONTACTS

Corso Europa, 13 - 20122 Milano

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

segreteria@consiliabm.com | info@consiliabm.com