



# Disconoscimento delle operazioni di pagamento non autorizzate

La comunicazione Banca d'Italia  
del 17 giugno 2024



# Comunicazione di Banca d'Italia del 17 giugno 2024 sul rimborso delle operazioni non autorizzate

## Ambito e scopo dell'intervento di Banca d'Italia

La Banca d'Italia, il 17 giugno 2024, ha pubblicato una **Comunicazione** per **richiamare** l'attenzione dei prestatori di servizi di pagamento (**PSP**) sull'esigenza di adottare **condotte conformi** alle regole in materia e **improntate alla correttezza** dei rapporti con la clientela.

In particolare, al fine di **rafforzare la fiducia degli utenti nei servizi di pagamento**, Banca d'Italia ritiene **essenziale** garantire **il diritto di disconoscere operazioni non autorizzate e ottenere tempestivamente i relativi rimborsi**.

... nel caso in cui sia stata eseguita **un'operazione di pagamento non autorizzata**, il prestatore di servizi di pagamento **rimborso al pagatore l'importo dell'operazione medesima immediatamente e in ogni caso al più tardi entro la fine della giornata operativa successiva** a quella in cui prende atto dell'operazione o riceve una comunicazione in merito **a meno che** il prestatore di servizi di pagamento del pagatore **abbia ragionevoli motivi per sospettare una frode e comunichi tali motivi** per iscritto alla pertinente autorità nazionale competente (i.e. **alla Banca d'Italia**)...



L'art. 11 del D.lgs. 11/2010 è frutto del recepimento dell'art. 73 della Direttiva PSD 2.



Il PSR propone un aggiornamento del dettato normativo (focus)

# Comunicazione di Banca d'Italia del 30 ottobre 2023 sull'obbligo di segnalazione di cui all'art. 11 del D.lgs. n. 11/2010

Il 30 ottobre 2023, la **Banca d'Italia** ha pubblicato una Comunicazione con cui ha fornito **precisazioni** sui **presupposti della sospensione del rimborso** delle **operazioni non autorizzate** da parte dei PSP e sulle modalità con cui comunicare tale sospensione.

I PSP hanno l'obbligo di **rimborsare immediatamente** al pagatore l'importo di un'operazione non autorizzata (ai sensi dell'art. 11, c. 1, del D.lgs. n. 11/2010).

In particolare, **il rimborso deve essere:**

- (i) integrale:** pari all'**intero importo** dell'operazione non autorizzata;
- (ii) immediato:** deve avvenire **immediatamente** e comunque **non oltre la fine della giornata operativa successiva** a quella in cui il PSP è venuto a conoscenza dell'operazione non autorizzata;
- (iii) non svantaggioso:** la **data valuta** dell'accredito del rimborso **non** deve essere **successiva alla data di addebito** dell'importo.

Il PSP può dimostrare successivamente che l'operazione di pagamento era autorizzata; in tal caso, **ha il diritto di chiedere e ottenere la restituzione dell'importo rimborsato** (art. 11, commi 1 e 2-bis, del Decreto).

Un'**eccezione all'obbligo di rimborso** si verifica quando il **PSP ha un motivato sospetto** che l'operazione non autorizzata sia il risultato di un **comportamento fraudolento** da parte dell'utente, caratterizzato da **elementi specifici** che indicano l'intenzione dell'utente di **ingannare** il PSP il quale **non** può consistere nella **mera inosservanza dolosa o colposa degli obblighi di comunicazione e custodia** previsti per l'utente (art. 7 Decreto).

In caso di **sospensione del rimborso**, il PSP deve **comunicarlo immediatamente** per iscritto alla Banca d'Italia (art. 11, comma 2, Decreto).

Se il PSP **dispone di elementi** che provano il **comportamento fraudolento, doloso o gravemente colposo dell'utente** entro la fine della giornata operativa successiva alla scoperta dell'operazione non autorizzata, **non sussistono i presupposti per la sospensione del rimborso e per la relativa segnalazione alla Banca d'Italia.**

# Autorizzazione delle operazioni e frodi informatiche

Nonostante l'introduzione della **Strong Customer Authentication – SCA** ad opera della PSD2, permangono significative problematiche in relazione alle **frodi connesse agli strumenti di pagamento**, il cui numero è cresciuto negli ultimi anni.

«**Le frodi informatiche sono volte a catturare le credenziali di accesso ai servizi bancari online per effettuare operazioni di pagamento non autorizzate dal cliente.**» (Relazione sull'attività dell'Arbitro Bancario Finanziario nell'anno 2023)

Alle tecniche di **frode** “tradizionali” si sono dapprima affiancate e poi sostituite le tecniche di c.d. social engineering che costituiscono il mezzo utilizzato da parte di frodatori per disporre, o più frequentemente far disporre allo stesso utente, operazioni di pagamento che vedono come beneficiari (finali) gli stessi frodatori.

## Phishing

Tipologia di frode effettuata tramite un'e-mail o un rinvio ad un sito web “civetta” con il logo contraffatto di un istituto di credito o di una qualsiasi società commerciale in cui il pagatore viene invitato a inserire, in appositi campi, i propri dati riservati per rubarli.

## Vishing

Truffa simile al phishing, che avviene per telefono, tramite il quale il frodatore cerca di indurre la vittima a fornire dati personali, fingendosi un dipendente / incaricato della banca o del PSP. Per concretizzare tale tecnica, il terzo frodatore utilizza tecniche di persuasione, di inganno ed in grado di ledere la capacità cognitiva e di giudizio della vittima.

## Smishing

Forma di phishing che utilizza messaggi di testo inviati su telefoni cellulari, per indurre in errore i clienti, invitandoli ad aprire link dannosi con lo scopo di sottrarre loro i dati personali o indurli a comunicare le proprie credenziali/informazioni personali.

## Spoofing

Fattispecie in cui i frodatori riescono a camuffare la provenienza della e-mail o dell'sms “civetta”, facendola comparire all'interno di un thread di messaggi, autentici e legittimi, intercorsi con il proprio intermediario.

# Focus: la nuova formulazione normativa proposta all'interno del Payments Service Regulation (PSR)

Nel progetto di **revisione della disciplina**, emerge chiaramente la **necessità di rafforzare la tutela degli utenti contro il rischio di frode**, in quanto i processi di autenticazione forte non sempre possono eliminare tale rischio.

Infatti, la maggior parte delle **frodi di "ingegneria sociale"** (come phishing, vishing, smishing e spoofing) **avviene prima dell'applicazione dell'autenticazione forte**.

Si riconosce che la **distinzione tra operazioni autorizzate e non autorizzate è sempre più complessa da applicare nella pratica**.

Non è più possibile limitare i rimborsi alle sole operazioni non autorizzate.



Per questo motivo, a livello europeo, è stata **proposta una nuova definizione di "autorizzazione" all'esecuzione di operazioni di pagamento**.

**Per essere considerata valida, un'autorizzazione deve essere data con piena cognizione dall'utente e senza manipolazioni.**

In sostanza, il nuovo Regolamento PSR potrebbe introdurre una suddivisione in tre categorie: operazione autorizzata, operazione autorizzata oggetto di frode, e operazione non autorizzata.

Il legislatore europeo propone di disciplinare le operazioni oggetto di "frode con furto di identità" con il nuovo articolo 59 del Regolamento PSR.

Inoltre, in caso di "**colpa grave**" dell'utente, **non** ci sarebbe **diritto al rimborso** per le operazioni autorizzate fraudolente.

La colpa grave è definita come un **comportamento significativamente negligente, valutato in base a tutte le circostanze concrete e alle specifiche del diritto nazionale**.

Pur individuando alcuni casi sintomatici di colpa grave, il legislatore europeo intende affidare **all'EBA l'adozione di orientamenti specifici relativi a questo concetto**.

# Focus: la nuova formulazione normativa proposta all'interno del Payments Service Regulation (PSR)



Art. 56 [ . . ] nel caso di un'operazione di pagamento non autorizzata il prestatore di servizi di pagamento del pagatore **rimborsa al pagatore l'importo dell'operazione di pagamento non autorizzata, immediatamente e in ogni caso al più tardi entro la fine della giornata operativa successiva** a quella in cui prende atto dell'operazione non autorizzata o riceve una notifica in merito, a meno che il **prestatore di servizi di pagamento del pagatore abbia ragionevoli motivi per sospettare una frode** e comunichi tali motivi per iscritto alla pertinente autorità nazionale competente.

Qualora abbia **ragionevoli motivi per sospettare una frode** commessa dal pagatore, il prestatore di servizi di pagamento del pagatore, **entro 10 giornate operative successive** a quella in cui prende atto dell'operazione o riceve una notifica in merito, compie una delle azioni seguenti:

- **rimborsa al pagatore l'importo dell'operazione di pagamento non autorizzata** se il prestatore di servizi di pagamento del pagatore ha concluso, dopo ulteriori indagini, che il pagatore non ha commesso alcuna frode;
- fornisce una motivazione del rifiuto del rimborso e indica gli organismi ai quali il pagatore può deferire la questione [ . . ]

Fonte: proposta di Regolamento del parlamento europeo e del consiglio relativo ai servizi di pagamento nel mercato interno e che modifica il regolamento (UE) n. 1093/2010

## Inoltre

**Cons. 79** [ . . . ] I consumatori dovrebbero essere adeguatamente tutelati nel contesto di determinate operazioni di pagamento fraudolente che hanno autorizzato senza che ne conoscessero la natura fraudolenta [ . . . ] I casi di "spoofing" in cui i truffatori fingono di essere dipendenti del prestatore di servizi di pagamento di un cliente [ . . . ] indurli a compiere alcune azioni sono purtroppo sempre più diffusi nell'Unione [ . . . ]. Pertanto non è più possibile limitare i rimborsi alle sole operazioni non autorizzate, come prevedeva la direttiva (UE) 2015/2366. Aprire a un diritto di rimborso sistematico ogni operazione fraudolenta, autorizzata o non autorizzata, sarebbe tuttavia sproporzionato e finanziariamente molto costoso...

**Cons. 80** [ . . . ] Non appena viene a conoscenza di essere stato vittima di questo tipo di frode, il consumatore dovrebbe segnalare senza indebito ritardo l'incidente alla polizia, preferibilmente tramite procedure per i reclami online, ove messe a disposizione dalla polizia, e al suo prestatore di servizi di pagamento, fornendo tutte le prove a sostegno necessarie. Non dovrebbe essere concesso alcun rimborso qualora tali condizioni procedurali non siano soddisfatte.

# Comunicazione di Banca d'Italia del 17 giugno 2024 - Principali criticità riscontrate sui disconoscimenti



**Rifiuto non fondato del rimborso**, dovuto all'**errata applicazione dei criteri di valutazione** dei disconoscimenti, **non coerente con il regime di responsabilità** dei PSP e dei clienti nell'uso degli strumenti di pagamento.



**Carenze nell'esecuzione dei rimborsi**, in relazione ai **tempi di evasione del disconoscimento** – spesso appesantiti da adempimenti non richiesti dalla disciplina – sia al **ripristino dello stato del conto** di pagamento.



**Lacune nell'informativa alla clientela**, con riferimento alla rappresentazione delle **modalità con cui notificare il disconoscimento**, quanto alla **comunicazione del motivo del diniego del rimborso**.



**Inadeguatezza dei meccanismi di tokenizzazione** delle carte di pagamento della clientela **nelle applicazioni di “wallet provider”** esterni, spesso svolta senza SCA.

# I principali adempimenti richiesti ai PSP da Banca d'Italia

## Attività richieste ai PSP:

È richiesto ai PSP di **condurre un'autovalutazione coerente degli assetti, delle procedure e delle prassi in tema di disconoscimento** delle operazioni di pagamento, nonché di **adottare un piano di rimedio, entro 12 mesi dalla pubblicazione delle linee guida**, in relazione ai seguenti aspetti:

- 1** Adozione di **specifica policy interna** che regoli il **processo di gestione** dei disconoscimenti, disciplinando uniformemente tutte le categorie di operazioni non autorizzate per **evitare che vengano trattate come reclami ordinari**.
- 2** **Rispetto dei criteri di riparto delle responsabilità** tra PSP e cliente nell'ambito dell'**istruttoria** sulle richieste di disconoscimento, basando le **procedure automatizzate** per verificare l'eventuale dolo o colpa grave del cliente su **griglie granulari** che consentano una adeguata verifica dell'eventuale dolo o colpa grave dell'utente. I PSP devono comunque garantire una valutazione completa anche per casi non espressamente tipizzati.
- 3** Avvio di **iniziative di sensibilizzazione e formazione del personale** coinvolto nella valutazione dei disconoscimenti.
- 4** Adozione di **presidi interni** volti a garantire il **rispetto delle tempistiche di rimborso** (evitando che la presa in carico della pratica sia subordinata alla ricezione di documentazione aggiuntiva) e del **mantenimento dell'uniformità della data valuta** tra rimborso e addebito.
- 5** Adozione di **documentazione di trasparenza** recante **informazioni chiare sui diritti dei clienti e modalità di comunicazione** in caso di disconoscimenti, **evitando riferimenti generici** alla normativa. Inoltre, deve essere **garantita trasparenza** sul diritto dei PSP di **recuperare le somme rimborsate** e le **comunicazioni post-disconoscimento devono essere chiare e comprensibili**.
- 6** Adozione di **documentazione di trasparenza** recante **informazioni chiare sui diritti dei clienti e modalità di comunicazione** in caso di disconoscimenti, **evitando riferimenti generici** alla normativa. Inoltre, deve essere **garantita trasparenza** sul diritto dei PSP di **recuperare le somme rimborsate** e le **comunicazioni post-disconoscimento devono essere chiare e comprensibili**.
- 7** **Valutazione dei precedenti dell'ABF** in materia per adeguare le procedure interne e per velocizzare le valutazioni in termini di disconoscimenti.
- 8** Rafforzamento delle **procedure di tokenizzazione delle carte** (a prescindere dal canale di enrolment).

# L'approccio suggerito da PwC in merito alla Comunicazione di Banca d'Italia sui disconoscimenti

Potenziali  
ambiti di  
supporto PwC



Esercizio di  
autovalutazione



Adeguamento  
normativo



Formazione Interna  
e monitoraggio  
normativo

Dettaglio  
attività

Assistenza nella **conduzione dell'autovalutazione di conformità** delle **procedure interne** di gestione dei disconoscimenti, della **documentazione di informativa precontrattuale e dei contratti** per la prestazione dei servizi di pagamento per verificarne il **livello di conformità** rispetto alle prescrizioni di Banca d'Italia.

**Redazione/revisione della policy, dei processi e delle procedure interne** al fine di renderle conformi alla normativa di riferimento e di immediata comprensione per tutti gli operatori interni coinvolti.

Supporto nella **revisione e aggiornamento** della documentazione **precontrattuale e contrattuale**.

Supporto nella **organizzazione di eventi di formazione e sensibilizzazione del personale** coinvolto al fine di garantire una corretta attuazione delle prescrizioni legislative e delle raccomandazioni di vigilanza di Banca d'Italia.

**Attività di monitoraggio** normativo e delle decisioni dell'Arbitro Bancario Finanziario (**ABF**) per garantire coerenza nelle soluzioni adottate.



## Contatti

### **Fabrizio Cascinelli**

Partner PwC Italia,  
Legal - Financial Regulation

+39 345 698 1767  
fabrizio.cascinelli@pwc.com

### **Luca Bettinelli**

Senior Manager PwC Italia,  
Legal - Financial Regulation

+39 346 504 6320  
luca.bettinelli@pwc.com