PSD2, la conosci davvero?

Le dieci cose da sapere sulla Payment Services Directive 2

DOCUMENTO ACCESSIBILE A IPOVEDENTI E NON VEDENTI*

noi & UniCredit

Documento sviluppato con le Associazioni dei Consumatori partner del Programma Noi&UniCredit

ADICONSUM · ADOC · ASSOUTENTI · Casa del Consumatore · CITTADINANZATTIVA
CODACONS · CONFCONSUMATORI APS · Federconsumatori · LEGA CONSUMATORI · MOVIMENTO CONSUMATORI
MOVIMENTO DIFESA del Cittadino · U.Di.Con. · 1955 UNC CONSUMATORI.IT

UniCredit

* Accessibile su lettori con lingua italiana conformi agli standard PDF/UA

1 CHE COSA È LA SECONDA DIRETTIVA SUI SERVIZI DI PAGAMENTO (PAYMENT SERVICES DIRECTIVE - PSD2)?

É la direttiva europea 2015/2366 sui **servizi di pagamento nel mercato interno** entrata in vigore il 13 gennaio 2016 (abrogando la direttiva 2007/64/CE - PSD) e recepita dal Parlamento italiano l'11 dicembre 2017.

ATTENZIONE
La PSD2 è stata recepita nell'ordinamento nazionale con il D. lgs. n.218 del 15 dicembre 2017, entrato in vigore il 13 gennaio 2018.

2 QUALI SONO GLI OBIETTIVI DELLA PSD2?

Le principali finalità della direttiva sono **contrastare le frodi e accrescere la fiducia dei consumatori** nei pagamenti digitali modernizzando il quadro normativo che regola i servizi digitali innovativi.

ATTENZIONE
La PSD2 favorisce inoltre l'**aumento della competitività** incoraggiando lo sviluppo di nuovi prodotti e l'apertura del mercato a soggetti non bancari.

3 A CHI SI RIVOLGE?

Le nuove disposizioni si applicano a **tutti i prestatori di servizi di pagamento (PSP) autorizzati dalla Banca d'Italia**, ossia banche, istituti di pagamento (IP) e istituti di moneta elettronica (IMEL) e a soggetti comunitari ed extra comunitari che operano sul territorio italiano in base a specifiche autorizzazioni. Rientrano nell'ambito di applicazione della nuova disciplina anche le c.d. **Terze parti** (Third Party Providers - TPP), ossia gli operatori di servizi di pagamento diversi da quelli presso i quali sono radicati i conti degli utenti e che prestano servizi online di informazione sui conti (c.d. Account Information Service Provider - AISP) e di disposizione di ordini di pagamento (c.d. Payment Initiation Services Provider - PISP).

ATTENZIONE
Per garantire trasparenza e sicurezza a banche e clienti le terze parti devono essere **registrate**, **autorizzate** e **regolamentate** a livello dell'Unione Europea.

4 QUALI SONO I SERVIZI INTERESSATI?

La direttiva **si applica a tutti i servizi di pagamento prestati nell'UE**, tra cui bonifici, addebiti diretti, carte di credito, debito e prepagate, portafogli elettronici e altri pagamenti via internet. La PSD2 prevede inoltre lo sviluppo dell'Open Banking, che consente ai clienti di autorizzare terze parti ad accedere ai propri dati bancari per l'offerta di nuovi servizi.

ATTENZIONE
La PSD2 non ha invece impatti ad esempio sugli incassi domestici (MAV, bollettini bancari, Ri.Ba.).

5 CHE COSA SONO LE OPERAZIONI ONE LEG?

Sono le operazioni di pagamento disposte, in tutte le valute, in cui anche uno solo dei prestatori di servizi di pagamento è situato nell'Unione Europea.

ATTENZIONE
La PSD2 prevede che anche le operazioni one leg rientrino nell'ambito di applicazione della normativa al fine di garantire maggiore uniformità del quadro normativo.

6 QUALI SONO LE PRINCIPALI NOVITÀ INTRODOTTE DALLA PSD2?

La PSD2 ha introdotto importanti novità quali:

- **obblighi di trasparenza**: sono stati rafforzati i diritti dei consumatori e la trasparenza in relazione agli obblighi di informazione, esecuzione delle operazioni di pagamento e condizioni economiche;
- **ampliamento di ambito di applicazione**: l'ambito di applicazione della normativa è stato esteso alle operazioni di pagamento in tutte le valute;
- **nuove misure di sicurezza**: è stata introdotta l'**autenticazione forte dell'utente (Strong Customer Authentication - SCA)** per accedere al proprio conto online, disporre ordini di pagamento elettronico e per effettuare qualsiasi azione, tramite canali a distanza, che possa comportare rischi di frodi nei pagamenti e altri abusi;
- **accesso ai conti online tramite Third Party Provider (TPP)**: è stata prevista la possibilità di accedere alle informazioni relative al proprio conto corrente e alle transazioni effettuate, nonché di disporre ordini di pagamento, attraverso terze parti.

ATTENZIONE
La direttiva impone il **divieto per gli esercenti di applicare ai propri clienti una maggiorazione per l'uso di un determinato strumento di pagamento**. Nello specifico, secondo quanto previsto dal regolamento 751 del 2015, le commissioni interbancarie non possono essere superiori allo 0,2% del valore dell'operazione per i pagamenti con carte di debito e allo 0,3% per quelle con carta di credito.

7 COME VIENE CONSENTITO ALLE TERZE PARTI L'ACCESSO AI CONTI ONLINE?

L'accesso ai servizi delle terze parti avviene previo **consenso** da parte dell'utente, **esplicitamente rilasciato loro e notificato alla banca di radicamento del conto**. Per permettere ad un utente l'utilizzo dei servizi erogati dalle terze parti, la banca presso cui detiene un conto online dovrà fornire l'accesso:

- tramite un **canale dedicato** (c.d. Application Programming Interface - API) oppure
- consentendo alla terza parte l'**accesso diretto** agli stessi canali online della banca utilizzati dell'utente.

ATTENZIONE
In entrambe i casi, dovrà essere garantita la **sicurezza della comunicazione e degli scambi di informazioni** tra la banca e le terze parti, nel rispetto della privacy dall'utente.

8 QUALI SONO LE NUOVE MISURE DI SICUREZZA INTRODOTTE?

La principale misura di sicurezza prevista dalla normativa è l'autenticazione forte dell'utente (Strong Customer Authentication - SCA). Si tratta di una procedura per convalidare l'identificazione dell'utente che garantisce una maggiore sicurezza ed è basata sull'**uso di due o più elementi di autenticazione** (c.d. autenticazione a due fattori) appartenenti ad almeno due categorie tra le seguenti:

- **conoscenza:** qualcosa che solo l'utente conosce, come una password o un PIN (Personal Identification Number) ovvero un numero identificativo personale;
- **possesso:** qualcosa che solo l'utente possiede, come un token/chiavetta, o uno smartphone;
- **inerenza**: qualcosa che caratterizza l'utente, come l'impronta digitale o il riconoscimento facciale.

I fattori devono essere reciprocamente indipendenti, cioè la violazione di uno non compromette l'altro. Inoltre, almeno uno degli elementi dovrebbe essere **non riutilizzabile, non replicabile e non trafugabile via Internet**. La procedura di autenticazione deve essere progettata in modo tale da proteggere la riservatezza dei dati di autenticazione.
La SCA si applica per:

- **accedere al conto online**;
- **disporre un'operazione di pagamento elettronico**;
- **effettuare qualsiasi azione**, tramite un canale a distanza, **che può comportare un rischio di frode nei pagamenti o altri abusi**.

ATTENZIONE
Per autorizzare un pagamento elettronico a distanza è richiesta, oltre alla SCA, l'applicazione del **dynamic linking** ovvero un codice univoco legato all'importo della transazione e al suo beneficiario, quindi in caso di cambio di importo o beneficiario il codice è nullo e deve esserne generato un altro.

9 COSA ACCADE IN CASO DI OPERAZIONI DI PAGAMENTO NON AUTORIZZATE O NON CORRETTAMENTE ESEGUITE?

L'utente, nel caso di un'operazione di pagamento non autorizzata o non correttamente eseguita, ha il diritto di ottenerne il rimborso o la rettifica solo se comunica **senza indugio** tale circostanza al proprio prestatore di servizi di pagamento (PSP). Tale comunicazione, in ogni caso, deve essere fatta **entro 13 mesi dalla data di addebito**.
Il rimborso dell'addebito disconosciuto dovrà essere:

- **integrale**: il rimborso deve essere pari all'intero importo dell'operazione non autorizzata;
- **immediato**: il rimborso deve avvenire immediatamente e in ogni caso al più tardi entro la fine della giornata operativa successiva a quella in cui il PSP ha avuto conoscenza dell'operazione non autorizzata;
- **non svantaggioso**: la valuta dell'accredito del rimborso non deve essere successiva alla data di addebito dell'importo.

Il rimborso delle operazioni disconosciute è da intendersi salvo buon fine (SBF), in quanto il PSP, **anche in un momento successivo** al rimborso, può dimostrare che, in realtà, l'operazione di pagamento era stata autorizzata dall'utente oppure è conseguente ad una sua azione colposa o dolosa; in tal caso, il PSP ha diritto di chiedere direttamente all'utente e ottenere da quest'ultimo la restituzione dell'importo rimborsato.

ATTENZIONE
Un'eccezione all'obbligo di rimborso opera nel caso in cui il PSP abbia il motivato sospetto che l'operazione non autorizzata derivi da un comportamento fraudolento posto in essere dall'utente.

10 CHE COSA CAMBIA PER PER I TEMPI DI RISPOSTA AI RECLAMI RELATIVI ALLE OPERAZIONI DI PAGAMENTO?

Per questa tipologia di reclami le tempistiche per la gestione dei reclami scritti da parte dei PSP si riducono da **30 giorni solari a 15 giorni lavorativi**.

ATTENZIONE
Nel caso in cui non sia possibile rispettare il termine dei 15 giorni lavorativi il PSP invia una risposta interlocutoria con indicazione delle **ragioni del ritardo** specificando il termine entro il quale verrà fornita la risposta definitiva e comunque **non oltre 35 giorni lavorativi.**