I pagamenti nel commercio elettronico: una mappa per orientarsi

Sommario

INTRODUZIONE

A chi è rivolto questo documento?

A tutti coloro che comprano beni o servizi online e vogliono capire meglio come funzionano i pagamenti sul web. Tutti più o meno abbiamo fatto esperienza di acquisti sul web e probabilmente abbiamo sentito parlare della PSD2, la nuova normativa europea sui servizi di pagamento, ma cosa sappiamo veramente dei pagamenti digitali, dei loro vantaggi, dei loro rischi e delle loro regole?

Perché la Banca d'Italia pubblica questo documento?

Perché tutti possiamo orientarci con consapevolezza in questa importante evoluzione, che deve realizzarsi in modo sicuro e a vantaggio dell'interesse comune.
La disponibilità di nuovi servizi - sempre più moderni, veloci e comodi - e la presenza di nuovi operatori specializzati nell'utilizzo delle nuove tecnologie (cd. Fintech) richiedono agli utenti uno sforzo di comprensione: senza pretesa di esaustività, intendiamo spiegare gli schemi di funzionamento dei pagamenti digitali e dare una visione d'insieme dei potenziali rischi e delle regole applicabili.

Avvertenze. Questo documento è pubblicato dalla Banca d'Italia senza finalità di interpretazione o di attuazione delle disposizioni di legge; le disposizioni normative, qualora richiamate, sono esposte con finalità soltanto illustrativa e divulgativa. Il documento fa riferimento a strumenti di pagamento elettronici e non si occupa dei trasferimenti di valute virtuali. Per l'esatta indicazione degli obblighi e delle tutele previsti dalla normativa vigente per i prestatori e gli utenti di servizi di pagamento, si invitano in ogni caso tutti i soggetti interessati a consultare le fonti normative di riferimento, riepilogate alla fine di questo documento.

Come abbiamo impostato il documento?

Come una mappa dinamica. I concetti più importanti per orientarsi nel mondo dei pagamenti digitali sono illustrati con un linguaggio non tecnico e con livelli di approfondimento crescente, partendo dalla descrizione della concreta esperienza di un acquisto su un sito di e-commerce.

Come si articola il documento?

Nella prima sezione "**Come si paga online?"** diamo il quadro d'insieme delle principali modalità di pagamento utilizzabili *Vai a "Come si paga online?"*:

- nella sotto-sezione "**Pagare online con una carta di pagamento"** spieghiamo il funzionamento delle diverse tipologie di carta - di credito, prepagata, di debito - e gli specifici rischi, obblighi e tutele connessi con l'utilizzo di tali strumenti di pagamento; *Vai a "Carta di pagamento"*
- nella sotto-sezione "**Pagare online tramite bonifico/PISP**" illustriamo lo schema di pagamento con bonifico, così come innovato dalla PSD2 con l'introduzione del servizio di "disposizione di ordini di pagamento", e illustriamo i relativi rischi, obblighi e tutele per i clienti; *Vai a "Bonifico/PISP"*

- nella sotto-sezione “Pagare online **utilizzando un portafoglio elettronico o wallet**” presentiamo le forme di portafoglio elettronico disponibili per i pagamenti online, con i relativi rischi e peculiarità. *Vai a "Wallet"*

Nella sezione “**Un nuovo servizio “di pagamento”: il servizio di informazione sui conti - AIS**”, presentiamo le modalità di funzionamento del nuovo servizio AIS introdotto dalla PSD2, con i relativi rischi, obblighi e tutele per il cliente. *Vai a "AIS"*

Nella sezione “**Obblighi e tutele”** si trova uno schema riassuntivo degli obblighi dei diversi attori coinvolti nel pagamento e delle tutele che sono garantite ai clienti; gli iperlink consentono di accedere a varie sotto-sezioni di approfondimento, che riportano in dettaglio gli obblighi e le tutele, articolati per materia e per soggetto coinvolto. *Vai a "Obblighi e tutele"*

Completano la pubblicazione:

- un **glossario** dei principali termini tecnici utilizzati nel linguaggio dei pagamenti digitali che ha il solo fine di agevolare la comprensione del testo; *Vai a "Glossario"*
- un riepilogo delle **fonti normative** di riferimento; *Vai a "Fonti normative"*

COME SI PAGA ONLINE?

Partiamo dall'inizio. Il cliente ricerca sul sito web di commercio elettronico o sull'applicazione telefonica i servizi o gli articoli di proprio interesse. Terminata la fase di selezione, accede alla sezione del sito o dell'applicazione dedicata alla finalizzazione dell'acquisto: qui il cliente seleziona una delle opzioni di pagamento disponibili e avvia il pagamento. Le modalità disponibili sono, di solito, le seguenti:

- **carta di pagamento**

  Le carte di pagamento sono lo strumento più utilizzato per pagare sui siti di commercio elettronico. Il loro funzionamento si basa sull'utilizzo di un dispositivo (point of sale) POS virtuale del tutto simile a quello fisico presente nei negozi ed è prevista immediata conferma dell'avvenuto pagamento.

  Esistono tre tipologie di carte di pagamento che, pur utilizzando il medesimo POS virtuale, hanno un diverso schema di funzionamento:

  - carta di credito: l'acquisto del bene viene pagato grazie all'utilizzo della linea di credito connessa alla carta;
  - carta prepagata: per poter effettuare i pagamenti occorre "caricare" sulla carta la provvista, costituta da moneta elettronica, prima dell'utilizzo;
  - carta di debito: consente di utilizzare i fondi disponibili sul proprio conto di pagamento.

Vai a "Carta di pagamento"

- **bonifico/PISP**

Il bonifico è un'operazione di pagamento che realizza un trasferimento di fondi da un conto di pagamento a un altro; esso è poco diffuso per i pagamenti online in quanto non consente di concludere l'acquisto nello stesso momento in cui si esegue il pagamento, se non nei casi in cui vi è un rapporto diretto fra il commerciante e l'intermediario presso cui il cliente detiene il conto ovvero vi sono accordi specifici tra banche. La PSD2 ha però introdotto il servizio di disposizione di ordini di pagamento (*payment initiation service* – PIS) che consente a un intermediario autorizzato (*payment initiation service provider* - PISP) di interporsi fra il commerciante online e l'intermediario e far sì che il cliente possa disporre un trasferimento di fondi dal proprio conto a quello del commerciante online, selezionando la modalità di pagamento direttamente dal sito di e-commerce.

Vai a "Bonifico/PISP"

- **portafoglio elettronico o wallet**

Si va diffondendo in rete la possibilità di pagare tramite portafoglio elettronico o wallet; esistono due tipologie di wallet, con caratteristiche diverse tra loro:

  - pass through wallet: si tratta di un contenitore nel quale il cliente registra i propri strumenti di pagamento, che vengono utilizzati quando si effettua una transazione

(tale modalità di pagamento è quella tipicamente adottata da Google Pay, Amazon Pay, Apple Pay e Samsung Pay, per citare alcuni dei più diffusi);

- staged wallet: con l'utilizzo di questo portafoglio il cliente accede al proprio conto online ed effettua trasferimenti di denaro da conto a conto, in modalità simile al bonifico. La particolarità è che il cliente e il commerciante online detengono il conto presso l'intermediario che offre il servizio di wallet (un esempio di questo servizio è Paypal).

Vai a "Wallet"

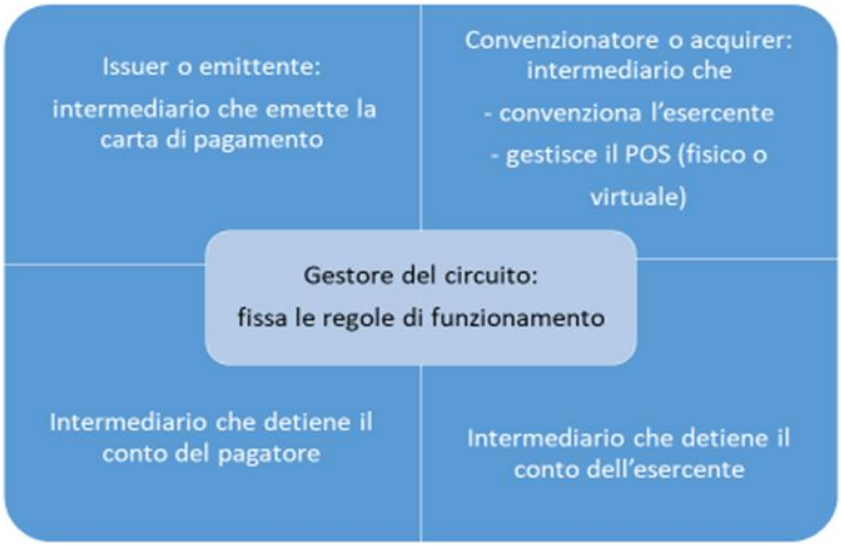
In alternativa all'utilizzo di strumenti di pagamento elettronici è possibile prenotare la merce online ed eseguire pagamento e ritiro presso il negozio ovvero pagare in contrassegno al momento della consegna. In entrambi i casi la vendita si conclude in un momento successivo alla scelta sul sito web.

Pagare online con una carta di pagamento

Le carte di pagamento (di credito, prepagate e di debito) sono emesse da un intermediario autorizzato, che si chiama emittente. Nel caso della carta di debito l'emittente coincide con l'intermediario che detiene il conto del cliente (fatto salvo il caso del CBPII, vedi glossario). Nelle carte di credito l'emittente è, di solito, un soggetto diverso da quello che detiene il conto del cliente. Per richiedere le carte prepagate non è necessario essere già titolari di un conto.

Nell'operazione con carta rileva anche un altro intermediario, convenzionatore o acquirer, che gestisce il POS (fisico o virtuale) presso l'esercente, e può essere diverso dall'intermediario che detiene il conto dell'esercente.

Il regolamento finale dell'operazione avviene sempre accreditando il conto dell'esercente e addebitando quello del cliente, ma il funzionamento dell'operazione con carta e i rapporti fra l'emittente, l'acquirer e gli intermediari presso cui sono aperti i conti dipende dalle regole fissate dal gestore del circuito. I più noti circuiti di carte di credito sono Visa, Mastercard, American Express, Diners, mentre i circuiti di carte di debito più diffusi in Italia sono Bancomat e Maestro.



1. Come funziona un pagamento con carta su un sito di e-commerce?

E' necessario distinguere due tipologie di operazioni che hanno regole diverse anche se la carta utilizzata è la stessa.

1.1. Transazione a iniziativa del cliente

In questo caso è il cliente che avvia il pagamento. Al check-out il cliente troverà fra le modalità di pagamento il logo di uno o più circuiti a cui la carta è affiliata. Il commerciante online è convenzionato con un acquirer che lo abilita a ricevere pagamenti mediante un'applicazione web.

Il pagamento si articola in diverse fasi:

- dopo aver selezionato il metodo di pagamento, il cliente viene indirizzato dalla pagina del sito di e-commerce al POS virtuale gestito dall'acquirer, dove inserisce i dati della carta di pagamento in maniera sicura e avvia la transazione.

ATTENZIONE: I commercianti online talvolta richiedono al cliente il consenso a conservare i dati della carta in fase di registrazione o in occasione del primo pagamento, così da poterli riutilizzare in ogni successivo pagamento effettuato sul sito di e-commerce.

- l'acquirer effettua controlli formali di validità della carta per prevenire, ad esempio, la digitazione errata dei codici;
- il cliente viene temporaneamente re-indirizzato sul sito web dell'emittente, dove inserisce le credenziali per l'autenticazione forte – salve le ipotesi di esenzione previste dalla normativa *(vai a obblighi di sicurezza)*;
- l'emittente verifica le credenziali inserite, valuta il livello di rischio della transazione tramite appositi meccanismi di monitoraggio *(vai a obblighi di sicurezza)* e svolge i controlli autorizzativi (disponibilità, limiti di utilizzo, verifiche antifrode), inviandone l'esito all'acquirer;
- l'acquirer comunica al merchant l'esito del pagamento; se positivo, l'esercente può avviare la procedura per la consegna del bene o la fornitura del servizio acquistato;
- il cliente è re-indirizzato sul sito di e-commerce, dove gli viene comunicato l'esito della transazione (transazione di pagamento andata a buon fine o rigettata).

ATTENZIONE: *In caso di blocchi nel processo, controllare sempre con l'emittente l'esito dell'operazione prima di effettuare nuovamente il pagamento.*

1.2. Transazione a iniziativa del beneficiario

Un'altra modalità di utilizzo della carta consente l'avvio della transazione di pagamento da parte del commerciante online, in un momento successivo alla scelta della merce. In questo caso il cliente fornisce all'esercente i dati della propria carta, ad esempio compilando un apposito modulo sul sito, e lo autorizza ad addebitare il corrispettivo in un momento successivo.

L'autorizzazione può essere concessa per una singola transazione (ad esempio per il pagamento di pacchetti turistici su siti di viaggi) o per più pagamenti (come accade, ad esempio, per le erogazioni periodiche a favore di associazioni benefiche o enti di ricerca). La transazione viene avviata dall'esercente senza necessità di altri comportamenti attivi da parte del pagatore per l'importo già predeterminato, o per importi ulteriori se c'è l'autorizzazione in tal senso del cliente.

2. Cosa deve fare il cliente in caso di transazione non autorizzata?

2.1. Furti o smarrimenti

(vai a obblighi cliente) – (vai a rimborsi e responsabilità)

E' importante ricordare che il cliente che si accorge dello smarrimento o del furto di una carta o dell'esecuzione di un'operazione con carta da lui non autorizzata deve il più presto possibile comunicarlo all'emittente.

2.2. SCA o non SCA

(vai a obblighi di sicurezza)

Nel caso in cui la transazione di pagamento con carta sia avviata dal cliente (paragrafo 1.1), salvo ipotesi di esenzione, la transazione sarà sottoposta a doppio fattore di autenticazione (strong customer authentication - SCA). E' l'emittente della carta che mette a disposizione dell'utente i mezzi per l'autenticazione forte. E' sempre l'emittente che valuta se per una certa transazione è necessaria la SCA ovvero a decidere, laddove ne ricorrano le condizioni, di optare per un'ipotesi di esenzione prevista dalla normativa; tuttavia, l'*acquirer* può proporre di applicare un'esenzione all'emittente, che potrà accordarla o meno.

2.3. Obblighi di rimborso - transazione a iniziativa del pagatore

(vai a rimborsi e responsabilità)

E' l'emittente che ha un obbligo di rimborso nei confronti del cliente in caso di transazione non autorizzata, salvo rivalersi poi, in casi specifici, nei confronti dell'acquirer o del beneficiario. Se non è stata richiesta la SCA, l'emittente può rifiutare il rimborso solo se ritiene che il cliente abbia agito con frode. Se è stata richiesta la SCA, il rimborso può essere rifiutato se l'intermediario dimostra la frode, il dolo o la colpa grave del cliente.

ATTENZIONE: *Il cliente che ha agito con intento fraudolento non ha mai diritto di essere rimborsato. Il cliente in colpa grave ha sempre garanzia di rimborso in assenza di SCA.*

2.4. Obblighi di rimborso - transazione a iniziativa del beneficiario

(vai a rimborsi e responsabilità)

Quando l'operazione di pagamento su carta è disposta su iniziativa del beneficiario (paragrafo 1.2) non è prevista l'autenticazione del cliente nella fase di esecuzione della transazione, ma valgono le specifiche tutele previste per le operazioni di pagamento su iniziativa del beneficiario: il cliente ha a disposizione 13 mesi di tempo per chiedere il rimborso se non aveva mai dato al beneficiario del pagamento alcuna autorizzazione all'addebito; può comunque richiedere il rimborso all'emittente entro otto settimane, anche se aveva precedentemente autorizzato l'operazione, nei casi in cui l'importo non era predeterminato e superiore alle sue ragionevoli aspettative.

2.5. Chargeback

Le regole contrattuali previste da un circuito possono assicurare una tutela aggiuntiva al cliente in caso di operazioni non autorizzate. In particolare, la maggior parte dei circuiti di carte prevede il chargeback, vale a dire un meccanismo che consente all'emittente di recuperare direttamente dall'acquirer l'importo contestato.

ATTENZIONE: non va confuso il chargeback - che riguarda i rapporti fra emittente e acquirer - con il cashback che può voler dire due cose distinte: 1) rimborso al cliente da parte del negoziante di una piccola percentuale del pagamento effettuato con carta (es. a fronte di una spesa di 50 euro, il cliente riceve un rimborso o un buono spesa pari al 5% dell'importo pagato); 2) prelievo di contante richiesto al negoziante dal cliente in aggiunta a un pagamento con carta (es. il cliente che deve pagare 50

euro per un acquisto effettuato chiede al commerciante di pagare 70 euro per ricevere 20 euro in contanti).

Torna a "Come si paga online?"

Pagare online tramite Bonifico/PISP

Nel commercio su web l'operazione di pagamento tramite bonifico può essere realizzata in due forme diverse: la prima, **modalità differita,** non è eseguibile sul sito di e-commerce in cui si è effettuato l'acquisto e prevede un ordine di bonifico non direttamente collegato alla transazione commerciale; la seconda, **modalità online**, è possibile quando vi è un rapporto diretto fra il commerciante e l'intermediario presso cui il cliente detiene il conto o un accordo tra banche che consente di pagare con immediata certezza del buon esito per il commerciante convenzionato (ad esempio MyBank), oppure grazie all'intermediazione di un nuovo soggetto terzo. La PSD2 ha infatti introdotto il servizio di disposizione di ordini di pagamento (payment initiation service – PIS) che consente a un intermediario autorizzato (payment initiation service provider - PISP) di interporsi fra il commerciante online e l'intermediario e far sì che il cliente possa disporre un trasferimento di fondi dal proprio conto a quello del commerciante online, selezionando la modalità di pagamento direttamente dal sito di e-commerce. Il PISP rientra tra i c.d. Third Party Providers (TPP), soggetti terzi che hanno il diritto di accedere ai conti dell'utente, se autorizzati da quest'ultimo, anche in assenza di un rapporto contrattuale con l'intermediario presso cui tali conti sono radicati (detto anche account servicing payment service provider – ASPSP). Il PISP non entra mai in possesso dei fondi dell'utente, che rimangono depositati presso i conti di cui il cliente è titolare.

1. Come funziona un pagamento con bonifico su un sito di e-commerce?

1.1. Modalità differita

Il commerciante online comunica al cliente l'IBAN del conto su cui effettuare il pagamento. Il cliente, per completare l'acquisto, effettua l'ordine di pagamento, ad esempio tramite il servizio di home banking, e ne dà riscontro al commerciante nelle modalità concordate (es. via mail). Il commerciante procede alla spedizione della merce o alla fornitura del servizio solo dopo aver avuto conferma dell'avvenuto accredito del bonifico sul proprio conto che, solitamente, avviene nella giornata operativa successiva a quella in cui è stato disposto il pagamento da parte del cliente.

1.2 Modalità online tramite PISP

Il bonifico non viene effettuato direttamente dal cliente ma quest'ultimo autorizza un intermediario, il PISP, a disporlo per proprio conto. Il pagamento si articola, nei modelli operativi prevalenti, in più fasi:

- dopo aver selezionato il nome del PISP in fase di check-out, il cliente viene indirizzato alla piattaforma del PISP dove inserisce: 1) il codice identificativo dell'intermediario presso cui detiene il conto; 2) USERID e password per poter accedere al conto online; e, se non sono già stati inseriti dal PISP; 3) l'importo e i dati del beneficiario; 4) il numero di ordine fornito dal commerciante online per permettere la riconciliazione del pagamento;
- i dati del pagamento vengono poi mostrati al cliente che conferma l'ordine, inserendo le credenziali per l'autenticazione forte – salve le ipotesi di esenzione previste dalla normativa *(vai a obblighi di sicurezza)*;
- il PISP dà riscontro al commerciante e al cliente dell'avvio del pagamento;

- il cliente è re-indirizzato sul sito di e-commerce, dove si potrà concludere l'acquisto.

ATTENZIONE: *prima di dare il proprio consenso al PISP all'esecuzione di un'operazione di pagamento, è opportuno verificare che il PISP sia stato autorizzato nello Stato Membro in cui ha la propria sede legale e che sia iscritto nel relativo albo, in cui sono indicati anche tutti gli stati dell'Unione in cui è abilitato a prestare i propri servizi. Dal marzo 2019 è attivo il Registro EBA degli istituti di pagamento e degli istituti di moneta elettronica, in cui sono censiti tutti gli operatori autorizzati nell'Unione Europea e i paesi in cui sono abilitati a prestare i propri servizi. Possono prestare questo servizio anche le banche, censite nel Registro dell'EBA consultabile al seguente link: https://eportal.eba.europa.eu/cir/faces/publicSearchCreditInstitution.xhtml#no-back-button.*

(vai a rimborsi e responsabilità).

2. Cosa deve fare il cliente in caso di transazione non autorizzata?

2.1. Modalità differita

L'utilizzo del bonifico in modalità differita richiede particolari attenzioni da parte del cliente prima dell'esecuzione della transazione sulla correttezza del negoziante con cui sta interloquendo. Poiché la transazione non è direttamente collegata all'acquisto online eventuali azioni di recupero successive potrebbero essere molto difficoltose.

2.2. Modalità online tramite PISP

Il cliente, in caso di operazioni non autorizzate, deve rivolgersi all'intermediario presso cui detiene il conto (ASPSP).

Norme specifiche disciplinano il riparto delle responsabilità nei rapporti interni fra PISP e ASPSP.

(vai a rimborsi e responsabilità).

ATTENZIONE: Si sono verificati casi di frode in cui un soggetto simula di vendere beni o servizi, richiede il pagamento tramite bonifico, ma dopo aver ricevuto le somme non consegna quanto dovuto. In questo caso non si è in presenza di una operazione non autorizzata in quanto l'intermediario che ha eseguito il bonifico ha ottemperato all'ordine ricevuto dal cliente e dunque non è responsabile dell'accaduto; esso potrà solamente attivarsi per cercare di recuperare la somma rivolgendosi all'intermediario presso cui il beneficiario detiene il conto. Il recupero può, tuttavia, rivelarsi complicato, in quanto, per recuperare le somme, è necessario il consenso del beneficiario che, se frodatore, presumibilmente non lo darà.

Torna a "Come si paga online?"

Pagare online utilizzando un Portafoglio elettronico o wallet

Alcuni siti di commercio online propongono, tra le opzioni di pagamento, anche la possibilità di utilizzare un wallet. Con tale denominazione ci si riferisce solitamente a due diverse tipologie di portafogli elettronici - **pass through** e **staged wallet** - che presentano differenti modalità di funzionamento e garanzie.

1. Come funziona un pagamento con wallet su un sito di e-commerce?

1.1. Pass through wallet

Il funzionamento si basa, di norma, sull'accordo esistente fra il gestore del wallet, che solitamente non è un intermediario, l'emittente dello strumento di pagamento e l'acquirer del negoziante online. Il pagamento si articola in più fasi:

- dopo aver selezionato il nome del wallet in fase di check-out, il cliente accede al wallet con le proprie credenziali;
- all'interno del wallet decide quale strumento usare fra quelli registrati;
- si avvia una transazione con lo strumento selezionato, seguendo un normale processo di pagamento con l'inserimento delle credenziali, se previsto, la conferma e la notifica di avvenuta esecuzione *(vai a obblighi di sicurezza)*.

ATTENZIONE: *il cliente deve valutare attentamente l'affidabilità del gestore del wallet presso cui registra i dati relativi ai propri strumenti di pagamento. In caso di dubbio è opportuno rivolgersi all'intermediario presso cui detiene il conto e/o all'emittente della carta di pagamento. Gli intermediari indicano, in genere, anche se determinati wallet sono "compatibili" con gli strumenti di pagamento di cui sono emittenti.*

1.2. Staged wallet

Il cliente e il commerciante online hanno entrambi un conto di pagamento o di moneta elettronica aperto presso l'intermediario, gestore del wallet. Il cliente seleziona il wallet come modalità di pagamento e ordina un trasferimento di denaro, simile a un bonifico, dal proprio conto a quello del commerciante, inserendo, se previsto, le credenziali per l'autenticazione forte.

2. Cosa deve fare il cliente in caso di transazione non autorizzata?

2.1. Pass through wallet

Il cliente nel caso in cui si accorga di un'operazione non autorizzata, deve rivolgersi sempre all'intermediario che ha rilasciato lo strumento di pagamento registrato nel wallet – l'emittente nel caso di carte – non al gestore del wallet. Gli obblighi di rimborso sono a carico dell'intermediario. Ove anche esista un contratto tra intermediario e gestore del wallet che regola un riparto di responsabilità nei loro rapporti interni, questo non inficia la tutela assicurata al cliente.

ATTENZIONE: *Il cliente deve dare immediata comunicazione dello smarrimento o furto del device all'intermediario che ha rilasciato lo strumento di pagamento caricato nel wallet. Deve porre*

particolare attenzione anche nella custodia delle credenziali di accesso al wallet, che possono rappresentare uno degli elementi per avviare il pagamento.

2.2. Staged wallet

Nel caso di transazioni non autorizzate, furto o smarrimento del device su cui è caricato il wallet, il cliente deve rivolgersi all'intermediario gestore del wallet presso il quale sono tenuti i conti del cliente e del commerciante.

Torna a "Come si paga online?"

UN NUOVO SERVIZIO "DI PAGAMENTO": IL SERVIZIO DI INFORMAZIONE SUI CONTI (AIS)

Nell'ambito dei servizi di pagamento una novità importante è rappresentata dal nuovo servizio di informazione sui conti (account information service – AIS) introdotto dalla PSD2.

Il servizio di informazione sui conti AIS rappresenta un ausilio per i clienti nella pianificazione e nel monitoraggio delle loro spese. Il prestatore del servizio di informazione sui conti (account information service provider – AISP), previo consenso, accede ai conti online del cliente aperti presso qualunque intermediario, e gli fornisce informazioni consolidate, ad esempio, sulle operazioni effettuate e il saldo. In questo modo il cliente può disporre di informazioni aggiornate sulla propria situazione finanziaria, senza necessità di accedere separatamente a tutti i conti online di cui è titolare. Tra i servizi offerti rientrano l'analisi delle spese per tipologia e la fissazione di un budget mensile.

L'ambito di applicazione della normativa in materia di servizi di pagamento, con il recepimento della Direttiva PSD2 nel nostro ordinamento, è stato esteso anche al servizio di informazione sui conti, al fine di garantire agli utenti dei servizi adeguata protezione con riguardo all'utilizzo di dati di pagamento da parte di soggetti terzi rispetto all'intermediario presso cui detengono il conto.

L'AISP, come il PISP, rientra tra i c.d. Third Party Providers (TPP), soggetti terzi che hanno il diritto di accedere ai conti dell'utente, se autorizzati da quest'ultimo, anche in assenza di un rapporto contrattuale con l'intermediario presso cui tali conti sono radicati (detto anche account servicing payment service provider – ASPSP).

Come il PISP, nemmeno l'AISP entra mai in possesso dei fondi dell'utente, che rimangono depositati presso i conti di cui il cliente è titolare.

Come funziona il servizio di informazione sui conti?

Il servizio è offerto attraverso tecnologie digitali, spesso tramite applicazioni sviluppate per specifici device (ad es. smartphone). L'utente installa l'applicazione sul proprio telefono e vi registra i propri conti accessibili online. A questo punto l'AISP può accedere ai conti registrati dell'utente e prestare anche ulteriori servizi (ad es. credit scoring, riconciliazione fatture), che devono però essere specificamente accettati dal cliente.

La prestazione del servizio di informazione sui conti è sottoposta a norme di sicurezza e ad obblighi informativi per la tutela dell'utente. L'AISP deve:

1. prestare il servizio solo dopo aver ricevuto un consenso esplicito da parte del cliente, che può essere rilasciato anche nel momento della conclusione del contratto quadro;
2. garantire che le credenziali del cliente non siano accessibili ad altri - a eccezione del cliente e degli intermediari titolari del conto - e che la loro trasmissione avvenga attraverso canali sicuri;
3. accedere solo alle informazioni dei conti registrati e alle relative operazioni di pagamento;
4. identificarsi presso l'ASPSP per ogni sessione di comunicazione, secondo modalità di comunicazione sicura;

5. non richiedere dati sensibili di pagamento collegati ai conti *(vai a obblighi di privacy)*. Per lo svolgimento del servizio di informazione sui conti, il nome del titolare e il numero del conto non costituiscono dati sensibili relativi ai pagamenti;
6. non utilizzare, accedere o archiviare dati per scopi diversi dall'esecuzione del servizio di informazione sui conti o degli altri servizi per i quali il cliente ha fornito il proprio consenso;
7. adempiere agli obblighi in materia di informativa precontrattuale previsti per la generalità dei servizi di pagamento, adattandoli al tipo di attività svolta. Tali operatori possono presentare l'informativa precontrattuale anche con modalità diverse da quelle previste per gli altri servizi di pagamento: ove offrano unicamente il servizio di informazione sui conti, non sono tenuti a predisporre il foglio informativo, il documento di sintesi o la copia del contratto idonea per la stipula *(vai a obblighi di trasparenza)*.

ATTENZIONE: *prima di registrare i propri conti per il servizio AIS, è opportuno verificare che l'AISP sia stato autorizzato nello Stato Membro in cui ha la propria sede legale e che sia iscritto nel relativo albo, in cui sono indicati anche tutti gli stati dell'Unione in cui è abilitato a prestare i propri servizi. Dal marzo 2019 è attivo il Registro EBA degli istituti di pagamento e degli istituti di moneta elettronica, in cui sono censiti tutti gli operatori autorizzati nell'Unione Europea e i paesi in cui sono abilitati a prestare i propri servizi. Possono prestare questo servizio anche le banche, censite nel Registro dell'EBA consultabile a questo link. (vai a rimborsi e responsabilità).*

L'utente deve fare molta attenzione, nel prestare il proprio consenso, all'eventuale autorizzazione allo svolgimento di servizi ulteriori rispetto a quello di AIS. L'eventuale richiesta, da parte dell'AISP, di essere autorizzato a cedere a terzi i propri dati va valutata con prudenza; essa non può essere condizione obbligatoria per l'offerta del servizio di informazione sui conti (vai a obblighi di privacy).

L'ASPSP deve consentire l'accesso ai conti da parte dell'AISP che si identifichi secondo le modalità stabilite dalle norme tecniche elaborate in sede europea.

Cosa deve fare il cliente in caso di accesso non autorizzato ai propri conti?

In caso di accesso non autorizzato ai propri conti o di cessione non autorizzata di dati a terzi, il cliente deve rivolgersi all'AISP o all'ASPSP, sulla base della fattispecie concreta verificatasi.

L'AISP è responsabile in caso di accesso ai conti in assenza di esplicito mandato conferito dal cliente, di accesso secondo modalità diverse rispetto alle pattuizioni contrattuali, nonché in caso di cessione a terzi di tali dati in mancanza di un preventivo esplicito consenso *(vai a obblighi di privacy)*.

L'ASPSP è responsabile nei confronti del cliente del mancato rispetto dell'obbligo di verifica della corretta identificazione e autenticazione dell'AISP al momento dell'accesso ai conti. Inoltre, l'ASPSP è chiamato a rispondere nei confronti del cliente anche nel caso in cui abbia consentito l'accesso all'AISP oltre quattro volte nell'arco di 24 ore (a meno che non risulti una diversa pattuizione contrattuale) o a seguito di revoca del consenso dell'utente. E' importante che il cliente comunichi tempestivamente al proprio ASPSP la revoca del consenso all'accesso ai conti da parte dell'AISP.

Torna a "Come si paga online?"

OBBLIGHI E TUTELE - schema riassuntivo

L'efficienza e la sicurezza dei pagamenti dipendono dal comportamento di tutti i soggetti coinvolti in una transazione di commercio elettronico: non solo gli intermediari che offrono il servizio di pagamento, ma anche i clienti che acquistano online un bene o un servizio e i commercianti che lo offrono.

Gli intermediari, in quanto operatori autorizzati all'offerta del servizio di pagamento, sono chiamati per legge al rispetto di un quadro articolato di obblighi, che attengono ai diversi profili di trasparenza informativa, correttezza, sicurezza e privacy.

I clienti devono rispettare essenzialmente obblighi di comportamento che attengono alla custodia degli strumenti di pagamento e delle credenziali di autenticazione e alla comunicazione in tempi brevi di eventuali fatti anomali (smarrimento, furto, esecuzione di operazioni non autorizzate). Questi obblighi sono previsti da disposizioni di legge e sono esplicitati e specificati nel contratto che regola la prestazione del servizio di pagamento.

I clienti sono tutelati da specifiche previsioni di legge che riconoscono il diritto al rimborso degli importi erroneamente o indebitamente addebitati; i clienti possono attivare diversi meccanismi di tutela per recuperare le somme: richiesta di rimborso rivolta direttamente all'intermediario, ricorso ai sistemi stragiudiziali di risoluzione della controversia (es. Arbitro Bancario Finanziario), ricorso all'Autorità Giudiziaria.

I casi di surcharge potranno essere segnalati all' Autorità Garante per la Concorrenza e il Mercato che verificherà se si tratta di pratiche commerciali scorrette e potrà, eventualmente, sanzionare gli esercenti.

Negli schemi che seguono sono riassunti gli obblighi che hanno, rispettivamente, intermediari e clienti e i divieti per i commercianti.

Intermediari

Tipologia di obbligo	Descrizione
Obblighi informativi	**fornire un'adeguata informativa in fase precontrattuale, al momento della stipula del contratto e nel corso del rapporto** *(Se vuoi saperne di più)*
Obblighi di correttezza	**non inviare strumenti di pagamento non richiesti dall'utente, se non per sostituire strumenti già in uso**
Obblighi in materia di spese	• **non addebitare spese per l'adempimento di obblighi informativi o per l'implementazione delle misure di sicurezza** • **trasferire la totalità dell'importo dell'operazione senza trattenere spese sull'importo trasferito** **se entrambi gli intermediari sono situati nell'Unione Europea, si applica il principio "share", in base al quale pagatore e beneficiario sostengono ciascuno le proprie tariffe**
Obblighi di esecuzione	**rispettare i tempi (di esecuzione, data valuta e disponibilità dei fondi,…) e modalità di esecuzione, con impegno alla rettifica in caso di mancato rispetto**
Obblighi di sicurezza	• **adottare le prescritte misure di sicurezza (SCA, crittografia, trattamento dati,…)** • **mettere a disposizione modalità per comunicare casi di furto, smarrimento, appropriazione indebita o frode** • **istituire meccanismi per inibire l'utilizzo degli strumenti di pagamento dopo la comunicazione di furto, smarrimento, appropriazione indebita o frode** *(Se vuoi saperne di più)*
Obblighi in materia di privacy	**adottare le misure di tutela e i presidi organizzativi richiesti dal GDPR** *(Se vuoi saperne di più)*

Clienti

Tipologia di obbligo	Descrizione
Obblighi di custodia	**custodire accuratamente gli strumenti di pagamento e le loro credenziali** *(Se vuoi saperne di più)*
Obblighi di comunicazione	**comunicare senza indugio all'intermediario, secondo le modalità previste nel contratto, lo smarrimento, il furto, l'appropriazione indebita o l'uso non autorizzato dello strumento** *(Se vuoi saperne di più)*
Obblighi contrattuali	**utilizzare lo strumento di pagamento in conformità con i termini esplicitati nel contratto e rispettare eventuali altri obblighi previsti nel contratto**

Commercianti

Tipologia di divieto	Descrizione
Divieto di surcharge	**il commerciante, beneficiario del pagamento, non può addebitare al pagatore spese relative all'utilizzo di specifici strumenti di pagamento**

Rimborsi e responsabilità
Spetta all'intermediario dimostrare che l'operazione di pagamento è stata autenticata, correttamente registrata e non ha subito le conseguenze di guasti tecnici o altri inconvenienti. ***L'intermediario è tenuto a rimborsare il cliente che lamenta un addebito non autorizzato a meno che non dimostri che questi abbia agito in modo fraudolento o non abbia adempiuto ai propri obblighi con dolo o colpa grave.*** *(Se vuoi saperne di più)*

Obblighi informativi degli intermediari

1. Premessa

Nelle fasi precedenti la stipula del contratto o l'esecuzione dell'operazione, gli intermediari devono consentire ai clienti di conoscere in tempo utile tutte le condizioni, anche economiche, che verranno applicate in relazione alla prestazione del servizio; successivamente, una volta che l'operazione di pagamento è stata eseguita, vanno rendicontati gli oneri effettivamente sostenuti e indicate le tempistiche di accredito a favore del beneficiario del pagamento.

2. Obblighi di trasparenza

2.1. Operazioni rientranti in un contratto quadro.

L'intermediario deve mettere a disposizione il foglio informativo relativo al contratto quadro del conto di pagamento e consegnare al cliente prima della conclusione del contratto alternativamente, il documento di sintesi delle condizioni contrattuali o la copia del contratto idonea per la stipula; tali documenti riportano tutte le informazioni prescritte dalla normativa, compresi i costi a carico dell'utente e le condizioni cui è subordinata la prestazione. Inoltre, per i contratti relativi a conti di pagamento offerti a consumatori, gli intermediari mettono a disposizione anche il "Documento informativo sulle spese" redatto in conformità del Regolamento (UE) 2018/34 del 28 settembre 2017, riportante tutte le spese che il consumatore è tenuto a pagare in relazione ai servizi collegati al conto di pagamento più rappresentativi a livello nazionale, indicati con la terminologia standardizzata europea e inclusi nell'elenco pubblicato dalla Banca d'Italia; il documento informativo sulle spese deve essere in ogni caso consegnato al consumatore prima della conclusione del contratto e riporta l'Indicatore dei Costi Complessivi (ICC) del conto, utile ad orientare la scelta del consumatore tra le diverse offerte di mercato; inoltre, immediatamente prima dell'esecuzione dell'operazione, l'intermediario deve fornire, su richiesta del cliente e secondo le modalità previste dal contratto, le informazioni sui costi che verranno applicati e sui tempi di esecuzione.

L'intermediario deve fornire un'informativa sulle operazioni eseguite contenente, tra l'altro, un riferimento univoco che consenta di individuare ciascuna di esse; ciò può avvenire sia subito dopo l'esecuzione di ciascuna operazione mediante la consegna di una ricevuta o in alternativa vi è il diritto del cliente – previsto nel contratto quadro – di richiedere un'informativa periodica almeno mensile (cd. estratto conto).

Ai consumatori titolari di un conto di pagamento, in aggiunta all'estratto conto e al documento di sintesi, – gli intermediari forniscono, gratuitamente e almeno una volta all'anno, un documento denominato "Riepilogo delle spese", redatto in conformità del Regolamento (UE) 2018/33 del 28

settembre 2017 , che riporta un riepilogo di tutte le spese sostenute dal consumatore nel periodo di riferimento nonché informazioni sugli interessi applicati sulle somme depositate o relativi ad eventuali sconfinamenti.

2.2. Singole operazioni di pagamento non rientranti in un contratto quadro.

Per le singole operazioni di pagamento non rientranti in un contratto quadro, sono previste modalità semplificate per ottemperare agli obblighi in materia di trasparenza. In questi casi, infatti, è previsto un set informativo più contenuto che può essere fornito o per il tramite di apparecchiature tecnologiche consultabili dal cliente (quest'ultimo può comunque richiedere che l'informativa sia fornita su supporto cartaceo o altro supporto durevole) oppure attraverso la consegna della copia del contratto idonea per la stipula. Per ciascuna operazione di pagamento eseguita deve essere fornita una ricevuta contenente, tra l'altro, un riferimento che consenta all'utente di individuare ogni operazione di pagamento, l'importo dell'operazione, tutte le spese, la data valuta dell'addebito o la data di ricezione dell'ordine di pagamento. A differenza di quanto previsto per i contratti quadro, l'intermediario può, a sua scelta, mettere a disposizione queste informazioni anziché consegnarle al cliente.

Se un ordine di pagamento per una singola operazione è trasmesso con uno strumento di pagamento contemplato da un contratto quadro con un altro intermediario, il prestatore della singola operazione può non fornire al cliente le informazioni che questi ha già ricevuto o riceverà in base al contratto quadro.

3. Obblighi di trasparenza in caso di servizio di disposizione di ordini di pagamento (PIS)

Se il servizio di disposizione di ordini di pagamento è prestato nell'ambito di un contratto quadro stipulato tra il PISP e l'utente, per consentire al cliente di conoscere in anticipo le condizioni economiche del servizio, il PISP deve mettere a disposizione il foglio informativo e consegnare al cliente, prima della stipula del contratto, la copia del testo contrattuale idoneo per la stipula; tali documenti riportano, tra le altre cose, l'importo delle commissioni applicabili al servizio nonché le modalità per prestare o revocare il consenso alla disposizione di un ordine di pagamento.

Nel caso di operazioni non rientranti in un contratto quadro, l'informativa precontrattuale viene fornita o per il tramite di apparecchiature tecnologiche consultabili dal cliente (quest'ultimo può comunque richiedere che l'informativa sia fornita su supporto cartaceo o altro supporto durevole) oppure attraverso la consegna della copia del contratto idonea per la stipula.

Nel corso della predisposizione dell'ordine di pagamento da parte del cliente, prima che questi confermi l'ordine, congiuntamente all'importo dell'operazione il PISP mostra anche le eventuali commissioni a suo favore a carico del cliente.

Subito dopo la prestazione del consenso da parte dell'utente, il PISP consegna una ricevuta contenente la conferma del buon esito dell'operazione di disposizione di ordine di pagamento, il riferimento univoco dell'operazione di pagamento e il relativo importo, nonché il riepilogo di tutte le eventuali commissioni pagate dall'utente a favore del PISP. Per le operazioni non rientranti in un contratto quadro, il PISP può mettere a disposizione le informazioni anziché consegnarle al cliente.

4. Obblighi di trasparenza in caso di servizio di informazione sui conti (AIS)

Gli operatori che offrono unicamente il servizio di informazione sui conti sono tenuti ad adempiere ai soli obblighi previsti in materia di informativa precontrattuale. Tali operatori possono presentare l'informativa precontrattuale anche con modalità diverse: non sono obbligati a redigere il foglio informativo, il documento di sintesi o la copia del contratto.

Torna a "Obblighi e tutele"

Obblighi di sicurezza degli intermediari

La Direttiva 2015/2366/CE (PSD2 –Direttiva sui Servizi di Pagamento) recepita nel nostro ordinamento con d.lgs. n. 218 del 2017, detta norme minime di sicurezza per l'offerta di servizi di pagamento e definisce un quadro giuridico di riferimento in grado di promuovere una revisione e un adeguamento continuo dei processi operativi e della stessa normativa alla evoluzione dei rischi tecnologici. Demanda all'Autorità Bancaria Europea (ABE) il compito di definire, con "Technical standard" e "Guidelines", le norme e le specifiche tecniche per diversi profili, tra cui l'individuazione di requisiti specifici per l'autenticazione forte e i possibili casi di esenzione.

1. Premessa

I servizi di pagamento sono soggetti a specifici requisiti tecnici e organizzativi di sicurezza, riguardanti sia i sistemi e le procedure utilizzati dagli intermediari sia gli strumenti di pagamento offerti ai clienti. Tali requisiti sono volti a garantire un livello base di sicurezza uniforme per tutti i servizi di pagamento elettronici regolamentati, al fine di minimizzare il rischio di frodi e favorire la fiducia dei cittadini nelle modalità di trasferimento della moneta.

Il livello di sicurezza di uno specifico strumento di pagamento dipende dal contesto di utilizzo e dalle ulteriori misure di sicurezza che gli intermediari decidono di predisporre in considerazione dei rischi ravvisati nel proprio modello di business. Per questa ragione, pur essendo fissato dalla normativa un livello minimo di sicurezza, i vari strumenti di pagamento presenti sul mercato sono caratterizzati, in generale, da livelli di sicurezza diversi.

2. Autenticazione forte (SCA)

Tra le principali misure di sicurezza previste dalla normativa, figura l'autenticazione forte del cliente (o SCA – *Strong Customer Authentication*). Si tratta di una procedura di autenticazione basata sull'uso di due o più elementi, classificati in almeno due categorie tra le seguenti:

- conoscenza (qualcosa che solo l'utente conosce, come una password o un PIN);
- possesso (qualcosa che solo l'utente possiede, come un token, o uno smartphone);
- inerenza (qualcosa che caratterizza l'utente, come l'impronta digitale).

Tali elementi (o credenziali di autenticazione) devono essere indipendenti, in modo che un'eventuale violazione di uno di essi non comprometta l'affidabilità degli altri. Su questa base, la normativa richiede ad esempio che se lo smartphone del cliente viene utilizzato per veicolare tutti gli elementi utilizzati per l'autenticazione, debbano essere adottate specifiche misure per la prevenzione e il contenimento del rischio di compromissione della sicurezza del dispositivo.

La procedura di autorizzazione di un pagamento tramite SCA deve garantire che:

- il codice di autorizzazione generato sulla base delle credenziali inserite dall'utente sia *monouso*, ovvero accettato una sola volta dal PSP;
- il codice di autorizzazione del pagamento sia legato indissolubilmente all'importo e al beneficiario: in questo modo, se carpito o intercettato, tale codice non può essere usato per altri pagamenti (i.e. pagamenti verso altri beneficiari o con diverso importo).

Fino a 500 euro, i PSP possono optare per l'esenzione dall'autenticazione forte del cliente a condizione che l'operazione di pagamento elettronico presenti un basso livello di rischio secondo i meccanismi di monitoraggio realizzati (cfr. *infra*) e che, per i pagamenti sotto la soglia, i propri sistemi di sicurezza consentano di mantenere il tasso di frode entro un limite fissato (cfr. tabella).

Tabella - Soglie di esenzione alla SCA e corrispondenti tassi di frode massimi consentiti (in percentuale del valore) per i pagamenti elettronici a distanza basati su carta e per i bonifici elettronici a distanza.

Valore della soglia di esenzione	Max. tasso di frode - carta	Max. tasso di frode – bonifico
€ 500	0,01 %	0,005 %
€ 250	0,06 %	0,01 %
€ 100	0,13 %	0,015 %

I pagamenti fino a 30 euro possono essere esentati dalla SCA a prescindere dal tasso di frode registrato; scatta però l'obbligo di SCA quando l'importo cumulativo delle precedenti operazioni di pagamento elettronico effettuate dall'utente superano i 100 Euro o, comunque, dopo 5 operazioni di pagamento consecutive eseguite senza SCA.

Un'altra importante opzione di esenzione dalla SCA riguarda i pagamenti verso i cosiddetti "beneficiari di fiducia": il PSP può dare ai clienti la possibilità di creare e aggiornare, tramite SCA, un elenco di beneficiari considerati affidabili ed esentare dalla SCA pagamenti dei propri clienti se il beneficiario è incluso nel rispettivo elenco.

La consapevolezza dei clienti sulle politiche di sicurezza adottate dai prestatori dei servizi di pagamento, in termini sia di misure di protezione predisposte che di esenzioni applicate, consente loro di scegliere uno strumento di pagamento anche valutandone la rispondenza alle proprie esigenze e alla propria sensibilità riguardo i profili di sicurezza. In ogni caso, poiché è il PSP (e non il cliente) a scegliere di avvalersi dell'esenzione per una certa transazione, se ne assume la responsabilità: qualora l'operazione esentata non sia stata autorizzata dal cliente, il PSP dovrà sempre rimborsare quest'ultimo, eccetto il caso in cui dimostri di essere stato vittima di una frode da parte dell'utente stesso.

3. Presidi di controllo tecnico-organizzativi

In aggiunta alla SCA, la normativa prevede ulteriori presidi di controllo di tipo tecnico-organizzativo, che concorrono a determinare il livello di sicurezza complessivo dei servizi di pagamento online. In particolare sono richiesti:

- presidi di controllo interno

- gli operatori devono dotarsi di meccanismi di monitoraggio delle operazioni che, tenendo conto degli aspetti che caratterizzano il normale comportamento dell'utente, consentano di rilevare operazioni di pagamento non autorizzate o fraudolente (un esempio tipico di operazione sospetta, che deve essere prontamente rilevata, è quello di un pagamento effettuato dopo un breve lasso temporale e da un luogo molto distante dal pagamento precedente);
- è obbligatorio il riesame delle misure di sicurezza: queste devono essere sottoposte periodicamente a test, nonché valutate, con riferimento al quadro giuridico applicabile, da revisori con competenze in materia di sicurezza informatica e pagamenti e indipendenti dal punto di vista operativo;

- notifiche da/verso i clienti
  - i clienti devono notificare senza indugio al prestatore dei servizi di pagamento, o al soggetto specificato da quest'ultimo, non appena ne abbiano conoscenza, lo smarrimento, il furto, l'appropriazione indebita o l'utilizzo non autorizzato dello strumento di pagamento; l'intermediario deve assicurare ai propri clienti la disponibilità in ogni momento di mezzi e modalità di comunicazione che consentano loro tale comunicazione tempestiva;
  - nel caso in cui l'intermediario sia vittima di un grave incidente operativo o di sicurezza, qualora gli interessi degli utenti siano messi a rischio, esso è tenuto a comunicare l'evento ai propri clienti, indicando tutte le misure a disposizione per attenuarne gli effetti.

    Si tratta di un importante presidio a tutela dell'utente, in assenza del quale l'utente non sarebbe messo in condizione di conoscere rischi concreti che potrebbero manifestarsi per la riservatezza dei propri dati finanziari o per la sicurezza degli stessi fondi detenuti nei propri conti.
  - l'intermediario può prevedere nel contratto con i propri clienti la facoltà di bloccare lo strumento di pagamento per fondati motivi di sicurezza; il blocco, in generale, deve essere comunicato tempestivamente al cliente, insieme ai motivi che lo hanno reso opportuno. Il cliente può richiedere lo sblocco dello strumento di pagamento tramite mezzi di cui l'intermediario assicura la disponibilità in ogni momento e lo sblocco o la sostituzione dello strumento deve in ogni caso essere effettuata dal PSP una volta cessati i motivi che ne hanno determinato il blocco.

    La possibilità per l'intermediario di bloccare (e sbloccare) tempestivamente lo strumento di pagamento può costituire una misura efficace a tutela dei fondi gestiti.

- segnalazioni all'Autorità competente e ad organismi di cooperazione
  - in caso di grave incidente riguardante l'operatività o la sicurezza di quest'ultima, anche qualora gli interessi finanziari degli utenti non siano messi a repentaglio, il PSP è tenuto è notificare senza indugio l'accaduto alla propria Autorità di riferimento;

- al fine di valutare il perseguimento dell'obiettivo – stabilito dalla PSD2 – di "*ridurre, al massimo grado possibile, il rischio di frode*", la normativa prevede che gli operatori forniscano, su base almeno annuale, dati statistici sulle frodi relative ai diversi strumenti di pagamento offerti all'Autorità competente (che a sua volta forniscono tali dati, in forma aggregata, all'ABE e alla BCE);
- un'ulteriore casistica da segnalare all'Autorità è quella in cui l'intermediario sospetti di essere stato frodato dal proprio cliente e per tale ragione sospenda il rimborso dell'operazione disconosciuta.

I PSP possono innalzare il livello di consapevolezza dei rischi insiti nel proprio modello di business e tenersi aggiornati sulle minacce da fronteggiare scambiando informazioni su incidenti occorsi e minacce di sicurezza rilevate, ad esempio aderendo ad organismi cooperativi specializzati nel campo della cyber security, quali il CERTFin, struttura governata dalla Banca d'Italia e dall'ABI, dedicata alla sicurezza cibernetica del settore finanziario italiano.

Torna a "Obblighi e tutele"

Obblighi degli intermediari in materia di privacy

Il Regolamento europeo sulla protezione dei dati (GDPR) valorizza l'importanza del consenso dell'interessato all'utilizzo dei propri dati e impone agli intermediari l'adozione di specifici presidi organizzativi che si aggiungono a quelli previsti dalla PSD2 in materia di sicurezza.

1. Premessa

Il *Regolamento (UE) 2016/679 (GDPR - Regolamento Generale sulla Protezione dei Dati)* disciplina nell'Unione europea il trattamento dei dati personali; tale regolamento è applicabile in tutti gli Stati membri dal 25 maggio 2018. L'ambito di applicazione territoriale si estende, al ricorrere di alcune condizioni, anche al di fuori del territorio dell'Unione; norme specifiche regolano il trasferimento di dati verso paesi terzi od organizzazioni internazionali.

Il GDPR rafforza il ruolo della informativa come strumento di trasparenza e la centralità del consenso dell'interessato al trattamento dei propri dati; il trattamento è consentito solo per scopi specifici e dichiarati, nei limiti del necessario. È previsto anche il diritto di ottenere la cancellazione dei propri dati personali (cosiddetto "diritto all'oblio"). Il consenso dell'interessato al trattamento dei dati personali deve essere libero, specifico, informato e inequivocabile, anche se espresso attraverso mezzi elettronici o con un semplice flag. Riguardo ai dati cd. "sensibili", ovvero i dati di cui all'art. 9 del GDPR (cfr. paragrafo 2.1), il consenso deve sempre riferirsi esplicitamente a tale tipo di informazioni. Gli interessati dovranno inoltre sapere se i loro dati sono trasmessi al di fuori dell'Ue e con quali garanzie; oggetto di informativa è anche il diritto di revocare il consenso a trattamenti specifici, in ogni momento.

2. Applicazione del GDPR ai servizi di pagamento

La *Direttiva 2015/2366/CE (PSD2 – Direttiva sui Servizi di Pagamento),* recepita nel nostro ordinamento con d.lgs. n. 218 del 2017, non costituisce lex specialis rispetto al GDPR. Il Regolamento dispiega i propri effetti dunque anche nell'ambito dei servizi di pagamento. Infatti, gli intermediari che offrono servizi di pagamento devono porre in essere una serie di attività volte a recepire nella propria organizzazione interna le innovazioni introdotte dal GDPR; tra queste ultime rilevano: la designazione di un responsabile della protezione dei dati, l'istituzione di un registro delle attività di trattamento e l'adozione di accorgimenti quali attività preventive di pianificazione e progettazione per la protezione dei dati (**privacy by design**) e misure di sicurezza da attuare nel continuo (**privacy by default**), per garantire il presidio del trattamento, i limiti allo stesso e la corretta conservazione dei dati.

Alcune misure organizzative e tecniche previste dal GDPR si sovrappongono, e in parte si aggiungono, a quelle stabilite dalla PSD2 e dalle *linee guida EBA in materia di sicurezza*. Per esempio, il Regolamento introduce obblighi di segnalazione per gli intermediari dei cd. *data breach* all'Autorità nazionale per la protezione dei dati. Tali obblighi si sommano agli obblighi di reporting alle autorità nazionali competenti previsti per gli incidenti gravi sulla base della PSD2 e delle linee guida EBA.

3. GDPR e PSD2

Riguardo ai rapporti tra GDPR e PSD2, sono emerse esigenze di armonizzazione, in relazione, in particolare, alla nozione di dati cd. "sensibili" e alla natura del consenso prestato dall'interessato/utente.

3.1. La nozione di dati sensibili

Preliminarmente, si osserva che la definizione di "dati sensibili" secondo la PSD2 e quella di "categorie particolari di dati" ex art. 9 GDPR (tradizionalmente considerati "dati sensibili") non coincidono. I primi sono infatti dati che «possono essere usati per commettere frodi»" (cfr. art. 4, punto 32, della PSD2); tra questi sono espressamente incluse le credenziali di sicurezza personalizzate fornite all'utente a fini di autenticazione, ovvero al fine di «verificare l'identità» dell'utente stesso oppure «la validità dell'uso di uno specifico strumento di pagamento» (cfr. art. 4, punti 29 e 31, della PSD 2). Non costituiscono, invece, dati sensibili relativi ai pagamenti il nome del titolare del conto e il numero del conto.

Le "categorie particolari di dati" ai sensi del GDPR sono invece riferite a dati personali che rivelano origini razziali o etniche, opinioni politiche, credenze religiose, convinzioni filosofiche o appartenenza sindacale, nonché dati genetici e dati biometrici, o relativi alla salute e alla vita sessuale di una persona. Tale definizione è generale, nel senso che la relativa disciplina si applica ogni qualvolta si tratti, anche nell'ambito dei servizi di pagamento, questo tipo di dati. La nozione di dati sensibili ai sensi della PSD2 non è in contrasto con il GDPR perché più cautelativa, ad esempio, laddove viene esclusa la possibilità per gli *intermediari che svolgono i servizi di disposizione di ordini di pagamento (PISP)* e *di informazione sui conti (AISP)*, rispettivamente, di conservare e richiedere dati sensibili relativi ai pagamenti collegati ai conti di pagamento.

E' utile osservare che una coincidenza nella tipologia di dati ex art. 9 GDPR e di dati sensibili ai sensi della PSD2 può realizzarsi ove si tratti di dati biometrici che vengano sfruttati ai fini di autenticazione dell'utente di un servizio di pagamento (e che costituiscono quindi un elemento delle credenziali di sicurezza). In tal caso si applicheranno, ciascuna in relazione al proprio contesto, entrambe le normative.

3.2. Il consenso al trattamento dei dati

a) Il consenso dell'interessato

Quanto alla nozione di consenso dell'interessato al trattamento dei dati contenuta nelle due normative in esame, lo *European Data Protection Board (EDPB)* ha chiarito che gli intermediari possono trattare i dati necessari all'esecuzione del servizio di pagamento sulla base di uno specifico ed esplicito consenso espresso preventivamente sul contratto. Il consenso previsto dalla PSD2 (art. 94) avrebbe pertanto natura contrattuale, con ciò distinguendosi dal consenso richiesto ai sensi del GDPR. Il GDPR (art. 6, c.1., lett.b) prevede, tra l' altro, quale presupposto di liceità del trattamento, che esso sia necessario per l'esecuzione di un contratto di cui l'interessato è parte; ciò premesso, da una lettura combinata del GDPR e della PSD2, come sopra interpretata, si evince che, una volta approvato il contratto per l'esecuzione di un servizio di pagamento, l'interessato non debba

ulteriormente prestare il consenso se il trattamento è funzionale all'esecuzione del contratto stesso (*cfr. anche Linee guida sul consenso ai sensi del regolamento (UE) 2016/679 del 28 novembre 2017, come modificate e adottate da ultimo il 10 aprile 2018*).

b) Il consenso del beneficiario (cd. silent parties)

Secondo l'EDPB, inoltre, all'intermediario che presta *servizi di informazione sui conti* non occorre uno specifico consenso per il trattamento dei dati del beneficiario del pagamento, posto che l'utilizzo di questi dati avviene, in conformità al GDPR, per il perseguimento di un legittimo interesse all'esecuzione del servizio (art. 6,c.1., lett.f).

c) Legittimità dell'accesso ai dati da parte delle terze parti

Allo stesso modo, *l'intermediario presso cui è aperto il conto (ASPSP)* può legittimamente consentire l'accesso ai dati dell'utente da parte degli intermediari che offrono il *servizio di disposizione di ordini di pagamento* e *di informazione sui conti* - che abbiano acquisito il consenso dell'utente - in virtù di specifiche disposizioni della PSD2 (artt. 66 e 67) - che obbligano gli ASPSP a tale ostensione - e, pertanto, in conformità al GDPR, secondo cui il trattamento dei dati in esecuzione di un obbligo di legge è lecito.

Torna a "Obblighi e tutele"

Obblighi di diligenza e di comunicazione del cliente

1. Premessa

Per assicurare efficienza e sicurezza nell'offerta di servizi di pagamento, gli obblighi posti in carico agli intermediari sono integrati con quelli posti in capo ai clienti. Il mancato rispetto degli obblighi rileva ai fini del rimborso da parte degli intermediari (*Vai a Rimborsi e responsabilità*).

Di seguito sono elencati gli obblighi previsti dalla legge cui è tenuto l'utente; tali obblighi sono solitamente richiamati anche nel contratto tra l'utente e l'intermediario e possono essere integrati da ulteriori obblighi posti in capo alla clientela che sono stabiliti pattiziamente dalle parti (obblighi contrattuali) e prevedono particolari cautele nell'utilizzo degli strumenti di pagamento.

2. Obblighi di diligenza

Il cliente è tenuto a prestare diligenza nella custodia delle credenziali identificative per l'accesso ai conti e dispositive per l'esecuzione delle operazioni di pagamento. Egli è tenuto inoltre alla verifica delle transazioni effettuate a valere sul proprio conto.

ATTENZIONE: *Nel caso di utilizzo online l'utente si autentica mediante l'uso di credenziali che assumono connotati digitali e devono poter essere inviate via Internet e controllate con mezzi automatici dagli intermediari. L'utente può contribuire alla sicurezza dell'ambiente in cui opera ponendo attenzione al proprio personal computer o qualunque device utilizzato, ad esempio verificare la sicurezzo della connessione del sito su cui si sta navigando (es. controllare che l'indirizzo sia preceduto dall'immagine di un lucchetto e dalla dicitura"https:") .*

3. Obblighi di comunicazione

Il cliente deve comunicare tempestivamente all'intermediario eventuali irregolarità nella prestazione del servizio. In particolare, vi è l'obbligo di comunicare senza indugio, non appena ne viene a conoscenza, che si è verificata un'operazione di pagamento non autorizzata o non correttamente eseguita, al fine di richiederne la rettifica.

ATTENZIONE: *Per consentire un più attento monitoraggio dell'utilizzo degli strumenti di pagamento è consigliabile, ove disponibile, l'attivazione di strumenti messi a disposizione dagli intermediari per favorire il monitoraggio delle operazoni disposte tramite gli strumenti di pagamento (ad esempio, il servizio di sms alert* o *quello di notifica via app).*

Il cliente deve comunicare all'intermediario, non appena se ne accorge, il furto o lo smarrimento degli strumenti di pagamento e/o delle credenziali, utilizzando i contatti che gli intermediari devono mettere a disposizione dei clienti a questi fini.

ATTENZIONE: E' importante verificare di essere sempre in possesso degli strumenti di pagamento e delle relative credenziali e controllare regolarmente le transazioni effettuate sul proprio conto, comunicando tempestivamente all'intermediario eventuali irregolarità nella prestazione del servizio.

Torna a "Obblighi e tutele"

Rimborsi e responsabilità

1. Premessa

La corretta esecuzione di un'operazione di pagamento dipende dal comportamento congiunto di intermediari e clienti. Il legislatore attribuisce agli intermediari l'onere di strutturare l'operazione di pagamento in modo sicuro e di fornire al cliente mezzi sicuri per l'esecuzione. I clienti devono rispettare specifiche norme di comportamento che tutelano loro stessi e il sistema.

2. Obbligo di rimborso dell'intermediario e onere della prova in caso di operazioni non autorizzate

Quando un cliente lamenta di aver subito un'operazione da lui non autorizzata spetta all'intermediario dimostrare che l'operazione di pagamento è stata autenticata, correttamente registrata e non ha subito le conseguenze di guasti tecnici o altri inconvenienti. L'astratta riconducibilità dell'operazione al titolare del conto o dello strumento non impedisce al cliente di disconoscerla se non ritiene di averla autorizzata.

In questi casi, l'intermediario è tenuto a rimborsare l'utente salvo dimostrare che:

- il suo cliente abbia agito con intento fraudolento e voglia quindi disconoscere operazioni effettivamente autorizzate per ottenere indebitamente il riaccredito delle somme addebitategli;
- il suo cliente non abbia adempiuto, con dolo o colpa grave, agli obblighi di custodia, di comunicazione e/o a quelli contrattuali; questo però è possibile solo se l'operazione di pagamento è stata eseguita con misure di sicurezza rafforzate (*vai ad Obblighi di sicurezza*).

ATTENZIONE: Il cliente, che non ha agito con intento fraudolento, è sempre rimborsato quando il pagamento è stato eseguito dall'intermediario senza richiedere forme di autenticazione forte (SCA). Viceversa, se il pagamento è stato effettuato con SCA, non solo il cliente che ha agito in modo fraudolento, ma anche quello che non abbia adempiuto con colpa grave ai suoi obblighi, ad esempio nella custodia degli strumenti, potrebbe non essere rimborsato. Se vi è stato furto o smarrimento dello strumento il cliente potrebbe essere chiamato a pagare una franchigia di 50 euro fino alla comunicazione all'intermediario dell'avvenuto furto o smarrimento, sempre che se ne sia potuto rendere conto. Sono gli intermediari, e non il cliente, che decidono se in una determinata operazione devono essere richieste, o meno, forme di SCA; è proprio per questo che il legislatore tutela di più il cliente quando l'intermediario ha deciso di non applicare la SCA. Gli intermediari ricercheranno di volta in volta il miglior equilibrio fra l'applicazione della SCA, che rende meno fluida la customer experience, e la non applicazione della SCA, che rende la transazione più veloce.

In via generale, l'intermediario deve eseguire il rimborso – anche se in via provvisoria – immediatamente, e comunque al massimo entro la giornata operativa successiva alla segnalazione ricevuta dal cliente; solo nel caso in cui l'intermediario abbia motivati sospetti di frode da parte del cliente può sospendere il rimborso, comunicandolo per iscritto alla Banca d'Italia. Se l'intermediario rimborsa, ma dalle analisi successive valuta che il cliente non aveva diritto a tale rimborso, può

recuperare la somma. Se il cliente non è d'accordo può presentare un reclamo all'intermediario e, successivamente, un ricorso all'Arbitro Bancario Finanziario che decide sulla controversia.

Il cliente ha, in via generale, 13 mesi di tempo dall'addebito per chiedere il rimborso di un'operazione che non ritiene sia stata da lui autorizzata o correttamente eseguita dall'intermediario. La richiesta di rettifica può avvenire anche in un momento successivo, qualora l'intermediario abbia omesso di fornire o mettere a disposizione dell'utente le informazioni relative all'operazione di pagamento: è onere dell'intermediario dimostrare di aver adempiuto a tale obbligo.

ATTENZIONE: *Anche se sono previsti 13 mesi di tempo per la richiesta del rimborso per un'operazione non autorizzata, il cliente deve comunque darne comunicazione non appena venutone a conoscenza. Una segnalazione tempestiva agevola il recupero dell'importo e dimostra, da parte del cliente, attenzione alla tenuta del proprio conto.*

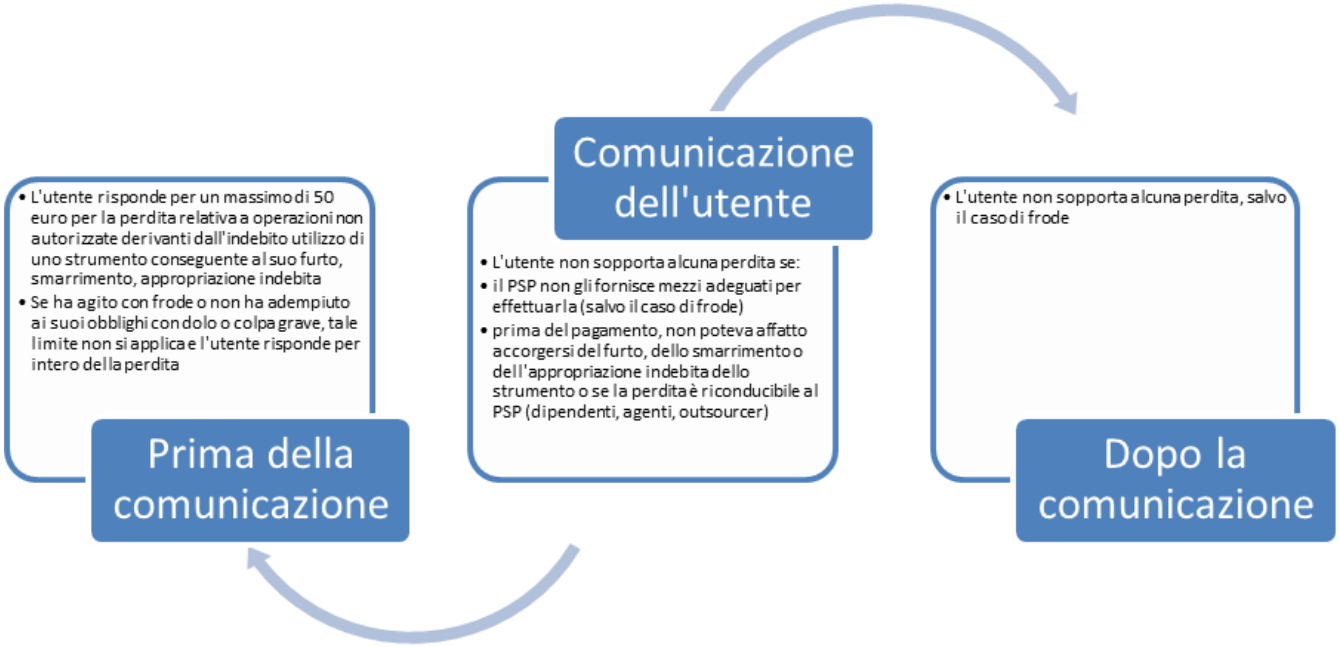
3. Furto, smarrimento e obbligo di rimborso dell'intermediario

Un caso particolare riguarda le operazioni non autorizzate in caso di furto, smarrimento o appropriazione indebita dello strumento di pagamento.

Il legislatore vuole incentivare i clienti a comunicare tempestivamente gli eventi sopra citati, comportamento questo complementare all'obbligo di custodia. La normativa, pertanto, stabilisce una franchigia non superiore a 50 euro che il cliente può dover sopportare per le operazioni non autorizzate effettuate fino al momento della comunicazione. Dopo la comunicazione, invece, gli intermediari possono bloccare gli strumenti e, pertanto, il cliente è tenuto indenne dalle conseguenze di ogni operazione eventualmente eseguita. Tuttavia, se l'utente agisce in maniera fraudolenta l'art. 12 d.lgs. 11/2010 prevede che questi risponda anche delle operazioni avvenute dopo la comunicazione e prima che l'intermediario disponga il blocco dello strumento.

Il cliente – salvo il caso in cui abbia agito in modo fraudolento – non sopporta alcuna perdita – e quindi neppure il pagamento nel limite dei 50 euro – se lo smarrimento, la sottrazione o l'appropriazione indebita dello strumento di pagamento non potevano essere notati prima del pagamento, oppure se la perdita è stata causata da azioni riconducibili all'intermediario o ad altri soggetti intervenuti nell'esecuzione dell'operazione (ad es. dipendenti, agenti, succursali etc.).

Il cliente può essere chiamato a rispondere dell'intera perdita relativa a operazioni di pagamento non autorizzate derivanti dall'utilizzo indebito dello strumento di pagamento conseguente al suo furto,smarrimento o appropriazione indebita, nel caso abbia agito in modo fraudolento o non abbia adempiunto ai propri obblighi con dolo o colpa grave.



4. Misure rafforzate di tutela nelle transazioni di pagamento iniziate dal beneficiario

Nelle operazioni di pagamento eseguite su iniziativa del beneficiario, il pagatore non avvia direttamente l'operazione di pagamento, ma subisce un addebito a suo carico, ordinato dal beneficiario che agisce sulla base di un'autorizzazione che gli ha dato il cliente stesso. Per questo tipo di operazioni non è mai richiesta la SCA (vedi scheda sicurezza) perché forme di autenticazione forte presuppongono la presenza del pagatore nel momento del pagamento e un suo comportamento attivo.

Per tutte le ipotesi in cui il trasferimento, pur se preventivamente autorizzato, non corrisponda alle sue ragionevoli aspettative, il cliente ha diritto al rimborso al ricorrere di entrambe le seguenti condizioni:

1) l'indeterminatezza dell'importo da trasferire al momento in cui il pagatore ha autorizzato il pagamento (è il caso, ad esempio, di un addebito preautorizzato per il pagamento della bolletta telefonica o dell'addebito dell'importo speso con la carta di credito);

2) l'importo trasferito sia superiore a quello che il pagatore avrebbe potuto ragionevolmente attendersi, avuto riguardo al suo precedente modello di spesa, le condizioni del contratto quadro e le circostanze del caso.

Una volta che l'utente abbia dichiarato la sussistenza delle condizioni di cui sopra, l'intermediario può chiedergli di produrre documenti e ogni altro elemento utile a provare quanto affermato. In particolare, la condizione di cui al numero 2) ha carattere soggettivo e va valutata caso per caso: è tuttavia possibile che gli intermediari definiscano criteri oggettivi, al ricorrere dei quali la differenza tra importo atteso e importo addebitato possa ritenersi "considerevole".

Nel contratto quadro le parti possono escludere il diritto al rimborso nei casi in cui: a) il pagatore abbia autorizzato direttamente il proprio intermediario; b) l'intermediario o il beneficiario abbiano fornito al pagatore le informazioni sulla futura operazione di pagamento almeno quattro settimane prima della sua esecuzione, secondo quanto concordato nel contratto quadro.

Il rimborso va richiesto entro otto settimane dalla data di addebito e deve essere corrisposto entro dieci giornate operative dalla ricezione della richiesta. In caso di rifiuto, l'intermediario, sempre nel termine di dieci giorni, deve fornire al pagatore una giustificazione del diniego e contestualmente comunicargli la possibilità di presentare un esposto alla Banca d'Italia ovvero di ricorrere all'ABF.

Nel caso in cui l'operazione sia stata richiesta dal beneficiario senza alcuna autorizzazione da parte del cliente, il cliente ha 13 mesi di tempo per chiedere il rimborso dell'importo. Anche in questo caso il rimborso non è dovuto se l'intermediario dimostra che il cliente ha agito in modo fraudolento.

5. Ulteriori misure di tutela offerte all'utente di servizi di pagamento

Se, dopo aver correttamente autorizzato la transazione di pagamento, l'utente desidera recedere dal contratto di acquisto, si applicherà la disciplina ordinaria prevista dal Codice civile e dal Codice del consumo. La transazione di pagamento è stata infatti correttamente autorizzata dal pagatore e non vi sono i presupposti normativi per il suo disconoscimento. Tuttavia alcuni intermediari e alcuni gestori di circuiti di pagamento offrono alla propria clientela garanzie aggiuntive, consentendo il rimborso, a specifiche condizioni, dell'operazione di pagamento effettuata.

Torna a "Obblighi e tutele"

GLOSSARIO

Acquirer – convenzionatore – prestatore di servizi di pagamento che convenziona un beneficiario, di solito un negoziante, per accettare e trattare operazioni di pagamento con carta che danno luogo a un trasferimento di fondi allo stesso beneficiario.

AIS – servizio di informazione sui conti (*account information service*) – un servizio online che fornisce informazioni consolidate relativamente a uno o più conti di pagamento detenuti dall'utente di servizi di pagamento presso un altro prestatore di servizi di pagamento o presso più prestatori di servizi di pagamento.

AISP – prestatore di servizi di informazione sui conti (*account information service provider*) – intermediario che offre il servizio di AIS.

ASPSP – prestatore di servizi di pagamento di radicamento del conto (*account servicing payment service provider*) – un prestatore di servizi di pagamento che offre e gestisce un conto di pagamento per un pagatore.

Autenticazione – la procedura che consente al prestatore di servizi di pagamento di verificare l'identità di un utente di servizi di pagamento o la validità dell'uso di uno specifico strumento di pagamento.

Beneficiario – una persona fisica o giuridica che è il destinatario dei fondi che sono stati oggetto di un'operazione di pagamento.

Bonifico – operazione di pagamento che permette a un pagatore di accreditare fondi sul conto del beneficiario, addebitando il proprio conto.

Carta di credito – carta rilasciata da un intermediario emittente sulla base di un contratto; essa consente acquisti presso gli esercenti convenzionati e prelievi di contante presso gli sportelli automatici. Le somme utilizzate sono restituite dal cliente all'emittente attraverso un addebito differito sul suo conto in un'unica soluzione (modalità *charge*), oppure secondo un piano rateale che prevede di norma la corresponsione di interessi (modalità *revolving*).

Carta di debito – carta rilasciata da un intermediario e abbinata a un conto. Consente acquisti presso gli esercenti convenzionati e prelievi di contante da sportelli automatici. A differenza della carta di credito, le singole operazioni vengono addebitate di volta in volta sul conto del debitore.

Carta di pagamento – una categoria di strumenti di pagamento che comprende carta di debito, carta di credito e carta prepagata.

Carta prepagata – carta rilasciata da una banca o da un istituto di moneta elettronica su cui viene caricata moneta elettronica.

CBPII – Card based payment instrument issuer – emittente, diverso da quello che offre il conto, di una carta dissociata dal conto dell'utente**.**

Chargeback – procedura con la quale vengono gestiti all'interno del cirucuito di carte, fra gli intermediari coinvolti, gli addebtiti e gli accrediti conseguenti alle richieste di rimborso dei pagamenti effettuati da parte dei titolari di carte di credito.

Circuito di carte di pagamento – piattaforma costituita dal complesso di regole e procedure che consentono di effettuare e ricevere pagamenti attraverso l'utilizzo di una determinata carta di pagamento.

Commissione interbancaria (interchange fee) – commissione applicata per ogni operazione direttamente o indirettamente, ad esempio mediante un terzo, tra l'emittente e il soggetto convenzionatore in relazione a un'operazione di pagamento basata su carta.

Consumatore – una persona fisica che, nei contratti di servizi di pagamento contemplati dalla presente direttiva, agisce per scopi estranei alla sua attività commerciale o professionale.

Conto di pagamento – un conto aperto presso un intermediario, a nome di uno o più utilizzatori di servizi di pagamento, per l'esecuzione di operazioni di pagamento.

Credit scoring – un metodo statistico e automatizzato utilizzato da banche e intermediari finanziari (in genere per la concessione del credito al consumo), che, sulla base di informazioni fornite dal cliente, attribuisce un punteggio (*score*) sul rischio di insolvibilità dello stesso.

Emittente di carta di pagamento – intermediario che fornisce al pagatore una carta per disporre operazioni di pagamento.

IBAN - International Bank Account Number – codice alfanumerico composto di 27 caratteri che individua univocamente un conto di pagamento.

Intermediario – cfr. Prestatore di servizi di pagamento.

Moneta elettronica – il valore monetario memorizzato elettronicamente, ivi inclusa la memorizzazione magnetica, rappresentato da un credito nei confronti dell'emittente che sia emesso dietro ricevimento di fondi per effettuare operazioni di pagamento e che sia accettato da persone fisiche o giuridiche diverse dall'emittente di moneta elettronica.

Operazione di pagamento – l'atto, disposto dal pagatore o per suo conto o dal beneficiario, di collocare, trasferire o ritirare fondi, indipendentemente da eventuali obblighi sottostanti tra il pagatore e il beneficiario.

Operazione di pagamento basata su carta (card based payment transaction) – servizio basato sull'infrastruttura e le regole commerciali di un circuito di carte di pagamento (es. Bancomat, Mastercard, Visa) per effettuare un'operazione tramite carta di pagamento.

Ordine di pagamento – un'istruzione data da un pagatore o da un beneficiario al proprio prestatore di servizi di pagamento con la quale viene chiesta l'esecuzione di un'operazione di pagamento.

Pagatore – una persona fisica o giuridica che autorizza l'ordine di pagamento.

Pass-through wallet – un "contenitore virtuale" attivo su un dispositivo informatico sul quale l'utente registra i propri strumenti di pagamento. Quando si effettua una transazione con questa tipologia di *wallet*, si utilizzano, tramite le loro credenziali, gli strumenti di pagamento ivi registrati.

PIS – servizio di disposizione di ordine di pagamento (*payment initiation service*) – un servizio che dispone l'ordine di pagamento su richiesta dell'utente di servizi di pagamento relativamente a un conto di pagamento detenuto presso un altro prestatore di servizi di pagamento.

PISP – prestatore di servizi di disposizione di ordine di pagamento (*payment initiation service provider*) – intermediario che presta il servizio di PIS.

POS (*point of sale*) – dispositivo, fisico o virtuale, utilizzato dai commercianti per l'accettazione di pagamenti con carte di pagamento

PSP – prestatore di servizi di pagamento (*payment service provider*) – uno dei seguenti soggetti: banche, Poste, istituti di moneta elettronica e istituti di pagamento.

SCA – **autenticazione forte del cliente** (*strong customer authentication*)– un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione.

Staged wallet – uno strumento di pagamento che può essere utilizzato direttamente per effettuare transazioni online. Solitamente corrisponde a un conto di moneta elettronica che viene ricaricato attraverso un altro strumento di pagamento abbinato (ad esempio con carta di pagamento o con bonifico).

Strumento di pagamento – un dispositivo personalizzato e/o insieme di procedure concordate tra l'utente di servizi di pagamento e il prestatore di servizi di pagamento e utilizzate per disporre un ordine di pagamento.

Surcharge – spesa applicata dal beneficiario, sotto forma di sovrapprezzo, a carico del pagatore e relativa all'utilizzo di uno specifico strumento di pagamento.

TPP (*third party providers*) – gli intermediari che si relazionano con l'ASPSP per la prestazione dei servizi di pagamento; essi includono PISP, AISP e CBPII.

Utente di servizi di pagamento (o utilizzatore di servizi di pagamento) – persona fisica o giuridica che si avvale di un servizio di pagamento in qualità di pagatore, di beneficiario o di entrambi.

Torna a "Introduzione"

n

RIEPILOGO DELLE PRINCIPALI FONTI NORMATIVE DI RIFERIMENTO

- Regolamento delegato (UE) 2018/389 della Commissione del 27 novembre 2017 che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri.
- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/C (Regolamento Generale sulla protezione dei dati).
- Regolamento (UE) 2015/751 del Parlamento europeo e del Consiglio del 29 aprile 2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta.
- Regolamento (UE) 2012/260 del Parlamento europeo e del Consiglio del 14 marzo 2012 che stabilisce i requisiti tecnici e commerciali per i bonifici e gli addebiti diretti in euro e che modifica il regolamento (CE) n. 924/2009 (cd. Regolamento SEPA).
- Direttiva (UE) 2015/2366 del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno, che modifica le direttiva 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE. PSD2 (*Revised Payment Service Directive*).
- Direttiva 2007/64/CE del Parlamento europeo e del Consiglio del 13 novembre 2007, relativa ai servizi di pagamento nel mercato interno, recante modifica delle direttive 97/7/CE, 2002/65/CE, 2005/60/CE e 2006/48/CE, che abroga la direttiva 97/5/CE (*Payment Service Directive*).
- D. lgs. 15 dicembre 2017, n. 218. Recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE, nonché adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta.
- D. lgs. 27 gennaio 2010, n. 11. Attuazione della direttiva 2007/64/CE, relativa ai servizi di pagamento nel mercato interno, recante modifica delle direttive 97/7/CE, 2002/65/CE, 2005/60/CE, 2006/48/CE, e abroga la direttiva 97/5/CE.
- D. lgs. 1° settembre 1993, n. 385: Testo unico delle leggi in materia bancaria e creditizia (TUB).
- Circolare della Banca d'Italia n. 285 del 17 dicembre 2013 e successive modifiche. Disposizioni di vigilanza per le banche.
- Provvedimento della Banca d'Italia del 23 luglio 2019. Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica.
- Provvedimento della Banca d'Italia del 29 luglio 2009 e successive modifiche. Trasparenza delle operazioni e dei servizi bancari e finanziari.
- EBA/GL/2020/01 del 22 gennaio 2020. Modifiche agli orientamenti EBA in materia di obblighi di segnanazione per i dati sulle frodi ai sensi della PSD2.
- EBA/GL/2018/07 del 4 dicembre 2018. Orientamenti EBA sulle condizioni per beneficiare dell'esenzione dal meccanismo di emergenza a norma dell'articolo 33, paragrafo 6, del regolamento (UE) 2018/389 (norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri).

- EBA/GL/2018/05 del 17 settembre 2018. Orientamenti EBA in materia di obblighi di segnalazione per i dati sulle frodi, ai sensi dell'articolo 96, paragrafo 6, della PSD2.
- JC 2014/43 del 27 maggio 2014. Joint Committee. Orientamenti sulla gestione dei reclami per il settore degli strumenti finanziari (ESMA) e per il settore bancario (ABE).

Torna a "Introduzione"