



# Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento: overview della nuova disciplina europea sui servizi di pagamento.



Il 28 giugno 2023 la Commissione europea ha presentato alcune proposte legislative, identificate collettivamente come "Financial data access and payments package", volte a promuovere l'innovazione e la concorrenza nel settore dei pagamenti.

In particolare, il "pacchetto" comprende la terza Direttiva sui Servizi di Pagamento ("PSD3" - "Payment Services Directive"<sup>1</sup>), il nuovo Regolamento sui Servizi di Pagamento (PSR - "Payment Services Regulation"<sup>2</sup>) e il quadro normativo per l'accesso ai dati finanziari (FIDA - "Financial Data Access"). Lo stesso giorno, la Commissione ha, inoltre, pubblicato il cosiddetto "Pacchetto Moneta Unica" relativo all'uso del contante e all'Euro digitale. I nuovi testi legislativi in materia di servizi di pagamento abrogheranno e, contestualmente, sostituiranno la seconda direttiva sui servizi di pagamento (c.d. "PSD2")<sup>3</sup> e la seconda direttiva sulla moneta elettronica (EMD2)<sup>4</sup>, combinando le relative disposizioni in materia di servizi di pagamento e di moneta elettronica nell'ambito di una disciplina unitaria.

Nell'ambito della procedura legislativa - al fine di fornire ai parlamentari europei una panoramica dettagliata sull'attuazione, l'implementazione e l'efficacia della legislazione europea sui servizi di pagamento -, il 17 luglio u.s., il Servizio Europeo di Ricerca Parlamentare del Parlamento Europeo ha pubblicato un briefing<sup>5</sup> relativo alla revisione della Direttiva (UE) 2015/2366 sui servizi di pagamento.



<sup>1</sup>Proposta di Direttiva del Parlamento Europeo e del Consiglio relativa ai servizi di pagamento e ai servizi di moneta elettronica nel mercato interno, disponibile a: [https://eur-lex.europa.eu/resource.html?uri=cellar:e09b163c-1687-11e8-806b-01aa75ed71a1.0009.02/DOC\\_1&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar:e09b163c-1687-11e8-806b-01aa75ed71a1.0009.02/DOC_1&format=PDF).

<sup>2</sup>Proposta di Regolamento del Parlamento Europeo e del Consiglio relativa ai servizi di pagamento e ai servizi di moneta elettronica nel mercato interno, disponibile a: [https://eur-lex.europa.eu/resource.html?uri=cellar:04cc5bd5-196f-11e8-806b-01aa75ed71a1.0010.02/DOC\\_1&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar:04cc5bd5-196f-11e8-806b-01aa75ed71a1.0010.02/DOC_1&format=PDF).

<sup>3</sup>Direttiva (UE) 2015/2366, del 25 novembre 2015, relativa ai servizi di pagamento nel mercato interno.

<sup>4</sup>Direttiva 2009/110/CE del Parlamento Europeo e del Consiglio del 16 settembre 2009 concernente l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica, disponibile a: <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32009L0110>.

<sup>5</sup>I briefing del Parlamento Europeo sono documenti informativi - predisposti da esperti, consulenti o funzionari del Parlamento - che forniscono ai parlamentari informazioni dettagliate, dati, analisi, opinioni e raccomandazioni su una determinata questione, al fine di valutare adeguatamente le implicazioni delle decisioni e formulare politiche o emendamenti alle proposte legislative in discussione, garantendo così che le decisioni siano basate su informazioni accurate e complete.



# Il contesto

# Il contesto

Ripercorrendo brevemente le principali tappe dell'evoluzione della normativa europea sui servizi di pagamento, si può rilevare che la prima direttiva europea sui servizi di pagamento<sup>6</sup> (anche nota come “Payment Services Directive” o “PSD”) - emanata nel 2007 - aveva l'obiettivo fondamentale di creare un quadro giuridico armonizzato per un mercato dei pagamenti integrato all'interno dell'UE.

La seconda direttiva sui servizi di pagamento - entrata in vigore il 13 gennaio 2016 e con termine di recepimento nel 2018 - costituisce l'attuale framework normativo europeo per la regolamentazione dei pagamenti al dettaglio nell'UE, nazionali e transfrontalieri<sup>7</sup> e con essa il legislatore europeo ha affrontato gli ostacoli relativi ai nuovi tipi di servizi di pagamento e ha migliorato il livello di protezione e sicurezza dei consumatori<sup>8</sup>.

<sup>6</sup>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

<sup>7</sup>La PSD2 contiene sia norme in materia di prestazione di servizi di pagamento da parte dei prestatori di servizi di pagamento, sia norme relative all'autorizzazione e alla vigilanza di una specifica categoria di prestatori di servizi di pagamento, segnatamente gli istituti di pagamento (IP). Le altre categorie di prestatori di servizi di pagamento comprendono in particolare gli enti creditizi, che sono disciplinati dalla normativa bancaria dell'UE (Regolamento (UE) n. 575/2013 relativo ai requisiti prudenziali per gli enti creditizi, direttiva 2013/36/UE sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale sugli enti creditizi) e gli istituti di moneta elettronica (IMEL), che sono attualmente disciplinati dalla direttiva sulla moneta elettronica (Direttiva 2009/110/CE concernente l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica).

Nell'ambito delle strategie per i pagamenti al dettaglio e la finanza digitale, nel 2022, la Commissione ha svolto una valutazione in merito all'applicazione della PSD2, al fine di valutare se la relativa disciplina fosse ancora adeguata rispetto ai mutamenti tecnologici, sociali e di mercato medio tempore intervenuti.

Tale valutazione, passata anche attraverso una consultazione dell'Autorità Bancaria Europea (EBA)<sup>9</sup> e una consultazione pubblica<sup>10</sup>, ha rilevato che la direttiva ha effettivamente conseguito alcuni degli obiettivi originariamente fissati. In particolare, un rilevante impatto positivo è stato registrato nella prevenzione delle frodi, attraverso l'introduzione della autenticazione forte del cliente (Strong Customer Authentication - SCA). Inoltre, la PSD2 è stata particolarmente efficace nell'aumentare l'efficienza, la trasparenza e la scelta dei diversi tipi di strumenti di pagamento per gli utenti.

<sup>8</sup>Più nello specifico, le principali finalità della PSD2 sono state quelle di (i) garantire parità di condizioni tra gli operatori tradizionali e i nuovi fornitori di servizi di pagamento (carte, internet e dispositivi mobili), (ii) migliorare l'efficienza, la trasparenza e la facoltà di scelta per gli utenti dei servizi di pagamento (consumatori e commercianti), (iii) agevolare la prestazione di servizi di pagamento a livello transfrontaliero, (iv) favorire l'innovazione nei servizi di pagamento e (v) garantire elevati livelli di protezione per gli utenti dei servizi di pagamento in tutti gli Stati membri.

<sup>9</sup>EBA Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2)

<sup>10</sup>Payment services – review of EU rules, public consultation: [https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13331-Payment-services-review-of-EU-rules/public-consultation\\_en](https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13331-Payment-services-review-of-EU-rules/public-consultation_en)

# Il contesto

Tuttavia, dalla valutazione sono emerse anche alcune criticità, ad esempio, nel conseguimento di una effettiva condizione di parità tra prestatori di servizi di pagamento bancari e non bancari, il cui squilibrio deriva fundamentalmente dalla mancanza di un accesso diretto, da parte di questi ultimi, ai fondamentali sistemi di pagamento. Peraltro, nonostante la comparsa di un rilevante numero di nuovi prestatori di servizi di pagamento non bancari, nel territorio dell'Unione europea si sono registrati risultati contrastanti nell'adozione di servizi di open banking, soprattutto a causa di problemi relativi alle prestazioni delle interfacce di accesso ai dati dei clienti per i prestatori di tali servizi. Inoltre, sebbene l'offerta di servizi di pagamento a livello transfrontaliero sia in aumento, molti sistemi di pagamento (in particolare i sistemi relativi alle carte di debito) continuano ad avere una portata per lo più nazionale. Infatti, le condizioni per consentire la riduzione dei costi a carico degli esercenti non si sono ancora pienamente concretizzate e, per tale ragione, non è ancora stata realizzata alcuna soluzione di pagamento interamente paneuropea.

In conclusione, la valutazione ha rilevato che, nonostante la PSD2 abbia determinato significativi miglioramenti nel settore dei pagamenti, i relativi obiettivi sono stati conseguiti soltanto in parte. Pertanto, la Commissione ha deciso di proporre gli opportuni aggiornamenti normativi attraverso un nuovo Regolamento sui Servizi di Pagamento ("PSR") e la terza Direttiva sui Servizi di Pagamento ("PSD3"). Relativamente all'iter di approvazione della suddetta regolamentazione, in data 23 aprile 2024 il Parlamento Europeo ha approvato con emendamenti rispetto alle proposte della Commissione i testi della direttiva e del regolamento, evidenziando altresì la volontà di migliorare la prestazione di servizi di pagamento in tutti gli Stati Membri. Attualmente, con riguardo ad entrambi i dossier, sono in corso le discussioni del Consiglio dell'UE; si attende l'avvio delle discussioni e dei negoziati interistituzionali che coinvolgeranno congiuntamente la Commissione Europea, il Parlamento Europeo e il Consiglio dell'Unione Europea per giungere ad un testo finale di compromesso.

Scelta degli atti  
giuridici e coerenza  
con le attuali  
disposizioni vigenti

2

# Scelta degli atti giuridici e coerenza con le attuali disposizioni vigenti

Nell'ambito della valutazione della PSD2, una delle criticità rilevate attiene al fatto che non sempre i poteri delle autorità di vigilanza sono apparsi effettivamente adeguati alle relative funzioni<sup>11</sup> e, talvolta, l'applicazione della PSD2 all'interno dell'Unione Europea risulta disomogenea tra i singoli Stati membri, causando fenomeni di arbitraggio normativo. In tale contesto, i prestatori di servizi di pagamento si trovano in una situazione di incertezza riguardo ai propri obblighi.

Più nel dettaglio, si rileva che, come noto, la seconda direttiva sulla moneta elettronica (EMD2)<sup>12</sup> contiene norme in materia di autorizzazione e vigilanza degli istituti di moneta elettronica (“IMEL”), mentre la PSD2 contiene norme in materia di autorizzazione e vigilanza degli istituti di pagamento (“IP”) e stabilisce diritti e obblighi, anche in materia di trasparenza nei rapporti tra tutti i prestatori di servizi di pagamento (compresi gli IMEL) con i relativi utenti.

Poiché le operazioni di pagamento che utilizzano moneta elettronica sono già ampiamente disciplinate dalla PSD2, il quadro giuridico applicabile agli IMEL e agli IP è apparso già ragionevolmente coerente. Tuttavia, le prescrizioni in materia di autorizzazione, in particolare il capitale iniziale e il capitale corrente, unitamente ad alcuni concetti fondamentali che disciplinano le attività relative alla moneta elettronica, quali la relativa emissione, distribuzione e la rimborsabilità, presentano alcune differenze rispetto ai servizi forniti dagli IP.

In tale contesto, le autorità di vigilanza hanno incontrato difficoltà pratiche nel definire chiaramente i due regimi applicabili e nel distinguere i prodotti/servizi di moneta elettronica dai servizi di pagamento offerti dagli IP. Tale circostanza ha suscitato evidenti preoccupazioni in merito all'arbitraggio normativo e alla disparità di condizioni, oltre a causare problemi relativi alla possibile elusione delle prescrizioni della EMD2, approfittando della somiglianza tra servizi di pagamento e servizi di moneta elettronica.

<sup>11</sup>Impact Assessment Report, Par. 2.1.3. (Inconsistent powers and obligations of supervisors): “The Commission’s PSD2 review presented in the Evaluation Report (Annex 5) has revealed inconsistent application and insufficient enforcement of PSD2 provisions and found that many of the limitations to progress on PSD2’s objectives link to challenges related to varying powers and obligations of supervisors. Inconsistent application of the legal framework and insufficiently robust enforcement of rights and duties was often mentioned in stakeholders’ contributions on various topics, as well as noted by the EBA in its Advice”.

<sup>12</sup>Direttiva 2009/110/CE, del 16 settembre 2009, concernente l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica, e successive modifiche.

# Scelta degli atti giuridici e coerenza con le attuali disposizioni vigenti

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

Più nello specifico, la Commissione ha ritenuto opportuno introdurre le modifiche all'attuale framework normativo tramite due atti legislativi distinti: la proposta di direttiva, contenente, in particolare, norme in materia di autorizzazione e vigilanza degli istituti di pagamento<sup>13</sup> e una proposta di regolamento contenente le norme per i prestatori di servizi di pagamento, sia che prestino servizi di pagamento che di moneta elettronica.

<sup>13</sup>In tale ambito è apparsa appropriata la direttiva, dal momento che l'autorizzazione e la vigilanza degli istituti finanziari in generale (compresi gli istituti di pagamento e le altre categorie di prestatori di servizi di pagamento, come gli enti creditizi) restano di competenza nazionale degli Stati membri e non è proposta alcuna autorizzazione o vigilanza a livello dell'UE.



# 3

## Misure contro i fenomeni di frode

# Misure contro i fenomeni di frode

Una delle principali innovazioni della PSD2 è stata l'introduzione della autenticazione forte del cliente (Strong Customer Authentication, SCA), la quale, come noto, richiede l'utilizzo di almeno due fattori di autenticazione basati sulla conoscenza (ad esempio, una password), sul possesso (come una carta) o sull'inerenza (come, un'impronta digitale)<sup>14</sup>.

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

Le frodi come il phishing<sup>15</sup>, vishing<sup>16</sup>, smishing<sup>17</sup>, spoofing<sup>18</sup> e altre ancora, non possono essere efficacemente contrastate dalla SCA, perché, la maggior parte di queste truffe si verifica - sia dal punto di vista tecnico che legale - prima dell'applicazione della SCA.

<sup>14</sup>Nello specifico la PSD2 prevede che i prestatori di servizi di pagamento sono tenuti ad applicare l'SCA quando il pagatore accede a un conto di pagamento on line, dispone un'operazione di pagamento elettronico o effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi.

<sup>15</sup>Come noto, il phishing è una tipologia di frode ormai diffusa (tanto da essere definita dall'Arbitro Bancario e Finanziario come "tradizionale"), effettuata tramite un'e-mail "civetta" con il logo contraffatto di un istituto di credito (diverso da quello presso il quale insiste il conto corrente del pagatore) o di una qualsiasi società commerciale (Poste, DHL, Expedia, Amazon), in cui il pagatore viene invitato a inserire, in appositi campi, i propri dati riservati (quali ad esempio: numero di carta di credito, password di accesso al servizio di home banking, ecc.), motivando tale richiesta con ragioni di ordine tecnico.

<sup>16</sup>Il termine vishing deriva dall'unione fra due parole: "voice" e "phishing". Un attacco di vishing è simile al phishing, ma avviene per telefono o tramite messaggio vocale.

Peraltro, spesso è proprio lo stesso pagatore che, in buona fede, autorizza l'operazione di pagamento attraverso la SCA. Proprio per tale ragione, la Commissione ritiene che la differenza tra operazioni autorizzate e non autorizzate sia sempre più vaga e complessa da applicare nella pratica, sollevando anche dubbi relativamente al fatto se un'operazione possa effettivamente considerarsi autorizzata solo perché è stata eseguita la SCA.

Un ulteriore aspetto critico che è stato rilevato dagli operatori riguarda la scarsa consapevolezza dei consumatori riguardo alle principali tipologie di frodi. Questa circostanza ha evidenziato l'importanza dell'educazione dei consumatori e della loro alfabetizzazione in merito alle frodi e ai rischi associati a particolari strumenti di pagamento.

<sup>17</sup>Lo smishing è una forma di phishing che utilizza i telefoni cellulari come piattaforma di attacco, inviando messaggi di testo o SMS (da cui il nome "SMiShing") con l'intento di raccogliere informazioni personali, compresi il codice fiscale e/o il numero di carta di credito e/o i codici statici e dinamici dell'home banking delle potenziali vittime. Il contenuto dei messaggi consiste nell'attirare l'attenzione della vittima su operazioni sospette o anomalie nel processo di aggiornamento relativo alla sicurezza dei dati personali, invitandola a cliccare su un collegamento ipertestuale, al fine di intervenire sulle presunte anomalie. La vittima, attraverso il reindirizzamento a pagine web che copiano graficamente quelle della propria banca, è tratta in inganno e indotta a inserire le proprie credenziali (statiche e dinamiche). Lo smishing di regola può essere seguito dal vishing, ovvero da telefonate da parte del truffatore, il quale fingendosi un operatore della banca, si offre di "aiutare" il cliente nella risoluzione delle anomalie segnalate.

<sup>18</sup>Lo spoofing si verifica quando i frodatori riescono a camuffare la provenienza della e-mail o dell'sms "civetta", facendolo comparire all'interno del thread dei messaggi, autentici e legittimi, intercorsi con il proprio intermediario. Generalmente, tali messaggi contengono un collegamento ipertestuale che rinvia a pagine di phishing dove l'utente viene indotto ad inserire le proprie credenziali.

# Misure contro i fenomeni di frode

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

Al fine di sopperire alle criticità sopraindicate, la Commissione ha proposto (i) nuove misure volte a un maggiore utilizzo dell'autenticazione forte del cliente<sup>19</sup>, (ii) una base giuridica per lo scambio delle informazioni in materia di frodi tra prestatori di servizi di pagamento nel rispetto del Regolamento (UE) 2016/679 (“GDPR”)<sup>20</sup>, (iii)

dei sistemi di verifica della corrispondenza tra IBAN e nome del beneficiario a tutti i bonifici (attualmente prevista soltanto per i pagamenti istantanei)<sup>21</sup> e (iv) l'inversione condizionata di responsabilità (dagli utenti ai prestatori di servizi di pagamento) per le frodi nel caso in cui sussistano specifiche carenze da parte dei prestatori di servizi di pagamento (mancato funzionamento della verifica IBAN/nome e truffe con furto di identità di dipendenti della banca)<sup>22</sup>.

<sup>19</sup>In particolare, è stata introdotta una nuova disposizione che impone ai prestatori di servizi di pagamento di disporre di meccanismi di monitoraggio delle operazioni che migliorino la prevenzione e l'individuazione delle operazioni fraudolente. Tale disposizione chiarisce ulteriormente la nozione del concetto di “inerenza” e precisa che i suddetti meccanismi di monitoraggio delle operazioni devono basarsi sulle caratteristiche tipiche di ciascun pagatore nell'usuale utilizzo delle credenziali di sicurezza (ad esempio l'ubicazione al momento dell'operazione, il dispositivo utilizzato, le abitudini di spesa, il negozio in cui è stato effettuato l'acquisto, etc.). Per quanto riguarda l'applicazione dell'autenticazione forte del cliente nel caso di operazioni di pagamento disposte da esercenti, il Regolamento chiarisce che è necessario applicare la SCA al momento dell'istituzione del mandato, ma senza bisogno di applicarla per le successive operazioni. Inoltre, sono state introdotte alcune disposizioni volte a migliorare l'accessibilità della SCA per le persone con disabilità, persone anziane o le persone con scarse competenze digitali e coloro che non hanno accesso ai canali digitali o a uno *smartphone*, affinché dispongano almeno di un mezzo che le consenta di effettuare un'autenticazione forte del cliente.

<sup>20</sup>Ai fini del monitoraggio delle operazioni, sono state aggiunte alcune specifiche disposizioni che consentono ai prestatori di servizi di pagamento di scambiare, su base volontaria, dati personali quali gli identificativi unici di un beneficiario nell'ambito di accordi di condivisione delle informazioni. Tali accordi di condivisione delle informazioni devono definire i dettagli della partecipazione e degli elementi operativi, compreso l'uso di piattaforme informatiche dedicate. Tuttavia, prima di concludere tali accordi, i prestatori di servizi di pagamento devono effettuare una valutazione d'impatto sulla protezione dei dati e, se necessario, procedere a una consultazione preliminare dell'autorità di controllo, conformemente al GDPR.

<sup>21</sup>È stata introdotta una disposizione analoga a quanto previsto nella proposta della Commissione che modifica il regolamento SEPA per quanto riguarda i pagamenti istantanei, con la quale viene previsto l'obbligo per il prestatore di servizi di pagamento del beneficiario di fornire all'utente, su richiesta di quest'ultimo, un servizio che verifichi la corrispondenza dell'identificativo unico del beneficiario con il nome del beneficiario fornito dal pagatore e notifici al prestatore di servizi di pagamento del pagatore qualsiasi discrepanza rilevata. In

caso di mancata corrispondenza, il prestatore di servizi di pagamento del pagatore è tenuto a notificare al pagatore tale discrepanza e la relativa portata. La notifica deve essere effettuata prima che il pagatore finalizzi l'ordine di pagamento e prima che il prestatore di servizi di pagamento esegua il bonifico. In proposito la Commissione ritiene che, in generale, l'estensione della verifica IBAN/nome del beneficiario ai pagamenti interesserà 1.200-1.300 prestatori di servizi di pagamento, con un costo in media di alcune centinaia di migliaia di euro *una tantum* e di alcune decine di migliaia di euro per spese di manutenzione annue. Sarà tuttavia consentito addebitare ai clienti le spese per l'utilizzo di tale servizio permettendo un parziale recupero dei costi.

<sup>22</sup>Nella disposizione relativa alla responsabilità del prestatore di servizi di pagamento per operazioni di pagamento non autorizzate è stato aggiunto un chiarimento secondo cui solo ragionevoli motivi per sospettare una frode da parte del pagatore possono comportare un rifiuto del rimborso da parte del prestatore di servizi di pagamento. In tal caso, il prestatore di servizi di pagamento deve motivare il rifiuto del rimborso e indicare gli organismi ai quali il pagatore può deferire la questione. Il prestatore di servizi di pagamento del pagatore è ritenuto responsabile dell'intero importo del bonifico nel caso in cui non abbia notificato al pagatore una discrepanza rilevata tra l'identificativo unico e il nome del beneficiario fornito dal pagatore. Inoltre, è ritenuto responsabile quando un consumatore è stato indotto ad autorizzare un'operazione di pagamento da un terzo che ha finto di essere un dipendente del prestatore di servizi di pagamento del consumatore. In tale contesto, è stato inoltre introdotto l'obbligo per i prestatori di servizi di comunicazione e elettronica di cooperare con i prestatori di servizi di pagamento al fine di prevenire tali frodi. Il prestatore di servizi di pagamento del beneficiario, se la responsabilità è a lui imputabile, è tenuto a rimborsare il danno finanziario subito dal prestatore di servizi di pagamento del pagatore. Le disposizioni in materia di notifica e rettifica delle operazioni di pagamento non autorizzate o non correttamente eseguite, requisiti informativi e diritto di regresso sono state aggiornate al fine di rispecchiare la nuova disposizione in materia di responsabilità per l'applicazione non corretta del servizio di verifica della corrispondenza.

# Misure contro i fenomeni di frode

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

In particolare, il concetto di autorizzazione della transazione è centrale nelle discussioni in corso ed infatti, al fine di disciplinare correttamente le transazioni autorizzate dagli utenti, si ritengono rilevanti tre elementi: l'autenticazione della transazione, la volontà dell'utente a predisporre la transazione e la responsabilizzazione per le condotte tenute medesimo in relazione all'esecuzione della transazione stessa.

Pertanto, da quanto emerge dalle attuali discussioni, in ottica futura si potrebbe qualificare un'operazione di pagamento come correttamente autorizzata solo nel caso in cui sia posta correttamente in essere l'autenticazione del pagatore e sia accertata l'intenzione dell'utente di compiere tale pagamento; in tal caso non sorgerebbe alcuna responsabilità in capo al prestatore di servizi di pagamento.

Viceversa, una transazione è considerata non autorizzata nel caso in cui non sia stata correttamente effettuata l'autenticazione da parte del pagatore e, in tal caso, il saldo del conto di pagamento dovrebbe essere ripristinato. Infine, è stata identificata una terza casistica in cui è posta correttamente in essere l'autenticazione del pagatore ma non vi è l'intenzione del medesimo a completare la transazione e, pertanto, in tali casistiche, non potendo essere considerata né un'operazione di pagamento autorizzata né un'operazione di pagamento non autorizzata, è stata ipotizzata la possibilità di ripartire la perdita tra il prestatore di servizi di pagamento e l'utente vittima di frode.

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

In ogni caso resta fermo che, oltre all'ipotesi di ripartizione delle perdite, le Autorità competenti e i provider di servizi di pagamento dovranno porre in essere ogni sforzo al fine di recuperare i fondi dall'illegittimo beneficiario della transazione correttamente autenticata ma non effettivamente voluta dall'utente, ciò in un'ottica di tutelare e simultaneamente responsabilizzare l'utente.

# 4

Banca d'Italia e il necessario  
coordinamento con MiCAR  
e DORA/ Comunicazione  
Banca d'Italia di ottobre 2024

# Banca d'Italia e il necessario coordinamento con MiCAR e DORA/ Comunicazione Banca d'Italia di ottobre 2024

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

Con particolare riferimento ai token di moneta elettronica ("EMT"), tali token sono considerati l'equivalente tokenizzato della moneta elettronica e, pertanto, gli stessi sono ricompresi sia nella nozione di cripto-attività, che in quella di moneta elettronica e fondi (anche ai sensi di PSD3/PSR e TFR), ciò in considerazione dell'utilizzabilità di tali token come mezzo di scambio con finalità di pagamento.

Alla luce di ciò, la stessa Autorità segnala la possibile equivalenza tra i servizi "connessi al trasferimento" di EMT (previsti dal MiCAR) e i servizi di pagamento "tradizionali" in quanto le caratteristiche tipiche dei servizi connessi al trasferimento di token moneta elettronica potrebbero far rientrare questi ultimi all'interno dei servizi di moneta elettronica di cui alla PSD2. Tuttavia, in tale prospettiva si pone la questione dell'applicabilità ai servizi di trasferimento di EMT – in alcuni casi equiparabili ai servizi di pagamento - delle disposizioni della PSD2, in particolare quelle riguardanti l'autenticazione forte del cliente, le operazioni non autorizzate ed i relativi riflessi sul regime di responsabilità delle parti.

Inoltre, nella medesima Comunicazione di Banca d'Italia, si evince che, in considerazione del ruolo crescente delle imprese BigTech e Fintech nel settore dei pagamenti, è in fase di valutazione l'ampiamiento del perimetro del pacchetto PSD3/PSR anche a soggetti quali i "fornitori di servizi tecnici" che, pur non propriamente e direttamente coinvolti nella prestazione di servizi di pagamento, risultano necessari alla prestazione di tali servizi. Anche in tal caso, Banca d'Italia ha sottolineato la necessità di coordinare tale possibile estensione del perimetro applicativo con il Regolamento (UE) 2022/2554 relativo alla resilienza digitale per il settore finanziario, il c.d. DORA.

Infine, nonostante il pacchetto PSD3/PSR esclude esplicitamente i servizi di "cash-in-shop" e "cashback" dal proprio campo di applicazione, l'esclusione dei servizi di "cash-in-shop" sarebbe garantita solo nel caso in cui vengano rispettate due specifiche condizioni (i) il servizio è offerto da un soggetto che vende beni e servizi a titolo di occupazione principale; (ii) il prelievo massimo di contante è pari a Euro 50,00; tuttavia tale disciplina necessiterà di ulteriori chiarimenti e affinamenti al fine di garantire parità di trattamento ed evitare la concorrenza sleale tra gestori di ATM e dettaglianti che offrono servizi di cash-in-shop.

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



# Servizi “Open banking”

# Servizi “Open banking”

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

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

Da parte loro, gli ASPSP lamentano invece l'obbligo di sostenere costi di attuazione significativi per lo sviluppo delle interfacce di programmazione delle applicazioni (“application programming interface” o “API”)<sup>23</sup> che, tuttavia, non sono legittimati ad addebitare, a loro volta, ai prestatori terzi. Peraltro, gli ASPSP si dichiarano prevalentemente insoddisfatti per il basso utilizzo delle loro API da parte dei prestatori terzi, i quali utilizzano in via preferenziale le interfacce cliente, anziché le API appositamente predisposte.

<sup>23</sup>Secondo una relazione della Commissione, oltre 2 miliardi di Euro di costi di attuazione una tantum.

In tale contesto, per la revisione della PSD2, la Commissione ha scelto di focalizzarsi su una serie di modifiche mirate a ottimizzare l'efficacia dei servizi open banking, evitando però di apportare cambiamenti radicali che potrebbero destabilizzare il mercato o generare costi di attuazione significativi<sup>24</sup>. In particolare, le modifiche principali prevedono l'obbligo, salvo casi eccezionali, di disporre di un'interfaccia dedicata per l'accesso ai dati e la soppressione, salvo in casi eccezionali ed espressamente autorizzati, dell'obbligo per gli ASPSP di mantenere permanentemente un'interfaccia c.d. “di riserva”. Inoltre, al fine di consentire agli utenti di gestire comodamente le loro autorizzazioni rilasciate ai prestatori terzi per tali servizi, gli ASPSP sono tenuti a offrire un “pannello di gestione” che permetta di revocare l'accesso ai dati concesso a qualsiasi prestatore di servizi bancari aperti.

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

<sup>24</sup>Nello specifico, le disposizioni in materia di servizi open banking contengono una serie di modifiche rispetto alla PSD2 e incorporano alcune disposizioni attualmente contenute nel Regolamento delegato (UE) 2018/389 della Commissione per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione con uni e sicuri.

# Servizi “Open banking”

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

Più nello specifico, la Commissione ha ritenuto opportuno introdurre le modifiche all'attuale framework normativo tramite due atti legislativi distinti: la proposta di direttiva, contenente, in particolare, norme in materia di autorizzazione e vigilanza degli istituti di pagamento<sup>13</sup> e una proposta di regolamento contenente le norme per i prestatori di servizi di pagamento, sia che prestino servizi di pagamento che di moneta elettronica.



# 6

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

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

Dall'entrata in vigore della PSD2, si è verificato un incremento, sia in termini numerici che di rilevanza, dei prestatori di servizi di pagamento non bancari. Nonostante essi siano in grado di fornire servizi di conto di pagamento, a differenza delle banche, non possono - tendenzialmente - concedere prestiti<sup>25</sup> e devono garantire la sicurezza dei fondi dei clienti attraverso l'intermediazione di una banca. Inoltre, per poter offrire servizi di pagamento, è indispensabile avere accesso alle principali infrastrutture di pagamento che gestiscono e regolamentano le transazioni finanziarie.

In relazione all'accesso ai conti bancari da parte degli istituti, è opportuno sottolineare che, sebbene il secondo paragrafo dell'articolo 36 della PSD2 imponga agli enti creditizi di fornire una motivazione adeguata all'autorità di vigilanza competente in caso di rifiuto di concedere l'accesso ai conti di pagamento essenziali per la prestazione dei servizi di pagamento, si è notato che diverse banche non rispettano pienamente tali obblighi normativi. Alcune di esse forniscono spiegazioni insufficientemente dettagliate o addirittura adottano prassi che comportano inizialmente l'accesso ai conti bancari, per poi revocarlo senza fornire alcuna spiegazione. Questo tipo di comportamento può avere gravi conseguenze sulle attività degli IP e degli IMEL, minando la stabilità e l'efficienza delle loro operazioni.

<sup>25</sup>L'art. 114-*octies*, del D.lgs 1° settembre 1993, n. 385 ("TUB"), rubricato "Attività accessorie esercitabili", dispone che gli istituti di pagamento (e gli istituti di moneta elettronica, ai sensi del combinato dell'art. 114-*quater*, comma 3, lett. a) del TUB) possono esercitare, tra l'altro, anche l'attività di concessione di crediti in stretta relazione ai servizi di pagamento prestati e nei limiti e con le modalità stabilite dalla Banca d'Italia. Nello specifico, il finanziamento deve essere concesso nel rispetto delle seguenti condizioni: (i) il finanziamento deve essere accessorio e concesso esclusivamente in relazione all'esecuzione di un'operazione di pagamento; (ii) non deve essere superiore a dodici mesi; (iii) non deve essere concesso utilizzando fondi ricevuti o detenuti ai fini dell'esecuzione di un'operazione

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

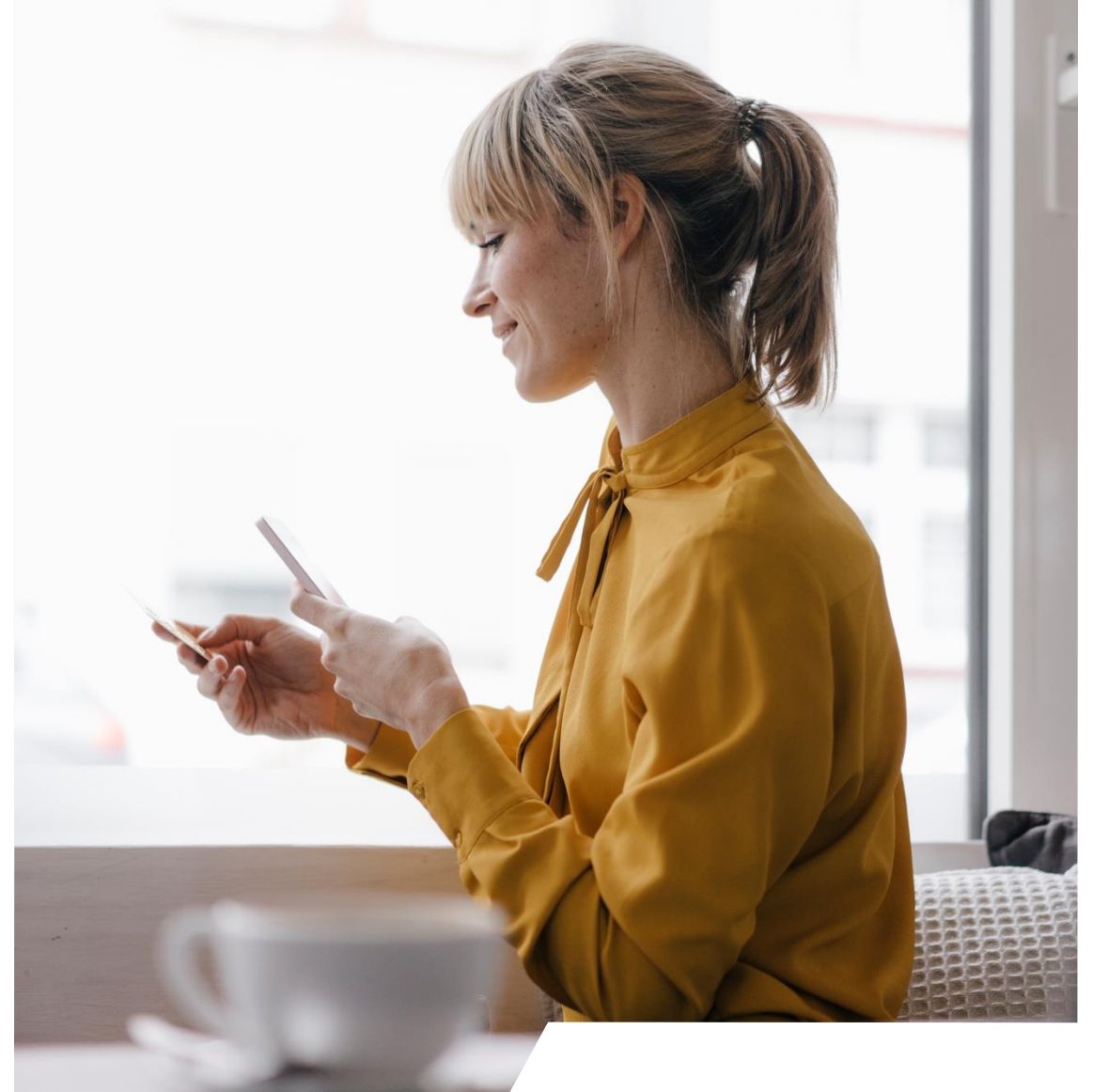
La proposta della Commissione di revisione della PSD2 contiene pertanto misure volte a porre rimedio a tali carenze e a migliorare la parità di condizioni. Le prescrizioni imposte alle banche per quanto riguarda i servizi di conto bancario a prestatori di servizi di pagamento non bancari saranno inasprite, imponendo un obbligo più severo di spiegare il motivo dell'eventuale rifiuto<sup>27</sup> e includendo tra le fattispecie soggette all'obbligo di spiegazione anche l'eventuale revoca del servizio. Infine, le banche centrali potrebbero, a propria discrezione, offrire servizi di custodia dei fondi detenuti dai prestatori di servizi di pagamento non bancari, fornendo così una eventuale soluzione di ripiego nel caso in cui dovessero non riuscire ad ottenere l'apertura di un conto presso una banca.

di pagamento; e (iv) l'istituto di pagamento dovrebbe dotarsi di una specifica dotazione minima di capitale pari al 6% dei finanziamenti erogati. Inoltre, il processo per l'erogazione del credito deve comprendere le seguenti fasi: 1) istruttoria; 2) erogazione; 3) monitoraggio delle posizioni; 4) interventi in caso di anomalia; 5) revisione delle linee di credito. <sup>26</sup>Direttiva 98/26/CE del Parlamento europeo e del Consiglio del 19 maggio 1998 concernente il carattere definitivo del regolamento nei sistemi di pagamento e nei sistemi di regolamento titoli.

<sup>27</sup>Tale giustificazione potrebbe essere rappresentata, ad esempio, da violazioni della legge da parte del prestatore di servizi di pagamento. In particolare, le relative motivazioni dovrebbero includere, tra le altre, fondato sospetto di attività illegali e di riciclaggio di denaro.

# Scelta degli atti giuridici e coerenza con le attuali disposizioni vigenti

Peraltro, anche le banche centrali saranno autorizzate a fornire, a loro discrezione, servizi di conto ai prestatori di servizi di pagamento non bancari. La Commissione propone, inoltre, di modificare la citata direttiva “concernente il carattere definitivo del regolamento” al fine di includere i prestatori di servizi di pagamento non bancari come possibili partecipanti a sistemi di pagamento designati. La nuova disciplina così modificata comprenderà norme rafforzate sull'ammissione degli IP come partecipanti ai sistemi di pagamento, con un'adeguata valutazione del rischio.





# Conclusione

# Conclusione

Alla luce dei risultati della valutazione sulla PSD2, la Commissione ha tratto due conclusioni fondamentali. Da un lato, ha riconosciuto la necessità di apportare modifiche mirate e tempestive al quadro normativo dei pagamenti dell'Unione europea. Dall'altro lato, ha ritenuto opportuno che tali modifiche rappresentino una graduale e fisiologica evoluzione, piuttosto che una rivoluzione. In questo senso, infatti, in alcuni ambiti, non sono emerse criticità tali da richiedere modifiche sostanziali. In altri ambiti, invece (ad esempio, in materia di open banking), la Commissione ha tenuto conto delle esperienze acquisite dall'entrata in vigore della PSD2 e degli investimenti già effettuati per conformarsi a queste norme. Ha anche valutato i potenziali costi associati ad una eventuale revisione totale delle disposizioni, ritenendo opportuno evitare di adottare scelte legislative che comportino nuovi oneri di attuazione significativi e risultati incerti.

Le proposte di revisione della PSD2 costituiscono un pacchetto di modifiche finalizzate a migliorare il funzionamento del mercato dei pagamenti nell'Unione europea e a rafforzare la tutela dei consumatori. Tali modifiche sono allineate agli obiettivi della strategia della Commissione per i pagamenti al dettaglio e si integrano con le iniziative in corso, come la proposta legislativa relativa ai pagamenti istantanei e la proposta relativa alla "finanza aperta" (FIDA), che la Commissione ha presentato congiuntamente alla revisione della PSD2.

Per quanto concerne il processo di recepimento e attuazione della terza direttiva e del regolamento sui servizi di pagamento, è da notare che, a seguito della presentazione da parte della Commissione europea in data 28 giugno 2023, il processo legislativo procede attraverso la fase di discussione e negoziazione presso il Parlamento europeo e il Consiglio dell'Unione europea. Durante questa fase, le proposte iniziali possono essere soggette a modifiche e integrazioni, e solamente dopo aver raggiunto un accordo sull'approvazione delle proposte, tali testi divengono legge europea.

Tuttavia, dopo l'adozione a livello europeo, gli Stati membri dell'Unione europea sono responsabili del recepimento e dell'implementazione delle relative disposizioni all'interno delle rispettive legislazioni nazionali, generalmente entro un termine massimo di due anni.

Il termine effettivo per l'implementazione e il recepimento di tali nuove norme in Italia sarà condizionato dalla celerità e dall'efficacia con cui il Parlamento italiano e le autorità nazionali completeranno il processo di recepimento e attuazione.



## Contatti

### **Fabrizio Cascinelli**

Partner PwC Italia,  
Legal - Financial Regulation

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

### **Luca Bettinelli**

Senior Manager PwC Italia,  
Legal - Financial Regulation

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