



BANCA D'ITALIA
EUROSISTEMA

Comitato Pagamenti **I**talialia



RAPPORTO SULLE OPERAZIONI DI PAGAMENTO FRAUDOLENTE IN ITALIA – Il semestre 2024

Agosto 2025

Indice

Sintesi	2
1. Le operazioni fraudolente per strumento di pagamento	4
1.1 Le principali evidenze	4
1.2 Bonifici SEPA: istantanei vs. ordinari	6
1.3 Prospettiva geografica delle operazioni fraudolente	7
1.4 Le operazioni fraudolente per canale di utilizzo degli strumenti di pagamento	8
2. Le principali tipologie di frode	10
3. Il ruolo dell'autenticazione forte del cliente	12
3.1 Utilizzo della SCA nei pagamenti elettronici	12
3.2 Tassi di frode nelle operazioni con e senza SCA	13
3.3 Utilizzo delle esenzioni dalla SCA	14
4. Le perdite da frode per portatore di responsabilità	18

Il rapporto è stato redatto da Guerino Ardizzi, Daniele Figoli, Andrea Nobili e Camilla Savarese del Servizio Strumenti e servizi di pagamento al dettaglio della Banca d'Italia

Sintesi

Il Rapporto fornisce un aggiornamento dei principali indicatori sulla sicurezza dei pagamenti digitali al dettaglio nel nostro Paese¹, utilizzando le segnalazioni semestrali dei prestatori di servizi di pagamento (PSP) relative alle operazioni fraudolente eseguite con i diversi strumenti di pagamento elettronici. Per **frode** o **operazione fraudolenta** si intende quella effettuata senza il consenso del legittimo titolare (cd. operazione di pagamento “non autorizzata” o “disconosciuta”) o in conseguenza di una manipolazione operata a danno di quest’ultimo da parte del frodatore (cd. “manipolazione del pagatore”).

Sebbene i casi di frode registrino un’incidenza limitata rispetto al totale delle transazioni al dettaglio e le relative perdite per gli utenti siano in gran parte attenuate dai meccanismi di tutela previsti dalla normativa di settore, la prevenzione e la riduzione dei rischi di frode nell’uso di strumenti di pagamento digitali costituiscono punti cardine per le Autorità di sorveglianza europee, al fine di garantire l’integrità dei sistemi di pagamento al dettaglio in Europa².

Il Rapporto considera dati in serie storica dal secondo semestre del 2022 al secondo semestre del 2024 e illustra le operazioni fraudolente con riferimento a: principali strumenti elettronici³ (bonifici, carte di pagamento, moneta elettronica e prelievi da ATM), canali di utilizzo (POS fisico vs *e-commerce*), prospettiva geografica (a livello nazionale vs transfrontaliero), tipologia delle frodi (operazioni non autorizzate vs casi di manipolazione), presidi di sicurezza (autenticazione forte vs altro) e ripartizione delle perdite tra clienti e PSP⁴.

Le principali evidenze riferite al secondo semestre del 2024 segnalano che:

- Il tasso di frode (incidenza delle operazioni fraudolente sul totale delle operazioni di pagamento) calcolato sul valore delle operazioni risulta contenuto e stabile nel tempo per i bonifici nel loro complesso (0,002%), mentre è più elevato ma in calo per la moneta elettronica (0,021%). Il tasso di frode per i bonifici istantanei risulta sensibilmente più elevato rispetto ai bonifici ordinari (rispettivamente 0,057% e 0,0015%, in valore; 0,027% e 0,001%, nel numero)⁵.
- I pagamenti con carte (debito e credito) e i prelievi da ATM si collocano su livelli intermedi di rischio, con tassi di frode rispettivamente pari a 0,017% e a 0,010%, in riduzione rispetto allo stesso periodo dello scorso anno. Analoghe considerazioni si evincono dall’analisi dei tassi di frode calcolati sul numero di operazioni.

¹ Cfr. [Banca d'Italia - La Banca d'Italia pubblica il Rapporto sulle operazioni di pagamento fraudolente in Italia](#).

² L’Eurosistema basa l’attività di monitoraggio delle frodi sulle informazioni statistiche segnalate dai PSP residenti nella UE/SEE (banche, istituti di pagamento e istituti di moneta elettronica) alle loro Autorità Competenti, ai sensi dell’Articolo 96(6) della Direttiva (UE) 2015/2366 (revised Payment Service Directive, PSD2). Nel ruolo di Autorità nazionale competente per i PSP residenti in Italia, la Banca d’Italia invia tali dati alla BCE con cadenza semestrale e in forma aggregata, in base al Regolamento (UE) 2020/2011 relativo alle statistiche sui pagamenti. Come previsto dal “Memorandum of Understanding” (MoU) tra EBA, BCE e BCN, tali dati sono utilizzati anche per estrarre gli aggregati di interesse per l’EBA, sulla base di apposite Linee Guida (“EBA Guidelines on fraud reporting under PSD2”).

³ Non sono considerati i bonifici effettuati “in modalità tradizionale” allo sportello e le statistiche sulle frodi relative agli “addebiti diretti” (pagamenti iniziati dal beneficiario).

⁴ Le definizioni degli aggregati contenute nel Rapporto sono in linea con le indicazioni del Regolamento Delegato (UE) 2018/389 della Commissione Europea che integra la PSD2 per quanto riguarda le norme tecniche di regolamentazione per l’autenticazione forte del cliente. I dati sono soggetti a possibili rettifiche da parte degli enti segnalanti sottoposti ad analisi di qualità volte a garantire una maggiore affidabilità nell’interpretazione delle dinamiche osservate.

⁵ Al fine di contenere i fenomeni fraudolenti, dal 9 ottobre 2025 diventerà obbligatorio per i prestatori di servizi di pagamento effettuare la verifica in tempo reale sull’IBAN e sui dati del beneficiario del bonifico (istantaneo e tradizionale) e segnalare eventuali discrepanze prima che il cliente autorizzi l’operazione di pagamento.

- L'importo medio delle operazioni fraudolente è maggiore per i bonifici ordinari (€ 5.864) e istantanei (€ 1.666), rispetto a quello delle carte di pagamento, della moneta elettronica e dei prelievi da ATM (rispettivamente, pari a: € 87, € 45, € 471).
- Le operazioni di pagamento "a distanza" (*e-commerce*) rimangono più esposte al rischio frodi di quelle "non a distanza" (al punto vendita fisico), sebbene questo divario si sia ridotto rispetto a un anno fa.
- Le operazioni transfrontaliere (soprattutto quelle al di fuori dello Spazio Economico Europeo - SEE) presentano un'incidenza di frodi significativamente superiore rispetto a quelle domestiche, in particolare per carte e moneta elettronica.
- Nei pagamenti con carte e con moneta elettronica e nei prelievi da ATM rilevano le operazioni effettuate senza il consenso del legittimo titolare (cd "non autorizzate" o "disconosciute"), quali lo smarrimento, la contraffazione (*skimming*), la mancata ricezione o il furto della carta e dei dati ad essa associati. Per i bonifici rileva, invece, la "manipolazione del pagatore", in cui il cliente viene indotto a effettuare un pagamento dal frodatore, che sfrutta informazioni raccolte tramite tecniche di *social engineering*. Il valore complessivo delle frodi da manipolazione ha registrato un incremento del 49% per tutti gli strumenti di pagamento rispetto allo stesso semestre dell'anno precedente; le frodi per pagamenti non autorizzati, per le quali i presidi SCA hanno maggiore efficacia, si sono, invece, ridotte (-7% su base annua).
- Per i pagamenti con carte e moneta elettronica, le transazioni con autenticazione forte del cliente (SCA) risultano più sicure di quelli senza SCA, soprattutto per la componente transfrontaliera. I pagamenti esenti da SCA, ovvero considerati poco rischiosi sulla base delle caratteristiche della transazione (es. operazioni di modico valore o ricorrenti), mostrano tassi di frode confrontabili con quelli delle operazioni con SCA.
- L'incidenza delle perdite da frode sostenute dall'utente è maggiore nel caso dei bonifici (89%) e dei prelievi da ATM (51%) rispetto ai pagamenti con carte (31%) e con moneta elettronica (40%). La ripartizione delle perdite tra i soggetti coinvolti nel pagamento è influenzata anche dalla tipologia di frode: ad esempio, nel caso della "manipolazione del pagatore" non è possibile attivare automaticamente i meccanismi di rimborso a favore del cliente previsti dalla normativa, rendendo più difficile il recupero delle somme.

1. Le operazioni fraudolente per strumento di pagamento

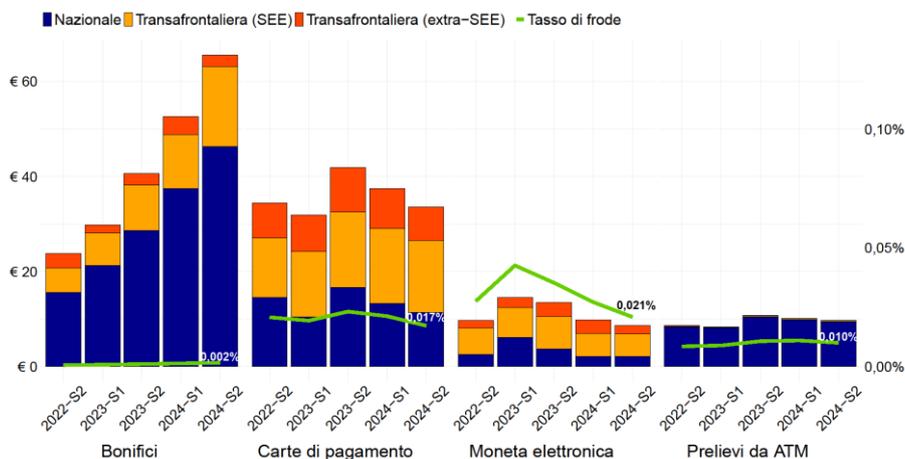
1.1 Le principali evidenze

Lo strumento con l'ammontare più elevato di operazioni fraudolente è il bonifico, seguito dalle carte di pagamento (Figura 1). In termini di frequenza, invece, il maggior numero di operazioni fraudolente riguarda le carte di pagamento, lo strumento più utilizzato (oltre il 70% del totale delle operazioni) seguite dalla moneta elettronica. Nel secondo semestre del 2024 il valore dei bonifici fraudolenti (esclusi quelli eseguiti allo sportello) disposti dalla clientela tramite PSP italiani ammonta a circa 65,5 milioni di euro (+61% su base annua; Figura 1), mentre il valore delle operazioni fraudolente con carte di pagamento (debito e credito) e quello con moneta elettronica emesse da PSP italiani si collocano, rispettivamente, a 34 milioni (-20%) e 9 milioni (-36%).

Figura 1. Livelli e tassi di frode delle operazioni fraudolente per strumento di pagamento e prospettiva geografica del PSP del beneficiario

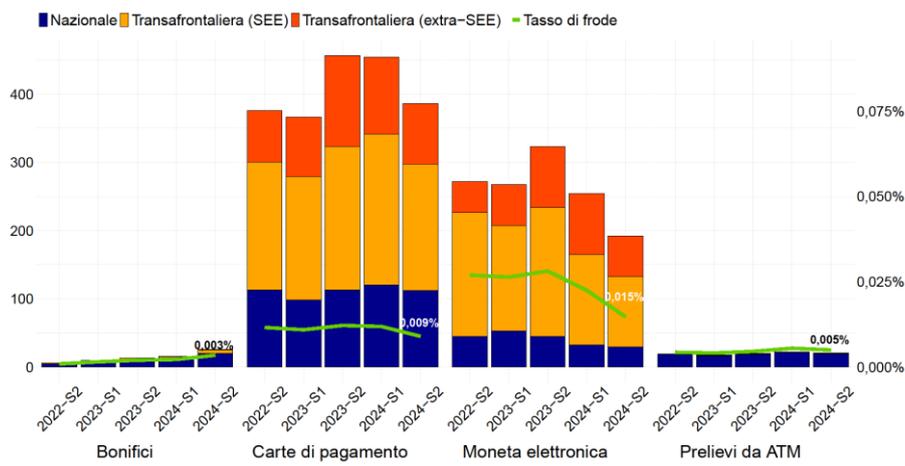
a) Valore delle operazioni fraudolente

(asse di sinistra: milioni di euro; asse di destra: in % del valore totale delle operazioni per strumento di pagamento)



b) Numero di operazioni fraudolente

(asse di sinistra: migliaia; asse di destra: in % del numero totale delle operazioni per strumento di pagamento)



Fonte: Elaborazioni su dati di matrice dei conti forniti dai PSP italiani.

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

Lo Spazio Economico Europeo (SEE) comprende i 27 Stati membri dell'Unione Europea (UE) e 3 Stati membri dell'Associazione Europea di Libero Scambio (EFTA), ovvero Islanda, Liechtenstein e Norvegia. Le operazioni effettuate con bonifico o con carta "a distanza" (internet, collegamenti telematici o telefonici) sono classificate come nazionali, transfrontaliere all'interno del SEE o transfrontaliere al di fuori del SEE (extra-SEE) a seconda della localizzazione del PSP del beneficiario. Le operazioni con carta "non a distanza" (pagamenti al punto vendita fisico e prelievi da ATM) invece sono classificate come nazionali quando sia il PSP del

beneficiario che il punto vendita fisico o lo sportello automatico nel caso dei prelievi sono situati in Italia; sono classificate come transfrontaliere all'interno del SEE o come transfrontaliere al di fuori del SEE (extra-SEE) sia se il PSP del beneficiario è rispettivamente all'interno o al di fuori del SEE, sia se il PSP del beneficiario è nazionale ma il punto vendita fisico o lo sportello automatico sono rispettivamente situati in un altro Stato del SEE o al di fuori del SEE.

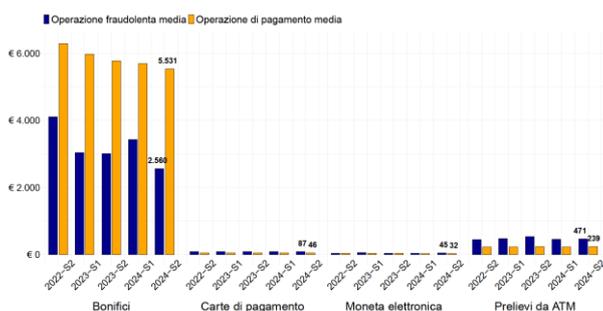
Nello stesso periodo, il numero di bonifici fraudolenti inviati tramite PSP italiani risulta essere circa 25.600 (+90% su base annua), mentre le operazioni fraudolente con carte di pagamento e moneta elettronica ammontano rispettivamente a 386.364 (-15%) e a 191.983 (-41%); il numero di prelievi da ATM fraudolenti è pari a 20.500 (+3%).

Il valore e il numero di operazioni fraudolente riflettono il diverso caso d'uso di ciascuno strumento e la sua diffusione nel mercato dei pagamenti al dettaglio. I bonifici sono, infatti, utilizzati prevalentemente per pagamenti (anche di elevato importo) tra persone fisiche (P2P) e tra imprese (B2B), mentre le carte di pagamento e la moneta elettronica (in Italia costituita in larga parte da carte prepagate), sono impiegate prevalentemente per l'acquisto di beni e servizi al punto vendita fisico o virtuale (P2B), originando un gran numero di transazioni di importo contenuto.

Il tasso di frode, definito come l'incidenza delle operazioni fraudolente sul totale delle operazioni di pagamento, è più elevato per la moneta elettronica e le carte di pagamento. Questo indicatore, calcolato sul valore delle transazioni, risulta molto contenuto e pressoché stabile nel tempo per i bonifici (0,002%) e più elevato, ma in diminuzione, per la moneta elettronica (0,021%, da 0,035% del secondo semestre del 2023); i pagamenti con carte e i prelievi da ATM si collocano su livelli intermedi, con tassi di frode rispettivamente pari a 0,017% e 0,01%. Un quadro simile emerge considerando i tassi di frode calcolati sul numero di transazioni.

Il valore medio delle operazioni fraudolente è più elevato per i bonifici (Figura 2). Nel secondo semestre del 2024 il valore medio fraudolento per i bonifici ammonta a circa € 2.560, più contenuto per le carte di pagamento, la moneta elettronica e i prelievi da ATM, rispettivamente pari a € 87, € 45 e € 471.

Figura 2. Valore medio delle operazioni di pagamento e di quelle fraudolente per strumento di pagamento (in euro)



Fonte: Elaborazioni su dati di matrice dei conti forniti dai PSP italiani.

Note: Il valore medio delle operazioni fraudolente per ciascuno strumento di pagamento è calcolato come rapporto tra il valore e il numero di operazioni fraudolente.

Nel complesso, le evidenze suggeriscono che l'esposizione a casi di frode, desumibile dal tasso di frode, è più elevata nei pagamenti con carte e con moneta elettronica, ma la perdita potenziale, catturata dall'importo medio della frode, è più ingente nel caso dei bonifici.

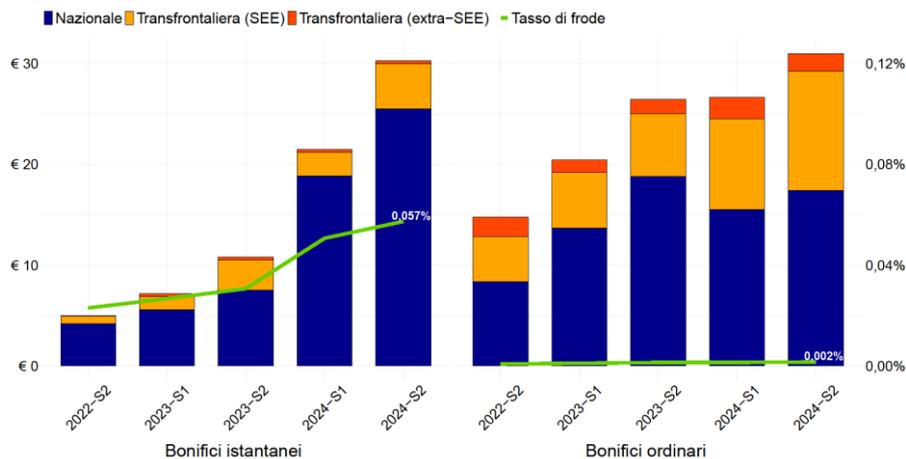
1.2 Bonifici SEPA: istantanei vs. ordinari

Il tasso di frode è rimasto stabile e molto contenuto (0,0015%) per i bonifici ordinari, mentre per quelli istantanei è aumentato (+90% su base annua) ed è di gran lunga più elevato (a 0,057%) (Figura 3). In termini di numero di operazioni, esso risulta pari allo 0,001% per i bonifici ordinari, contro lo 0,027% per i bonifici istantanei (rispettivamente 0,001% e 0,014% un anno prima).

Figura 3. Livelli e tassi di frode delle operazioni fraudolente: bonifici istantanei vs. bonifici ordinari per prospettiva geografica del PSP del beneficiario

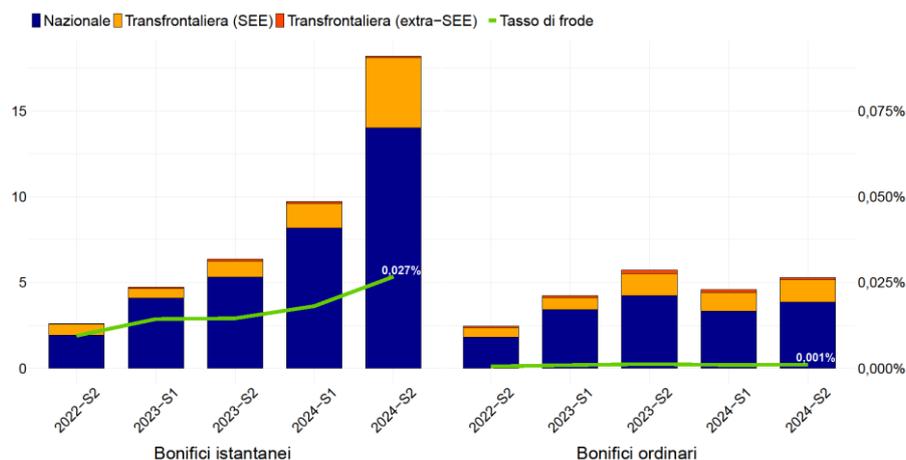
a) Valore delle operazioni fraudolente

(asse di sinistra: milioni di euro; asse di destra: in % del valore totale delle operazioni di pagamento)



b) Numero di operazioni fraudolente

(asse di sinistra: migliaia; asse di destra: in % del numero totale delle operazioni di pagamento)



Fonte: Elaborazioni su dati di matrice dei conti forniti dai PSP italiani.

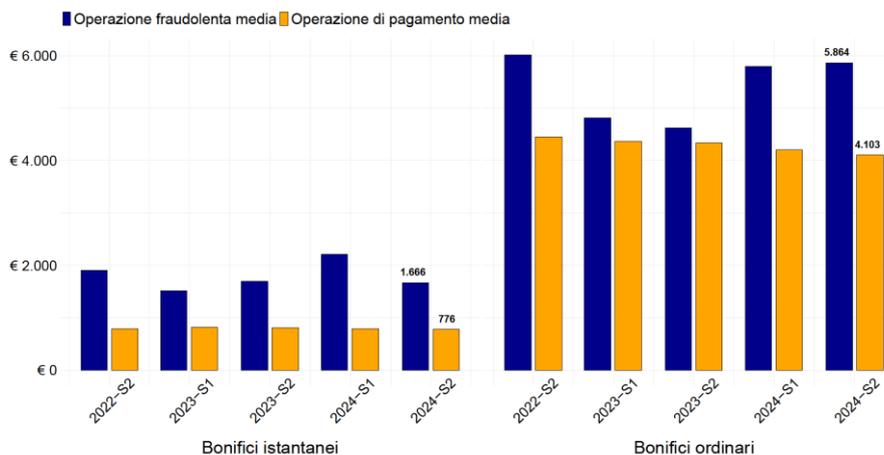
Note: l'insieme dei bonifici non considera quelli effettuati con modalità tradizionali, ovvero allo sportello.

Lo Spazio Economico Europeo (SEE) comprende i 27 Stati membri dell'Unione Europea (UE) e 3 Stati membri dell'Associazione Europea di Libero Scambio (EFTA), ovvero Islanda, Liechtenstein e Norvegia. Le operazioni effettuate con bonifico sono classificate come nazionali, transfrontaliere all'interno del SEE o transfrontaliere al di fuori del SEE (extra-SEE) a seconda della localizzazione del PSP del beneficiario.

Il valore medio delle frodi è circa 3,5 volte più elevato per i bonifici ordinari rispetto a quelli istantanei (Figura 4). Nel secondo semestre del 2024 l'importo medio delle operazioni fraudolente è pari a circa € 5.864 per i bonifici ordinari e a € 1.666 per i bonifici istantanei, pressoché stabili su base annua.

Figura 4. Importo medio delle operazioni di pagamento e di quelle fraudolente per i bonifici ordinari e istantanei

(importi in euro)



Fonte: Elaborazioni su dati di matrice dei conti forniti dai PSP italiani.

Note: L'importo medio delle operazioni fraudolente per ciascuno strumento di pagamento è calcolato come rapporto tra il valore e il volume delle operazioni fraudolente.

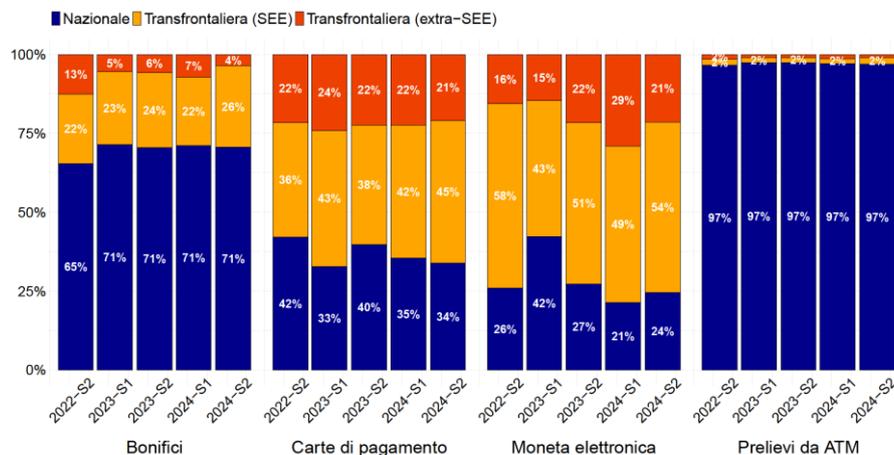
1.3 Prospettiva geografica delle operazioni fraudolente

Le operazioni fraudolente possono essere analizzate anche dal punto di vista della prospettiva geografica del PSP del beneficiario del pagamento, distinguendo per ciascuno strumento le operazioni nazionali da quelle transfrontaliere all'interno e all'esterno dello Spazio economico europeo (SEE).

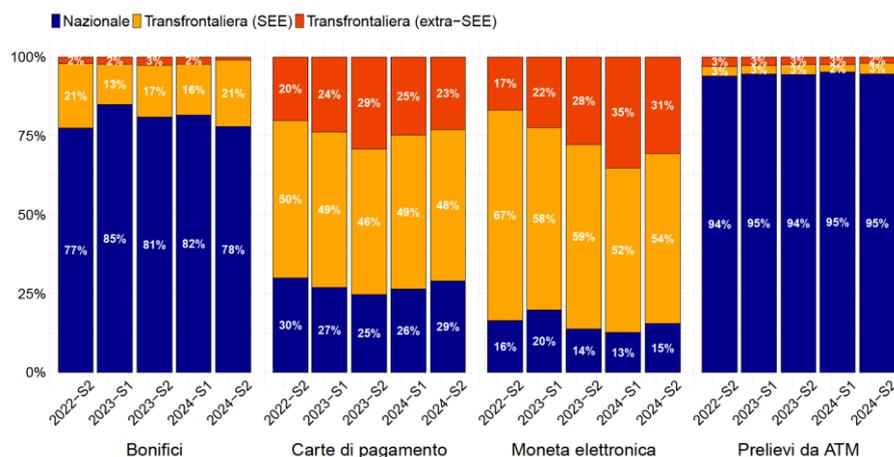
La maggior parte delle operazioni fraudolente con carte di pagamento e con moneta elettronica riguarda operazioni transfrontaliere (Figura 5). Nel secondo semestre del 2024 il 66% del valore complessivo delle operazioni fraudolente con carte di pagamento è costituito da operazioni transfrontaliere (71% considerando il numero di operazioni). Nel caso della moneta elettronica, l'incidenza sale al 75% e all' 85%, rispettivamente in termini di valore e di numero. Per i bonifici la quota di operazioni fraudolente transfrontaliere risulta più contenuta (30% in valore e 22% in numero).

Figura 5. Composizione delle operazioni fraudolente per strumento di pagamento e prospettiva geografica del PSP del beneficiario

a) Valore delle operazioni fraudolente
(quote percentuali)



a) Numero di operazioni fraudolente
(quote percentuali)



Fonte: Elaborazioni su dati di matrice dei conti forniti dai PSP italiani.

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

Lo Spazio Economico Europeo (SEE) comprende i 27 Stati membri dell'Unione Europea (UE) e 3 Stati membri dell'Associazione Europea di Libero Scambio (EFTA), ovvero Islanda, Liechtenstein e Norvegia. Le operazioni effettuate con bonifico o con carta "a distanza" (internet, collegamenti telematici o telefonici) sono classificate come nazionali, transfrontaliere all'interno del SEE o transfrontaliere al di fuori del SEE (extra-SEE) a seconda della localizzazione del PSP del beneficiario. Le operazioni con carta "non a distanza" (pagamenti al punto vendita fisico e prelievi da ATM) invece sono classificate come nazionali quando sia il PSP del beneficiario che il punto vendita fisico o lo sportello automatico nel caso dei prelievi sono situati in Italia; sono classificate come transfrontaliere all'interno del SEE o come transfrontaliere al di fuori del SEE (extra-SEE) sia se il PSP del beneficiario è rispettivamente all'interno o al di fuori del SEE, sia se il PSP del beneficiario è nazionale ma il punto vendita fisico o lo sportello automatico sono rispettivamente situati in un altro Stato del SEE o al di fuori del SEE.

1.4 Le operazioni fraudolente per canale di utilizzo degli strumenti di pagamento

In questa sezione viene fornita un'analisi delle operazioni fraudolente per canale di pagamento utilizzato dall'utente, ovvero distinguendo tra operazioni avviate "a distanza" (pagamenti via internet e tramite dispositivi mobili) e "non a distanza" (pagamenti presso il punto vendita fisico).

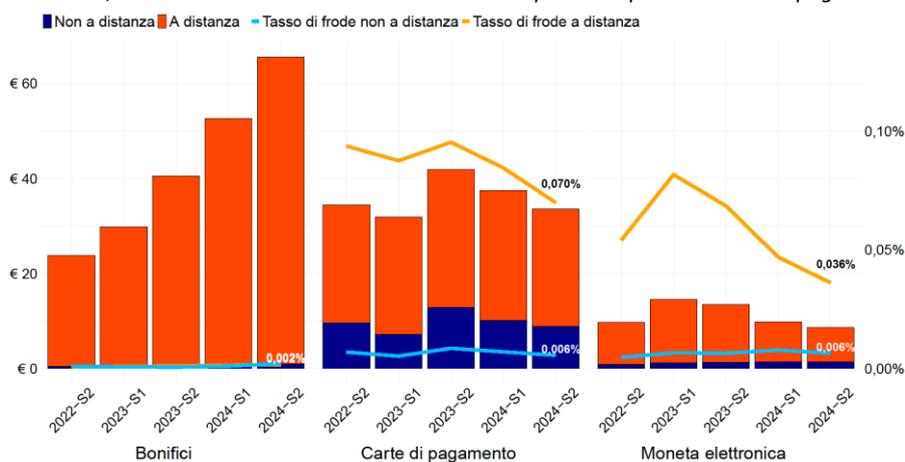
Nel caso delle carte di pagamento, le operazioni “a distanza” risultano più rischiose di quelle al punto vendita fisico (Figura 6). Nel secondo semestre del 2024 l’incidenza delle operazioni fraudolente nei pagamenti con carte utilizzate on line (ad esempio, sui siti e-commerce) rappresenta, infatti, il 73,5% del valore e il 76% del numero di frodi complessive, nonostante la maggior parte delle operazioni venga effettuata dagli utenti al punto vendita fisico. Il tasso di frode per le operazioni “a distanza” (0,07% in valore; 0,046% in numero) è dunque pari a oltre dieci volte quello per le operazioni “non a distanza” (0,006% in valore; 0,003% in numero), divario che sembra essersi ridotto nel corso del 2024.

Anche per la moneta elettronica, l’incidenza delle frodi è maggiore nelle operazioni “a distanza”, sebbene sia in riduzione. Nel secondo semestre del 2024 il 51% del valore delle operazioni risulta “non a distanza” (61% del numero), mentre l’84% del valore delle frodi riguarda le operazioni “a distanza” (88% del numero).

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

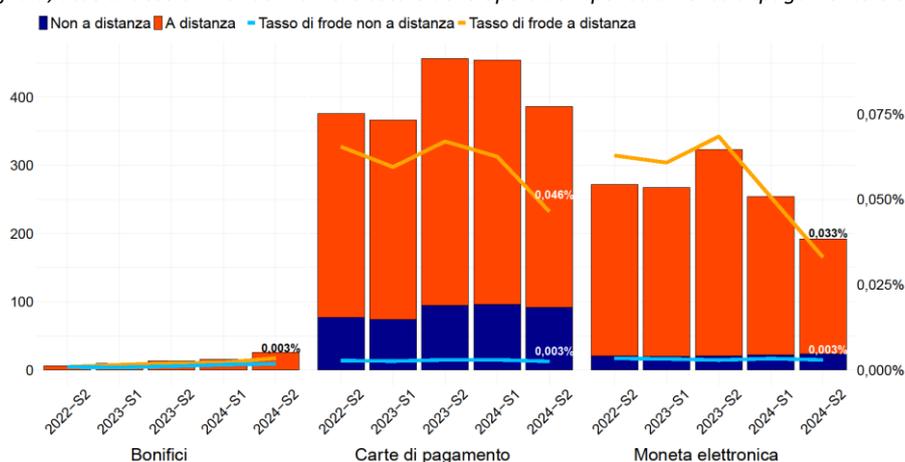
a) Valore delle operazioni fraudolente

(asse di sinistra: milioni di euro; asse di destra: in % del valore totale delle operazioni per strumento di pagamento e canale di utilizzo)



b) Numero di operazioni fraudolente

(asse di sinistra: migliaia; asse di destra: in % del numero totale delle operazioni per strumento di pagamento e canale di utilizzo)



Fonte: Elaborazioni su dati di matrice dei conti forniti dai PSP italiani.

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

La rischiosità dei bonifici risulta molto contenuta, nonostante la quasi totalità di quelli elettronici sia avviata “a distanza”.

2. Le principali tipologie di frode

Le Linee Guida dell'EBA sul *fraud reporting* ai sensi della PSD2 individuano tre principali categorie di frode:

1. **Emissione di un ordine di pagamento da parte di un frodatore:** tipologia di frode senza il consenso del legittimo titolare, in cui il frodatore effettua il pagamento a seguito di appropriazione indebita dello strumento stesso o di informazioni e dati confidenziali quali numeri di carta di credito, PIN e credenziali d'accesso (username, password) ai conti bancari on line.
2. **Modifica di un ordine di pagamento da parte del frodatore:** tipologia di frode senza il consenso del legittimo titolare, in cui il frodatore intercetta e modifica un ordine di pagamento legittimo durante la comunicazione elettronica tra il dispositivo dell'utente pagatore e il PSP (es. tramite malware o attacchi informatici), oppure interviene direttamente nel sistema del PSP prima che l'ordine sia autorizzato e liquidato.
3. **Manipolazione del pagatore:** tipologia di frode con il consenso del legittimo titolare, il quale, in buona fede, viene indotto dal frodatore a impartire un'istruzione di pagamento al proprio PSP a favore di un conto fraudolento. La manipolazione avviene soprattutto tramite tecniche di social engineering (*phishing, vishing, spoofing*), che imitano il comportamento di persone fidate (familiari, dipendenti del PSP, ecc.).

Queste categorie possono essere ulteriormente raggruppate in due macro-tipologie di frode, a seconda se il pagamento fraudolento avviene con il consenso del legittimo titolare indotto ad effettuarlo ("**manipolazione del pagatore**") o senza il suo consenso (cd. "**non autorizzate**" o "**disconosciute**"), tramite l'emissione o la modifica di un ordine di pagamento da parte del frodatore.

Nel secondo semestre del 2024 le frodi da manipolazione sono aumentate su tutti gli strumenti, con una crescita complessiva del 49% in valore e del 5% in numero di operazioni, rispetto allo stesso periodo dell'anno precedente, e si confermano più frequenti nel comparto dei bonifici. Nel secondo semestre del 2024 per i bonifici rappresentavano il 67% del valore e il 49% del numero delle frodi totali (Figura 7), in crescita anche nelle operazioni con carte di pagamento.

Le frodi da transazioni non autorizzate, che comprendono sia l'emissione sia la modifica dell'ordine di pagamento da parte del frodatore, mostrano una riduzione del 7% in valore e del 24% in numero di operazioni, suggerendo un effetto positivo delle misure di sicurezza, in particolare dell'adozione della Strong Customer Authentication (SCA), che ha avuto un impatto più incisivo nel contesto domestico.

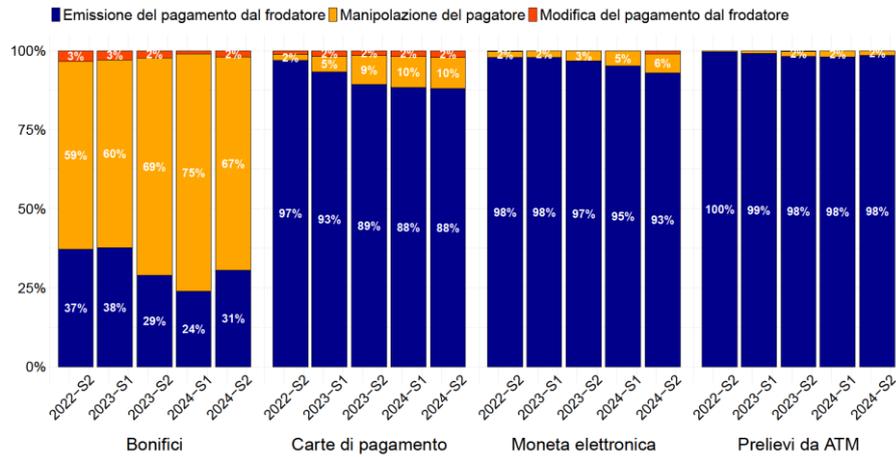
Le frodi da manipolazione sono particolarmente insidiose da contrastare poiché, essendo effettuate con il consenso dell'utente, eludono il presidio di sicurezza posto dalla SCA. Di conseguenza, essendo più difficile individuare la responsabilità del PSP, spesso l'onere della perdita grava maggiormente sull'utente. Nel caso dei bonifici, dove questa tipologia di frode è prevalente, l'89% delle perdite è sostenuto dal cliente, a fronte di quote molto più basse per carte (40%), moneta elettronica (31%) e prelievi da ATM (51%).

Questi dati evidenziano la necessità di rafforzare le misure di prevenzione e sensibilizzazione, anche in considerazione della crescente diffusione dei bonifici istantanei, che per loro natura non consentono il blocco o il richiamo della transazione una volta eseguita.

Figura 7. Operazioni fraudolente per tipologia di frode

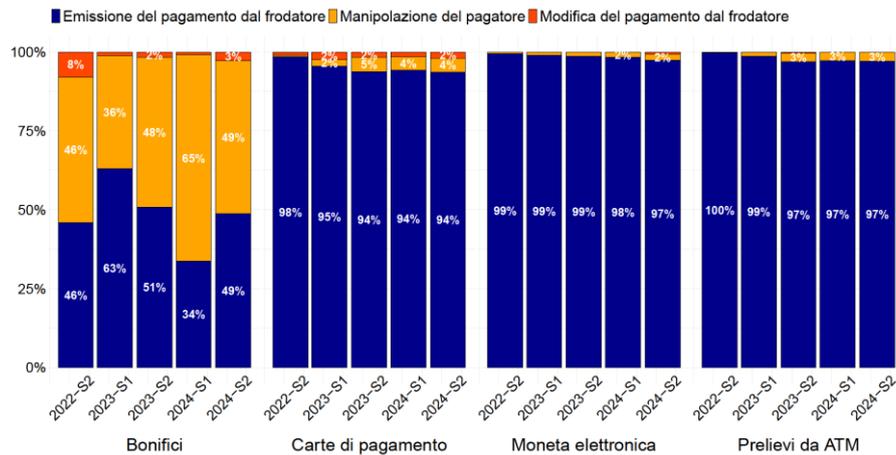
a) Valore delle operazioni fraudolente

(quote percentuali)



b) Numero di operazioni fraudolente

(quote percentuali)



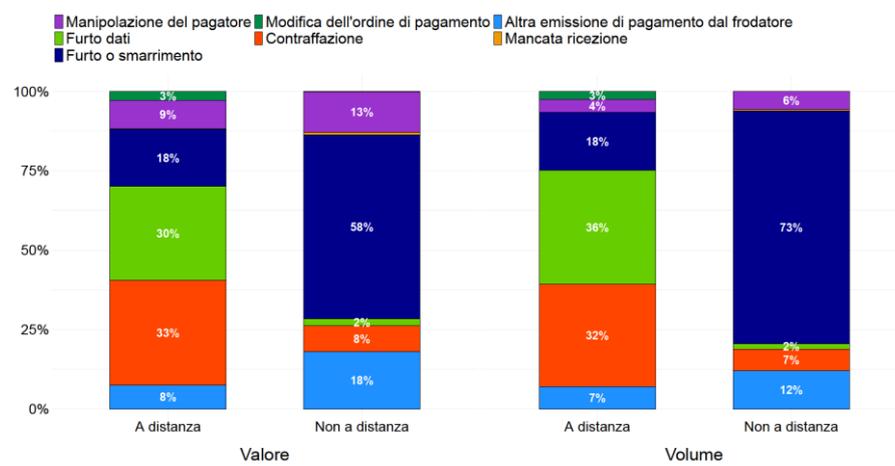
Fonte: Elaborazioni su dati di matrice dei conti forniti dai PSP italiani.

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

La gran parte (58% in valore e 73% nel numero) delle frodi nelle operazioni con carte di pagamento “non a distanza” avviene per furto o smarrimento, seguita dalla categoria “altra emissione di pagamento dal frodatore” (es. furto di account o identità), con il 18% in valore e il 12% in numero. L’incidenza delle frodi da contraffazione (es. clonazione della carta) rimane modesta, per la diffusione delle carte a microchip. Nelle operazioni “a distanza”, le frodi più frequenti sono la contraffazione (33% in valore e il 32% in numero) e il furto di dati che rappresenta il 30% del valore e il 36% del numero delle frodi. La categoria “altra emissione di pagamento dal frodatore” si attesta all’8% in valore e al 7% in numero (Figura 8).

Figura 8. Valore e numero delle operazioni fraudolente con carte di pagamento per canale di utilizzo e tipologia di frode nel secondo semestre del 2024

(quote percentuali)



Fonte: Elaborazioni su dati di matrice dei conti forniti dai PSP italiani.

3. Il ruolo dell'autenticazione forte del cliente

Questa sezione analizza il ruolo dell'autenticazione forte del cliente (*Strong Customer Authentication, SCA*)⁶ nei pagamenti elettronici - in relazione alla sua diffusione e al livello di sicurezza offerto - anche nel confronto con le operazioni di pagamento esenti dalla SCA, considerate poco rischiose dalla normativa vigente⁷ in base alle caratteristiche della transazione o ad altre misure di contenimento del rischio, e con le altre operazioni non soggette a SCA, dove rilevano ad esempio le cd. *Merchant Initiated Transaction (MIT)*⁸.

3.1 Utilizzo della SCA nei pagamenti elettronici

La maggioranza dei pagamenti elettronici avviene con autenticazione forte del cliente (Figura 9). Nel secondo semestre del 2024 le operazioni con SCA rappresentano il 71%, 77% e 68% del valore delle operazioni rispettivamente dei bonifici, delle carte di pagamento e della moneta elettronica.

Considerando il numero di operazioni, l'incidenza è ancora più elevata per i bonifici (82%), significativamente più bassa per le carte di pagamento e la moneta elettronica (48% e 42%, rispettivamente), per le quali quasi la metà delle operazioni risulta esente dalla SCA in quanto prevalentemente di modico valore.

⁶ La SCA è la principale misura di sicurezza prevista dalla PSD2 e consiste in una procedura per convalidare l'identificazione dell'utente pagatore basata sull'uso di due o più elementi di autenticazione (cd. "autenticazione a due fattori"), appartenenti ad almeno due categorie tra le seguenti: a) conoscenza (qualcosa che solo l'utente conosce, come ad esempio la password o un PIN); b) possesso (qualcosa che solo l'utente possiede, come un *token*/chiavetta o uno *smartphone*); c) inerenza (qualcosa che caratterizza l'utente, come ad esempio l'impronta digitale o il riconoscimento facciale). Queste credenziali di autenticazione devono essere indipendenti tra loro, in modo che un'eventuale violazione di uno di essi non comprometta l'affidabilità degli altri.

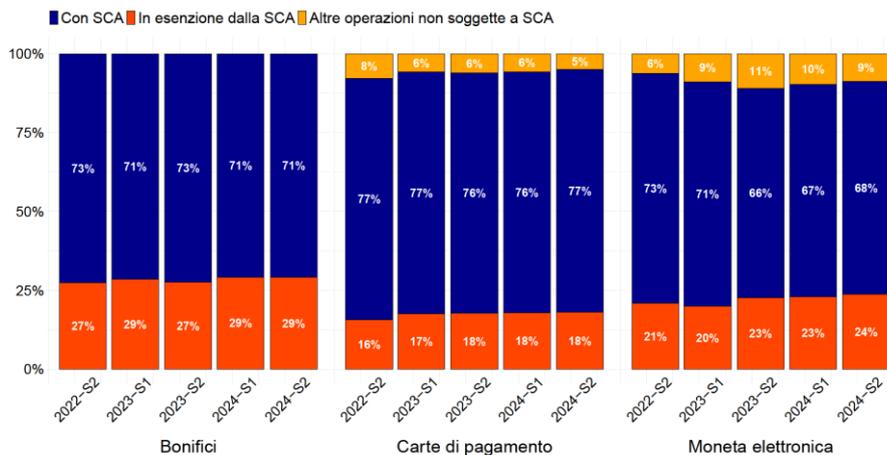
⁷ Cfr. il Regolamento Delegato (UE) 2018/389 della Commissione Europea che integra la PSD2, in relazione alle norme tecniche per l'autenticazione forte del cliente.

⁸ Le MIT sono operazioni di pagamento avviate dall'esercente o dal fornitore di servizi, previo accordo con il cliente pagatore ma senza l'azione diretta o l'autorizzazione attiva di quest'ultimo al momento della transazione; esse possono essere eseguite con modalità ricorrente ma il loro importo non è noto a priori, come ad esempio nel caso di pagamenti a fronte di "servizi di car o *bike sharing*" o di "pubblica utilità" (utenze telefoniche).

Figura 9. Operazioni di pagamento per tecnologia di autenticazione

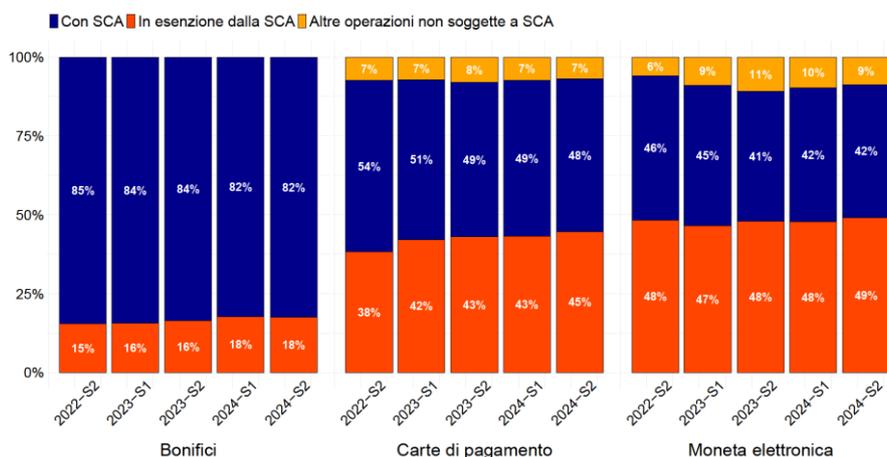
a) Valore delle operazioni di pagamento

(quote percentuali)



b) Numero di operazioni di pagamento

(quote percentuali)



Fonte: Elaborazioni su dati di matrice dei conti forniti dai PSP italiani.

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

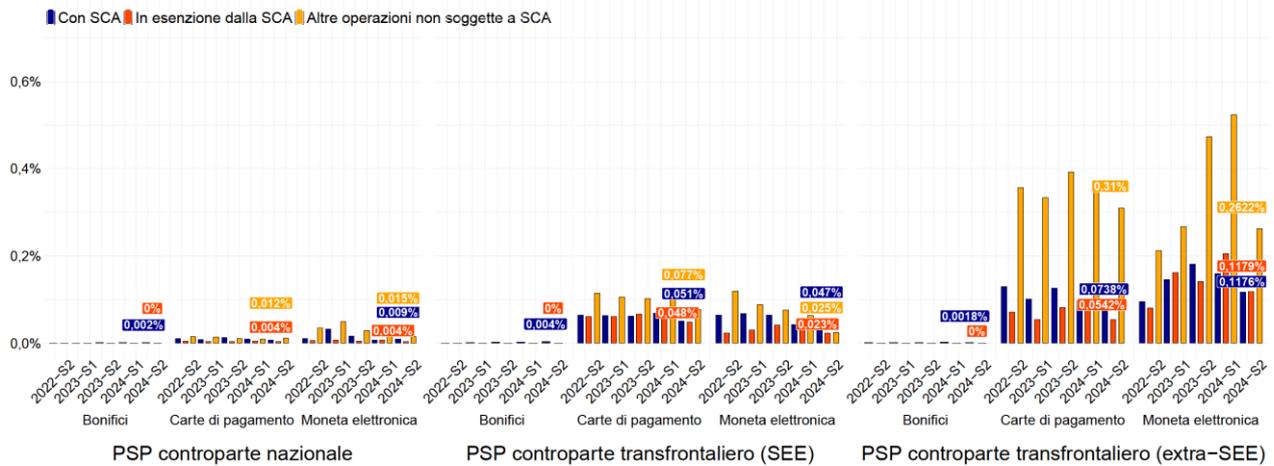
3.2 Sicurezza nelle operazioni con e senza SCA

I tassi di frode nelle operazioni con SCA risultano generalmente inferiori rispetto a quelli delle altre operazioni non soggette a SCA (Figura 10). Nel caso della moneta elettronica e delle carte di pagamento, la minore rischiosità delle operazioni con SCA è più evidente nelle operazioni *cross-border* extra-SEE.

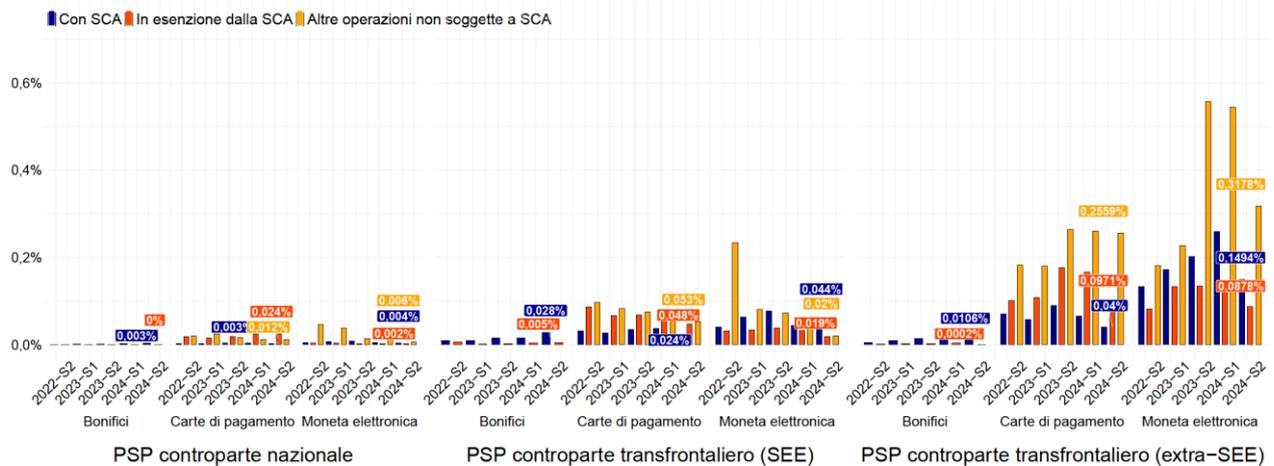
Le operazioni esenti da SCA garantiscono un livello di sicurezza analogo alle operazioni con SCA. Questa evidenza interessa tutti gli strumenti di pagamento.

Figura 10. Tassi di frode per strumento di pagamento, tecnologia di autenticazione e prospettiva geografica del PSP del beneficiario

a) Valore delle operazioni
(punti percentuali)



b) Numero di operazioni
(punti percentuali)



Fonte: Elaborazioni su dati di matrice dei conti forniti dai PSP italiani.

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

3.3 Utilizzo delle esenzioni dalla SCA

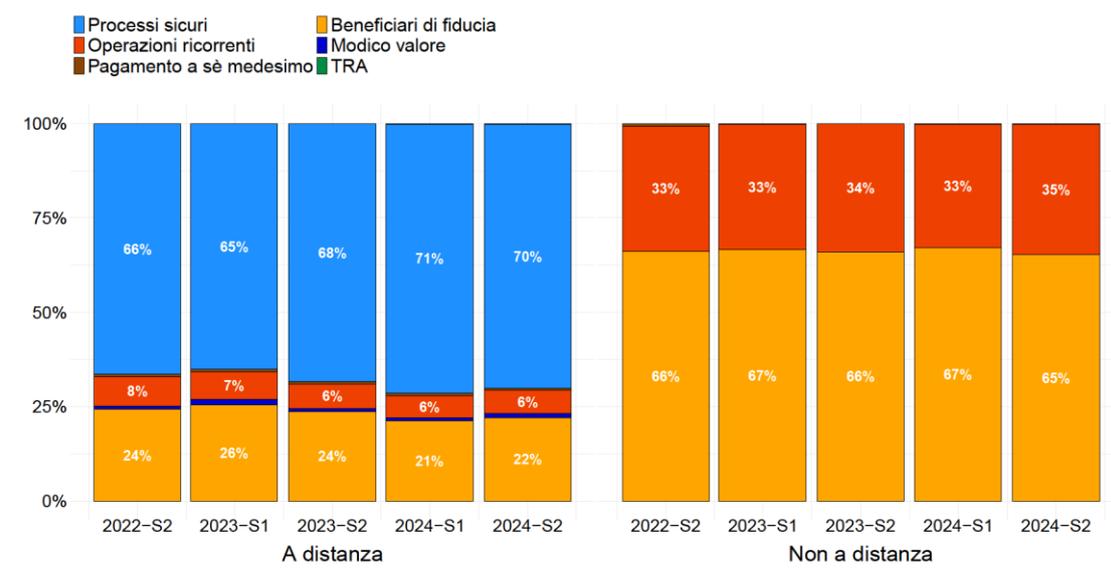
Le tipologie di esenzione dalla SCA variano in base allo strumento di pagamento e al canale di utilizzo (pagamento “a distanza” o “non a distanza”) per assicurare un adeguato bilanciamento tra livello di sicurezza garantito dalla SCA e facilità d’utilizzo dello strumento. Le esenzioni sono definite in base al livello di rischio, all’importo, alla frequenza e al canale di utilizzo del pagamento. In particolare, i PSP possono non applicare la SCA per:

- a) transazioni di “modico valore”, a distanza e in modalità “senza contatto” al POS, e che non superano un numero massimo di operazioni consecutive senza autenticazione forte del cliente;
- b) “terminali incustoditi per le tariffe di trasporto e le tariffe di parcheggio” ovvero i casi in cui la SCA non risulta facilmente applicabile per ragioni operative (ad esempio, per evitare code e potenziali incidenti ai caselli o altri rischi per la sicurezza);
- c) “beneficiari di fiducia” e “operazioni ricorrenti”, che si riferiscono entrambi a operazioni

ripetute periodicamente dopo un’iniziale autenticazione forte del cliente; nel primo caso, il ricevente appartiene a una lista di persone di fiducia precedentemente creata dal pagatore, nel secondo, il pagamento si ripete a favore dello stesso beneficiario con gli stessi parametri precedentemente impostati dal pagatore (ad esempio, la registrazione presso una piattaforma online per effettuare acquisti ricorrenti o per sottoscrivere abbonamenti a servizi periodici); d) “processi e protocolli di pagamento sicuri per le imprese”, dove il pagamento avviene tra persone giuridiche utilizzando processi e protocolli dedicati che garantiscano livelli di sicurezza equivalenti a quelli forniti dalla SCA; e) “transaction risk analysis” (TRA), per quelle operazioni a distanza valutate con un basso livello di rischio sulla base di analisi “real time” delle informazioni disponibili sul comportamento del cliente e sul tipo di pagamento effettuato; f) “pagamento a sé medesimo”, nel caso di bonifici per cui il pagatore e il beneficiario sono la stessa persona fisica o giuridica con conti di pagamento detenuti dallo stesso PSP.

Nel caso dei bonifici, le tipologie di esenzione prevalenti nelle operazioni “a distanza” sono connesse con i “processi sicuri” e con i “beneficiari di fiducia” (Figura 11), mentre nelle operazioni “non a distanza” (ovvero effettuate presso gli ATM) sono associate ai “beneficiari di fiducia” e alle “operazioni ricorrenti”. Nel secondo semestre del 2024 il 70% delle operazioni di pagamento con bonifici “a distanza” esenti dalla SCA sono state eseguite tramite processi e protocolli riservati alle imprese, il 22% verso “beneficiari di fiducia”, tipologia prevalente (65% dei casi) anche nelle operazioni “non a distanza” (ovvero all’ATM), per cui il restante 35% dei casi di esenzione riguarda le “operazioni ricorrenti”.

Figura 11. Composizione del numero di bonifici in esenzione dalla SCA
(quote percentuali)

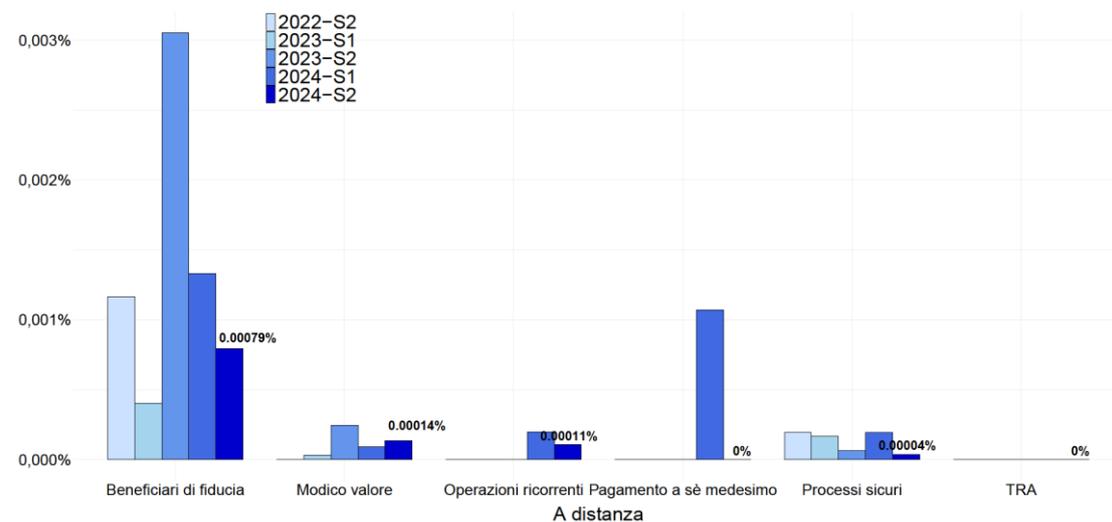


Fonte: Elaborazioni su dati di matrice dei conti forniti dai PSP italiani.

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

Per le “operazioni a distanza”, i tassi di frode più elevati per i bonifici effettuati in esenzione dalla SCA si riscontrano per i pagamenti verso “beneficiari di fiducia” e per quelli di “modico valore” (Figura 12).

Figura 12. Tassi di frode sul valore dei bonifici in esenzione dalla SCA nelle operazioni “a distanza”
(punti percentuali)



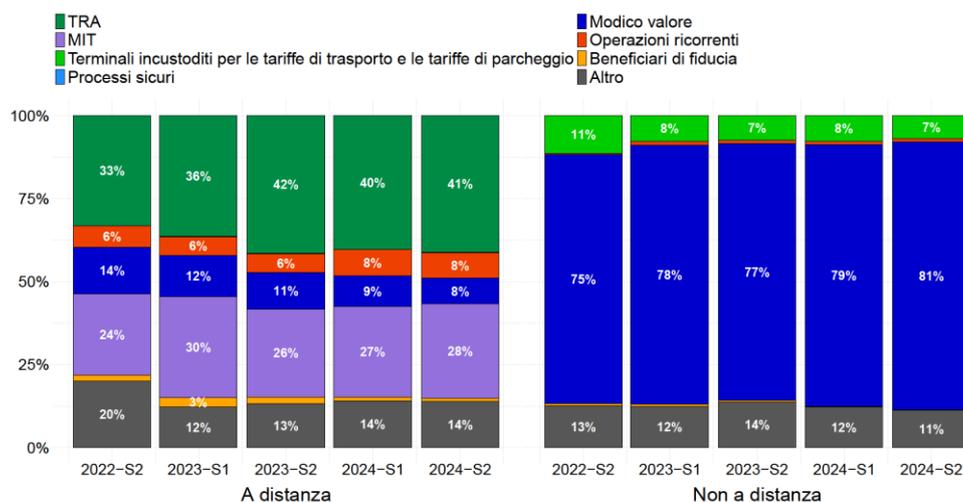
Fonte: Elaborazioni su dati di matrice dei conti forniti dai PSP italiani.

Nel caso delle carte di pagamento e della moneta elettronica, la tipologia di esenzione dalla SCA più frequente nelle operazioni “non a distanza” è quella per “modico valore” (rispettivamente 81 e 94%), mentre per le operazioni “a distanza” è quella associata alla *Transaction Risk Analysis*, “TRA” (41 e 18%), (Figure 13 e 14). Rileva anche la quota di operazioni non soggette a SCA cd. MIT⁷ nel caso delle operazioni “a distanza” con carte di pagamento (28%) e con moneta elettronica (20%).

I tassi di frode per le operazioni di “modico valore” risultano bassi anche rispetto alle altre tipologie di esenzione, così come le operazioni soggette a TRA paiono relativamente più sicure rispetto ad altre tipologie di esenzione. (Figure 15 e 16).

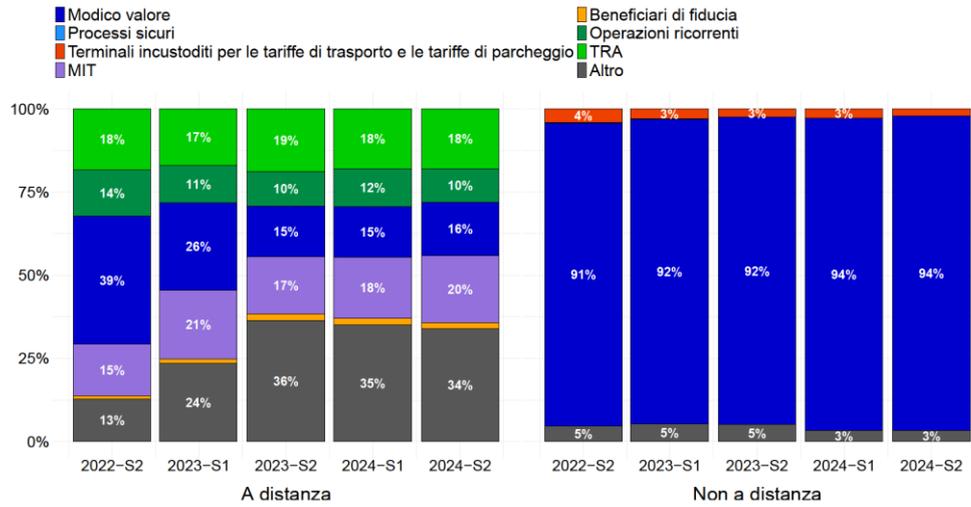
Figura 13. Composizione del numero di operazioni con carte di pagamento senza autenticazione forte del cliente

(quote percentuali)



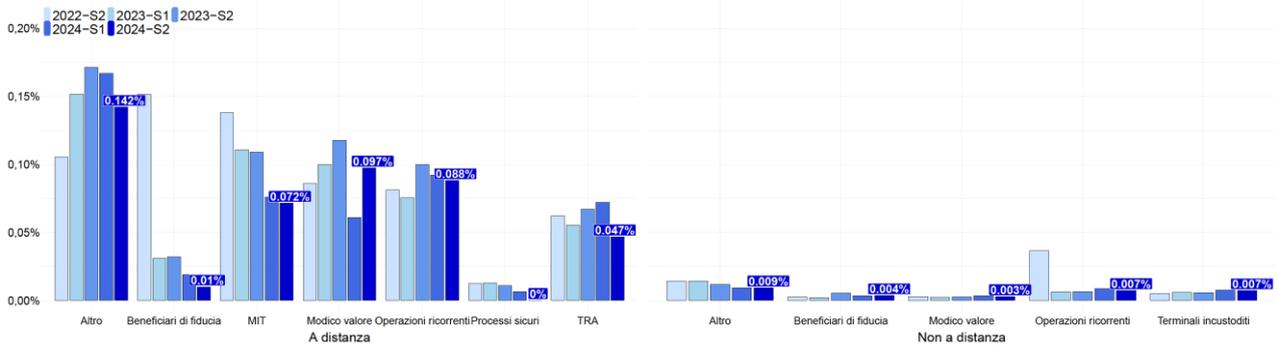
Fonte: Elaborazioni su dati di matrice dei conti forniti dai PSP italiani.

Figura 14. Composizione del numero di operazioni con moneta elettronica senza SCA
(quote percentuali)



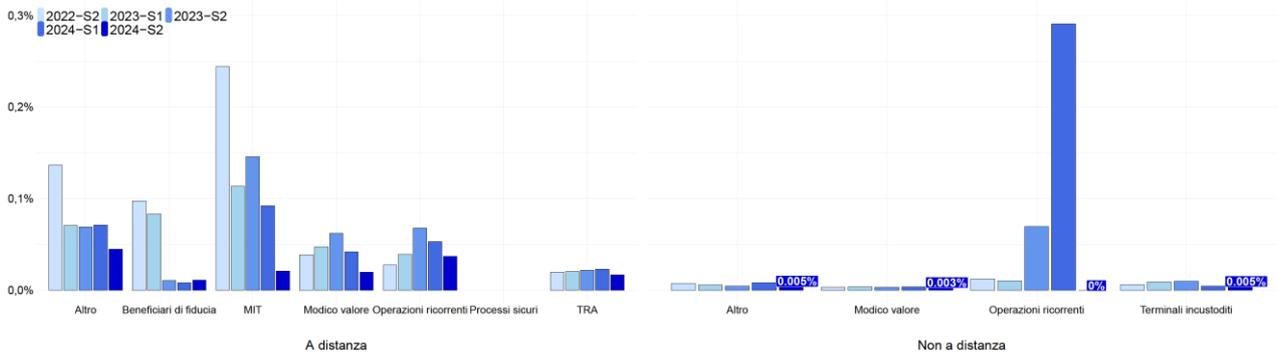
Fonte: Elaborazioni su dati di matrice dei conti forniti dai PSP italiani.

Figura 15. Tassi di frode sul valore delle operazioni con carte senza SCA per canale di utilizzo e tipologia di esenzione
(punti percentuali)



Fonte: Elaborazioni su dati di matrice dei conti forniti dai PSP italiani.

Figura 16. Valore dei tassi di frode della moneta elettronica senza SCA per canale di utilizzo e tipologia di esenzione
(punti percentuali)



Fonte: Elaborazioni su dati di matrice dei conti forniti dai PSP italiani.

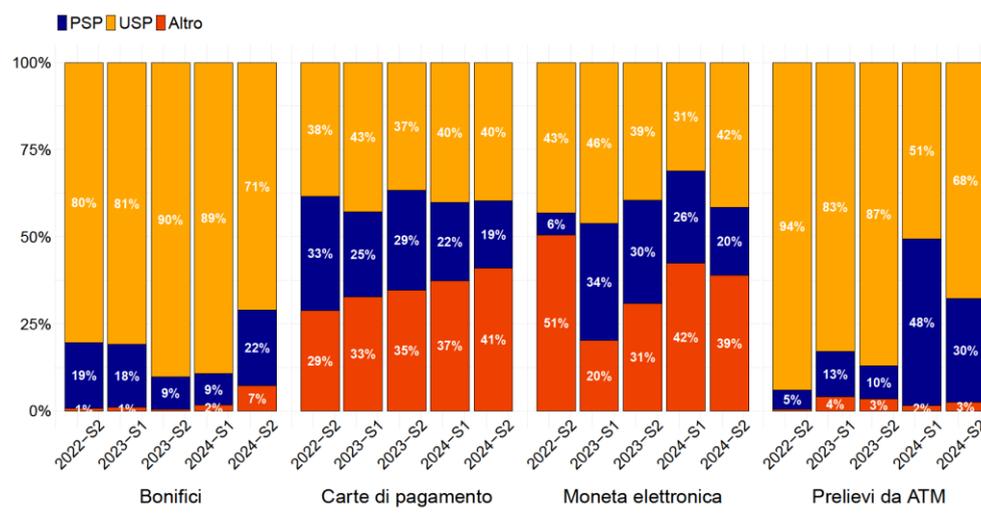
4. Le perdite da frode per portatore di responsabilità

Le informazioni disponibili sulle frodi permettono di analizzare anche la ripartizione delle perdite tra i soggetti coinvolti nell'operazione di pagamento, distinguendo tra quelle a carico del PSP del cliente ordinante, dell'utente del servizio di pagamento (USP) o da altri intermediari (ad esempio PSP del beneficiario).

La maggior parte delle perdite da frode è sostenuta dagli utenti nel caso dei bonifici e dei prelievi da ATM, dal PSP o da altri intermediari ("Altro") nel caso delle carte di pagamento e della moneta elettronica (fig. 17). Nel secondo semestre del 2024 la quota delle perdite da frode a carico dell'utente (USP) è stata pari al 71% per i bonifici e al 68% per i prelievi da ATM. Per le carte di pagamento e la moneta elettronica, invece, risulta più elevato l'onere a carico del PSP e di altri intermediari finanziari (con incidenze rispettivamente del 60% e 58%).

La ripartizione degli oneri tra i soggetti coinvolti nel pagamento è influenzata dalle caratteristiche degli strumenti utilizzati e dalla tipologia di frode prevalente. Nel caso dei bonifici, ad esempio, in cui prevale la tipologia di frode della "manipolazione del pagatore", non è possibile per il PSP attivare tutti i meccanismi di tutela previsti per le "operazioni non autorizzate" (cfr. paragrafo 2 "Le principali tipologie di frode").

Figura 17. Composizione delle perdite per strumento di pagamento e portatore di responsabilità
(quote percentuali)



Fonte: Elaborazioni su dati di matrice dei conti forniti dai PSP italiani.

Note: l'insieme dei bonifici considera anche i bonifici allo sportello, in quanto non è possibile scorporare la ripartizione delle perdite per canale di utilizzo del bonifico.