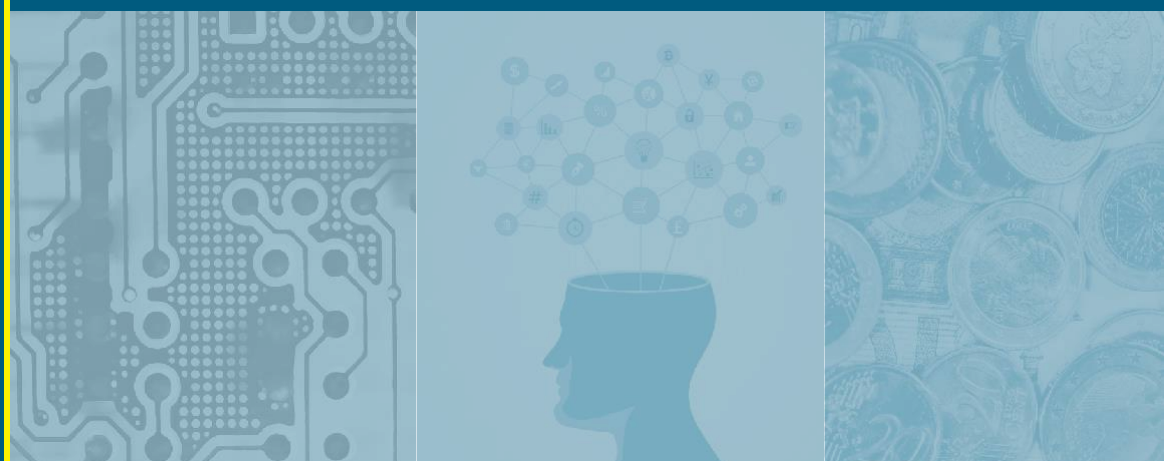




BANCA D'ITALIA
EUROSISTEMA

Comitato Pagamenti **I**talialia



RAPPORTO SULLE OPERAZIONI DI PAGAMENTO FRAUDOLENTE IN ITALIA

Febbraio 2025

Indice

Sintesi	2
1. Introduzione	4
2. Le operazioni fraudolente per strumento di pagamento	5
2.1 Le principali evidenze	5
2.2 Bonifici ordinari vs. istantanei	6
2.3 Prospettiva geografica delle operazioni fraudolente	8
2.4 Le operazioni fraudolente per canale di utilizzo degli strumenti di pagamento.....	9
3. Le principali tipologie di frode	11
4. Il ruolo dell'autenticazione forte del cliente	13
4.1 Utilizzo della SCA nei pagamenti elettronici.....	13
4.2 Tassi di frode nelle operazioni con e senza SCA	14
4.3 Utilizzo delle "esenzioni dalla SCA"	15
5. Le perdite da frode per portatore di responsabilità	18
6. L'Italia nel confronto europeo	19

Sintesi

La fiducia nei mezzi di pagamento è un bene pubblico il cui perseguimento richiede, tra l'altro, investimenti in tecnologia da parte degli operatori e la definizione di misure e/o regole volte a rafforzare la sicurezza nell'utilizzo degli strumenti di pagamento. La prevenzione e la riduzione dei rischi da frode nell'uso di strumenti digitali sono infatti punti cardine per le Autorità di sorveglianza europee al fine di assicurare l'integrità dei sistemi di pagamento al dettaglio in Europa.

Questo Rapporto fornisce un'analisi dei principali indicatori sulla sicurezza dei pagamenti al dettaglio nel nostro Paese, utilizzando le informazioni sul valore e sul volume delle operazioni fraudolente segnalate *in bonis* dai Prestatori dei Servizi di Pagamento (PSP) che operano in Italia.

Nel loro complesso i casi di frode con strumenti di pagamento elettronici sono eventi rari rispetto alla totalità delle transazioni al dettaglio effettuate nell'economia, e le relative perdite per l'utenza sono in gran parte attenuate da appositi meccanismi di tutela previsti dalla normativa di settore.

Le principali evidenze, elaborate su dati per il periodo dal primo semestre 2022 al primo semestre 2024, sono le seguenti:

- La maggior parte delle operazioni fraudolente in valore riguarda i bonifici iniziati elettronicamente (esclusi quelli eseguiti allo sportello tradizionale) e i pagamenti con carte di debito e credito. Per quanto riguarda i volumi, invece, le carte di pagamento rimangono lo strumento con il maggior numero di operazioni fraudolente, seguito dalla moneta elettronica. Gli importi e la numerosità delle transazioni fraudolente riflettono verosimilmente 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 di elevato importo nei trasferimenti tra persone fisiche (P2P) e tra imprese (B2B), mentre le carte di pagamento e la moneta elettronica, che in Italia è costituita in larga parte da carte prepagate, sono strumenti impiegati prevalentemente per l'acquisto di beni e servizi al punto vendita fisico o virtuale (P2B), originando pertanto un gran numero di transazioni ma di importo contenuto.
- Il tasso di frode (i.e. l'incidenza delle operazioni fraudolente sul totale) calcolato sul valore delle transazioni risulta contenuto e stabile nel tempo per i bonifici (0,001%), più elevato ma in calo per la moneta elettronica (0,025%). Su livelli intermedi di rischiosità si collocano invece i pagamenti con carta e i prelievi da ATM (0,019% e 0,010%, i rispettivi tassi di frode). Analoghe considerazioni si evincono dall'analisi dei tassi di frode calcolati sui volumi delle operazioni.
- Nel comparto dei bonifici il tasso di frode sia in valore sia in volume risulta molto più elevato per il bonifico istantaneo che per il bonifico tradizionale (0,048% e 0,017%, rispettivamente); questo strumento è tuttavia ancora in una fase di sviluppo ma il suo utilizzo potrà beneficiare, in prospettiva, dell'entrata in vigore della *Instant Payment Regulation* che introduce requisiti di esecuzione uniformi al fine di renderlo vantaggioso e sicuro per gli utenti.
- Il valore medio delle operazioni fraudolente è di gran lunga maggiore per i bonifici (€3.500), rispetto alle carte di pagamento, alla moneta elettronica e ai prelievi da ATM dove è ben più contenuto, rispettivamente pari a: €86, €39, €462. Queste evidenze nel loro complesso suggeriscono che la probabilità di registrare un'operazione fraudolenta, 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.
- Il tasso di frode per le carte di pagamento è sensibilmente maggiore nelle operazioni "a distanza" (i.e., e-commerce; 0,072% in valore; 0,052% in volume) rispetto a quelle "non a distanza" (al punto

vendita fisico; 0,006% in valore; 0,003% in volume) dove la presenza fisica garantisce un più efficace presidio di autenticazione del cliente. Anche per la moneta elettronica vi è analoga evidenza.

- Con riferimento alle principali tipologie di frodi, quelle con carte di pagamento e con moneta elettronica si riferiscono a operazioni effettuate senza il consenso del legittimo titolare (cd “non autorizzate” o disconosciute). Esse avvengono in larga parte “a distanza” quando il frodatore esegue il pagamento dopo aver raccolto illecitamente informazioni confidenziali o dati riservati (es: *phishing*); rientrano in questa categoria casistiche quali lo smarrimento, la contraffazione (*skimming*), la mancata ricezione, il furto della carta e quello dei dati ad essa associati. Per i bonifici rileva invece la cd. “manipolazione del pagatore”, dove il cliente stesso viene indotto a fare un pagamento dal frodatore sfruttando informazioni raccolte tramite *social engineering*.
- I tassi di frode nelle operazioni con autenticazione forte del cliente (SCA) risultano inferiori a quelli delle operazioni senza SCA soprattutto nel segmento delle transazioni transfrontaliere con carte di pagamento e moneta elettronica. Le operazioni cd. “esenti da SCA”, ovvero ritenute intrinsecamente poco rischiose sulla base delle caratteristiche della transazione (es: operazioni di modico valore o ricorrenti) o della clientela (es: operazioni a distanza valutate tramite la cd. *transaction risk analysis*), garantiscono tassi di frode pressoché confrontabili con quelli delle operazioni con SCA per tutti gli strumenti di pagamento.
- Una quota rilevante delle perdite viene sostenuta dall’utente del servizio di pagamento, nel caso dei bonifici (90%). Di contro, nel caso delle carte di pagamento, della moneta elettronica e dei prelievi ATM, l’onere risulta maggiormente ripartito tra PSP e utente (la quota a carico di quest’ultimo è pari al 40%, 31%, 51% rispettivamente). La quota di ripartizione degli oneri tra i soggetti coinvolti nel pagamento è influenzata anche dalla tipologia di frode che ad esempio nel caso di “manipolazione del pagatore” non consente di attivare tutti i meccanismi di tutela previsti invece per le “transazioni non autorizzate”.
- Secondo dati meno recenti (2023.S1), i tassi di frode sui diversi strumenti di pagamento in Italia sono pressoché in linea con quelli delle principali giurisdizioni europee. Con riferimento alle carte di pagamento, il nostro Paese riporta un tasso di frode inferiore nel confronto europeo sia in valore che in volume, riflettendo verosimilmente anche il minore livello di sviluppo del commercio elettronico, dove le frodi incidono di più. Nel caso della moneta elettronica, i tassi di frode sono più elevati in Italia dove è molto elevata l’incidenza delle carte prepagate tradizionali, molto utilizzate anche per le operazioni a distanza; il dato più recente per il nostro Paese (2024.S1), tuttavia, è in riduzione e suggerisce una convergenza verso quello medio europeo.

1. Introduzione

Per **frode** o **operazione fraudolenta** si intende l'operazione con uno strumento di pagamento effettuata senza il consenso del legittimo titolare (cd. operazione di pagamento "non autorizzata" o sconosciuta) o in conseguenza di una manipolazione operata a danno di quest'ultimo da parte del frodatore (cd. "manipolazione del pagatore").

Nel ruolo di "overseer", le banche centrali europee sono impegnate nell'attività di monitoraggio delle frodi associate ai diversi strumenti di pagamento, nella definizione di misure volte al loro contenimento e nella valutazione dell'affidabilità del sistema dei pagamenti nel suo complesso. A questi fini, l'Eurosistema si affida a informazioni statistiche sui valori e sui volumi delle operazioni di pagamento e dei corrispondenti utilizzi fraudolenti segnalati dai prestatori dei servizi di pagamento (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 Banca Centrale Europea (BCE) con cadenza semestrale e in forma aggregata, in base al Regolamento (UE) 2020/2011 relativo alle statistiche sui pagamenti.

Tali dati, oltre a soddisfare le esigenze statistiche della BCE, vengono anche utilizzati, in base al "Memorandum of Understanding" (MoU) tra EBA, BCE e BCN, per estrarre gli aggregati di interesse per l'EBA, sulla base di Linee Guida ("EBA Guidelines on fraud reporting under PSD2").

Il presente Rapporto è stato redatto utilizzando le informazioni sulle operazioni fraudolente in Italia anche nel confronto europeo al fine di esaminare i principali indicatori statistici sulla sicurezza del mercato dei diversi strumenti pagamenti al dettaglio (non riferiti al singolo operatore) nella prospettiva della Sorveglianza.¹

L'analisi considera i dati in serie storica dal primo semestre 2022 al primo semestre 2024 ed è condotta separatamente per i principali strumenti di pagamento elettronici attivati su iniziativa del pagatore², quali bonifici, carte di pagamento, moneta elettronica e prelievi da ATM. Sui dati sono possibili rettifiche significative da parte degli enti segnalanti ed è effettuata un'analisi di qualità volta a garantire una maggiore affidabilità nell'interpretazione dei trend osservati.

Il Rapporto è strutturato come segue. Il paragrafo 2 analizza le operazioni fraudolente associate a ciascuno strumento di pagamento, effettuando confronti in relazione a: *i*) bonifici istantanei vs. ordinari, data la loro rilevanza nella strategia europea sui pagamenti al dettaglio; *ii*) operazioni nazionali vs. transfrontaliere; *iii*) canale di utilizzo dei diversi strumenti, ovvero in prossimità del punto vendita fisico vs. "a distanza". Il paragrafo 3 si concentra sulle diverse tipologie di frode. Il paragrafo 4 approfondisce il ruolo dell'autenticazione forte del cliente (SCA) in relazione agli indicatori di sicurezza. Il paragrafo 5 si concentra sulla ripartizione delle perdite da frode tra i soggetti coinvolti nell'operazione di pagamenti, quali i prestatori di servizi (PSP) e gli utenti finali (USP). Il paragrafo 8, infine, confronta i principali risultati per l'Italia rispetto ad altre giurisdizioni europee.³

¹ Le definizioni degli aggregati contenuti 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.

² Nel presente Rapporto non sono considerate le statistiche sulle frodi relative agli "addebiti diretti" (pagamenti iniziati dal beneficiario) e al servizio di "acquiring di carte al POS", in quanto si modifica il punto di osservazione dei fenomeni (lato beneficiario vs lato pagatore) con il rischio di confrontare strumenti/servizi disomogenei; nel caso degli addebiti diretti, inoltre, sono tuttora in corso approfondimenti per migliorare la qualità del dato segnalato per via di un gap informativo del PSP del beneficiario su fenomeni fraudolenti realizzati a danno del pagatore.

³ Per maggiori dettagli cfr. EBA-BCE (2024), "2024 Report on Payment Fraud", August 2024.

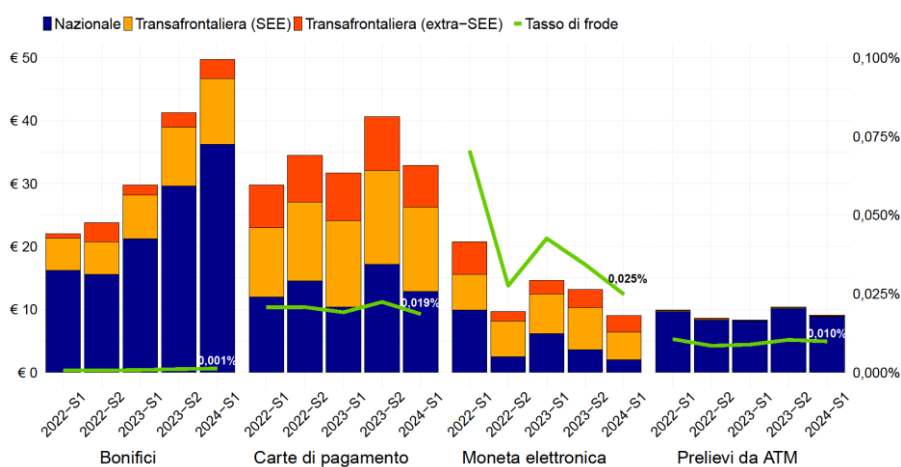
2. Le operazioni fraudolente per strumento di pagamento

2.1 Le principali evidenze

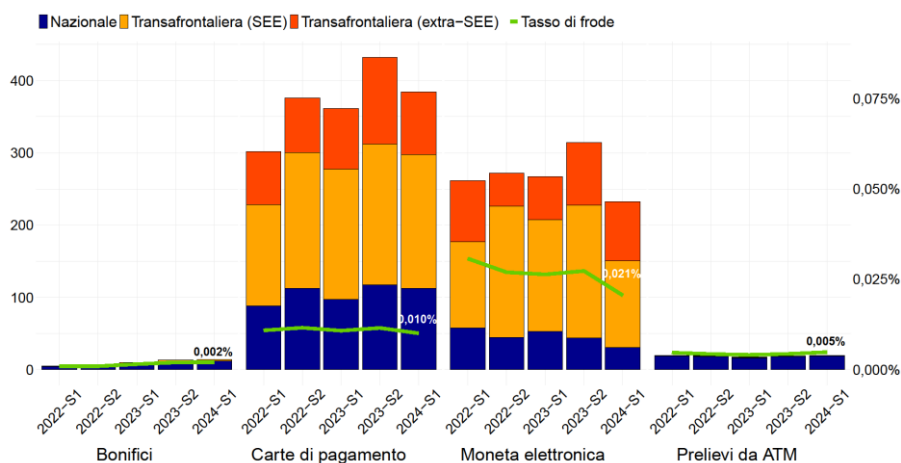
La maggior parte delle operazioni fraudolente in valore si osserva nei bonifici iniziati elettronicamente (sono esclusi quelli eseguiti allo sportello tradizionale) mentre, in termini di volumi, nelle carte di pagamento (debito e credito) e nella moneta elettronica (Figura 1). Nel 2024.S1 il valore dei bonifici fraudolenti ordinati tramite PSP italiani ammontavano a circa €50 milioni (+67% su base annua), mentre le transazioni fraudolente con carte di pagamento emesse da PSP italiani si collocavano a €33 milioni (+4%) e quelle con moneta elettronica a €13,1 milioni (+35%).

Figura 1. Operazioni fraudolente per strumento di pagamento e prospettiva geografica

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



b) Volume delle operazioni
(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: Per SEE si intende lo Spazio Economico Europeo che 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 con bonifico e con carta effettuate "a distanza" (internet, collegamenti telematici o telefonici) sono classificate come nazionali quando il PSP del beneficiario è situato in Italia mentre sono classificate come transfrontaliere all'interno del SEE (extra-SEE) quando il PSP del beneficiario è situato in un altro Stato all'interno del SEE (al di fuori del SEE). Le operazioni con carta "non a distanza" (pagamenti al punto vendita fisico e prelievi da ATM) sono classificate come nazionali quando il PSP del beneficiario (soggetto che convenziona l'esercente o che gestisce lo sportello automatico) e il punto vendita fisico e lo sportello automatico sono situati in Italia; sono classificate come transfrontaliere all'interno del SEE (extra-SEE) quando il PSP del beneficiario (soggetto che convenziona l'esercente o che gestisce lo sportello automatico) e/o il punto vendita fisico e/o lo sportello automatico è situato in un altro Stato all'interno del SEE (al di fuori del SEE).

Nello stesso periodo, il numero di bonifici fraudolenti inviati tramite PSP italiani erano meno di 13.000, mentre le operazioni fraudolente con carta e moneta elettronica ammontavano, rispettivamente, a 384.327 e 232.753. Il numero di prelievi ATM fraudolenti era anch'esso contenuto e pari a 17.700.

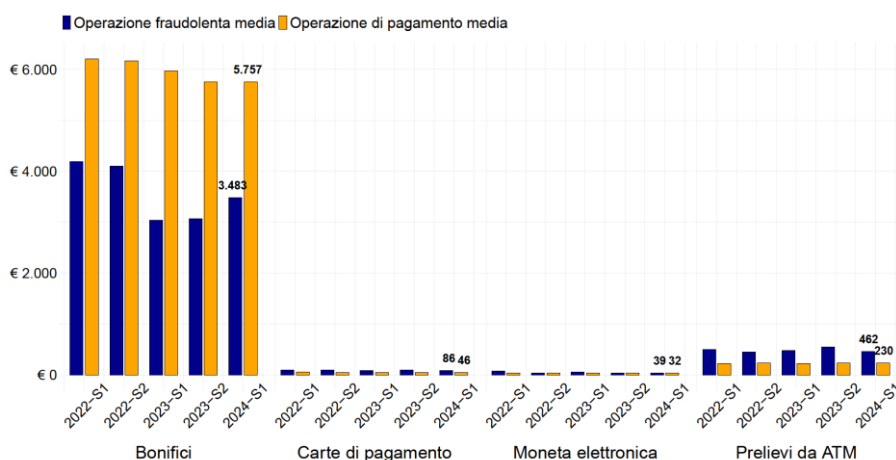
Gli importi e la numerosità delle transazioni fraudolente riflettono verosimilmente il diverso caso d'uso di ciascuno strumento e la sua diffusione nel mercato dei pagamenti al dettaglio. I bonifici sono infatti utilizzati prevalentemente per pagamenti di elevato importo nei trasferimenti tra persone fisiche (P2P) e tra imprese (B2B), mentre le carte di pagamento e la moneta elettronica, che in Italia è costituita in larga parte da carte prepagate, sono strumenti impiegati prevalentemente per l'acquisto di beni e servizi al punto vendita fisico o virtuale (P2B), originando pertanto un gran numero di transazioni ma di importo contenuto.

Il tasso di frode, definito come l'incidenza delle operazioni fraudolente sul totale delle operazioni, è più alto per la moneta elettronica e le carte di pagamento. Questo indicatore calcolato sul valore delle transazioni risultava molto contenuto e pressoché stabile nel tempo per i bonifici (0,001%) e più elevato ma in diminuzione per la moneta elettronica (0,025%); su livelli intermedi di rischiosità si collocavano invece i pagamenti con carta e i prelievi da ATM (0,019% e 0,010%, i rispettivi tassi di frode). Un quadro simile emerge anche considerando i tassi di frode sui volumi delle transazioni.

Il valore medio delle operazioni fraudolente è maggiore per i bonifici (Fig. 2). Nel 2024.S1 il valore medio fraudolento per i bonifici ammontava a circa €3.500 a fronte di valori ben più contenuti per le carte di pagamento, la moneta elettronica e i prelievi da ATM, rispettivamente pari a €86, €39, €462.

Figura 2. Valore medio delle operazioni di pagamento e di quelle fraudolente per strumento di pagamento

(importi 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 delle operazioni fraudolente.

Queste evidenze nel complesso suggeriscono che la probabilità di registrare un'operazione fraudolenta, 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.

2.2 Bonifici ordinari vs. istantanei

Nel segmento dei bonifici, il valore delle operazioni fraudolente si concentra prevalentemente in quelli ordinari, mentre in termini di volumi in quelli istantanei (Fig. 3). I bonifici istantanei si caratterizzano, infatti,

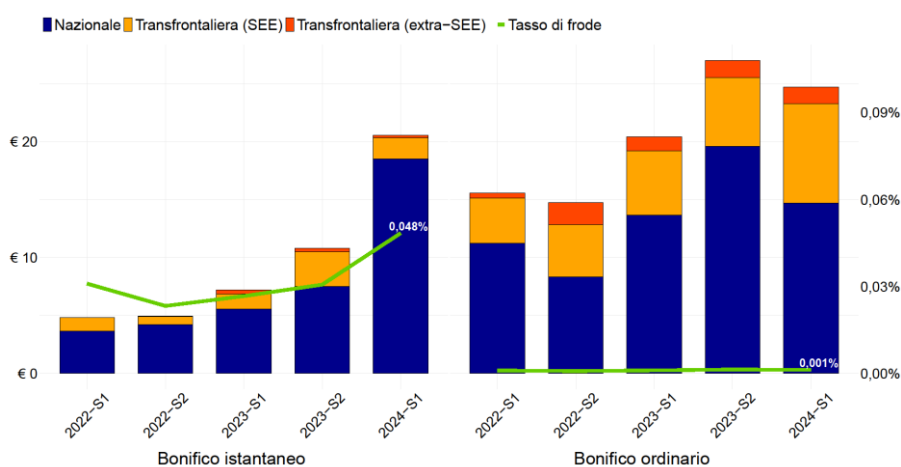
per un importo medio delle transazioni più basso rispetto a quelli ordinari, riflettendo verosimilmente il limite massimo di esecuzione di queste operazioni fissato dalla normativa regolamentare (pari a 100.000€) nonché i diversi casi d'uso.

Il tasso di frode è molto contenuto per i bonifici ordinari, ben più elevato per i bonifici istantanei. In particolare, nel 2024.S1 il tasso di frode in valore per i bonifici ordinari risultava pressoché stabile nel tempo e pari allo 0,001%, mentre per i bonifici istantanei si collocava allo 0,048%, in crescita su base annua. Con riferimento ai volumi, il tasso di frode era pari allo 0,001% per i bonifici ordinari, contro lo 0,017% per i bonifici istantanei.

Figura 3. Operazioni fraudolente per i bonifici ordinari e istantanei e per prospettiva geografica

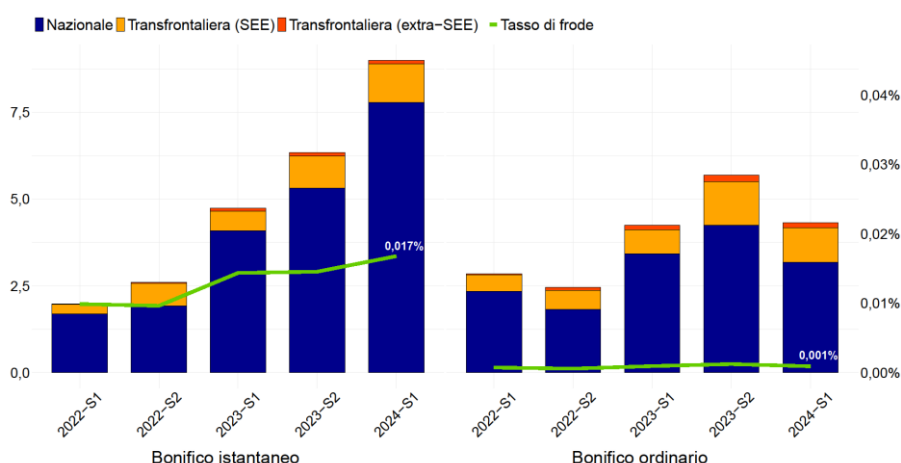
a) Valore delle operazioni

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



b) Volume delle operazioni

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

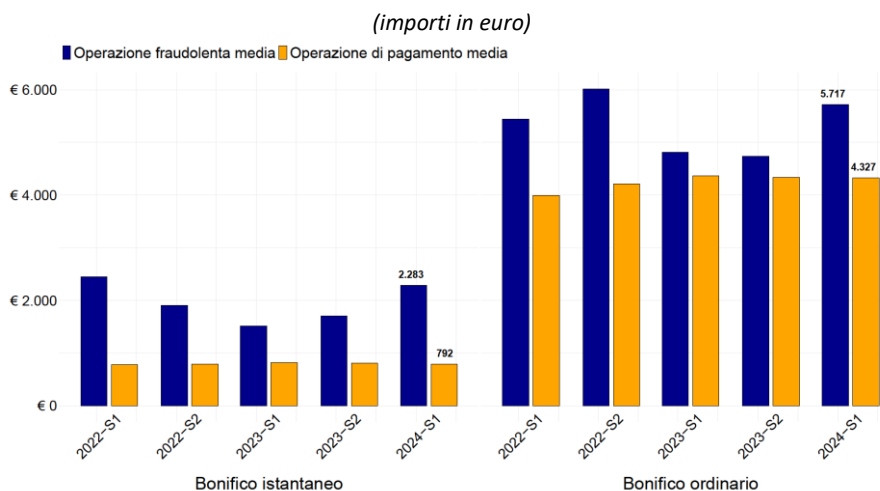


Fonte: Elaborazioni su dati di matrice dei conti forniti dai PSP italiani.

Note: Per SEE si intende lo Spazio Economico Europeo che 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 con bonifico e con carta effettuate "a distanza" (internet, collegamenti telematici o telefonici) sono classificate come nazionali quando il PSP del beneficiario è situato in Italia mentre sono classificate come transfrontaliere all'interno del SEE (extra-SEE) quando il PSP del beneficiario è situato in un altro Stato all'interno del SEE (al di fuori del SEE). Le operazioni con carta "non a distanza" (pagamenti al punto vendita fisico e prelievi da ATM) sono classificate come nazionali quando il PSP del beneficiario (soggetto che convenziona l'esercente o che gestisce lo sportello automatico) e il punto vendita fisico e lo sportello automatico sono situati in Italia; sono classificate come transfrontaliere all'interno del SEE (extra-SEE) quando il PSP del beneficiario (soggetto che convenziona l'esercente o che gestisce lo sportello automatico) e/o il punto vendita fisico e/o lo sportello automatico è situato in un altro Stato all'interno del SEE (al di fuori del SEE).

In relazione al valore medio della frode, il bonifico ordinario registrava valori di oltre il doppio superiori rispetto a quelli del bonifico istantaneo (Fig. 4). Nel 2024.S1 il valore medio delle operazioni fraudolente era pari a circa €5.700 e €2.300, rispettivamente, per i bonifici ordinari e per quelli istantanei, ma entrambi risultano in calo su base annua.

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



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 delle operazioni fraudolente.

Sebbene il bonifico istantaneo sia ancora in una fase di sviluppo, il suo utilizzo potrà beneficiare, in prospettiva, dell'entrata in vigore della *Instant Payment Regulation* che introduce requisiti di esecuzione uniformi al fine di renderlo vantaggioso e sicuro per gli utenti.

2.3 Prospettiva geografica delle operazioni fraudolente

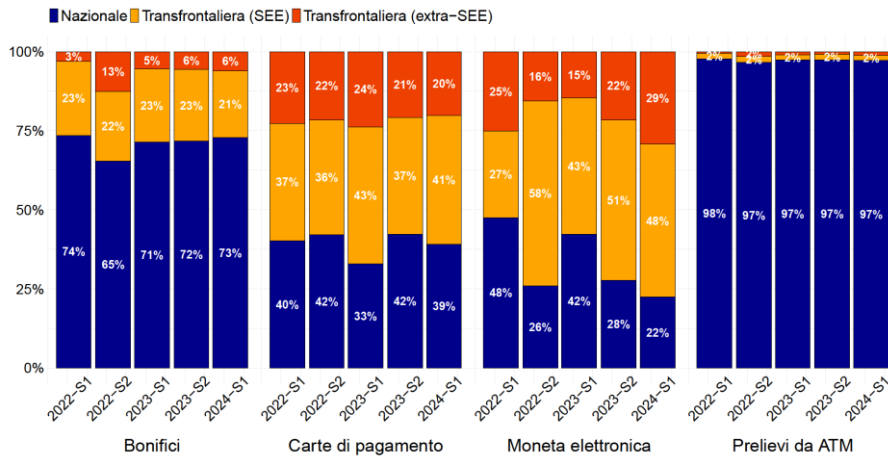
Le operazioni fraudolente possono essere analizzate anche in una prospettiva geografica, distinguendo per ciascuno strumento le operazioni "nazionali" da quelle transfrontaliere all'interno e all'esterno dello Spazio economico europeo (SEE).

La maggior parte delle operazioni fraudolente con carte di pagamento e con moneta elettronica sono relative a operazioni transfrontaliere (Fig. 5). Nel 2024.S1 il 61% del valore complessivo delle operazioni fraudolente con carte di pagamento era rappresentato da operazioni transfrontaliere (il 71% in termini di volumi). Nel caso della moneta elettronica, l'incidenza delle frodi con operazioni transfrontaliere saliva al 78% e 87%, rispettivamente, in termini di valore e di volumi. Per i bonifici, invece, la quota di operazioni fraudolente transfrontaliere risultava essere più contenuta (27% in valore e 17% in volume), in coerenza con il diverso caso d'uso che caratterizza questo strumento, poco utilizzato dagli utenti soprattutto nel commercio elettronico internazionale.

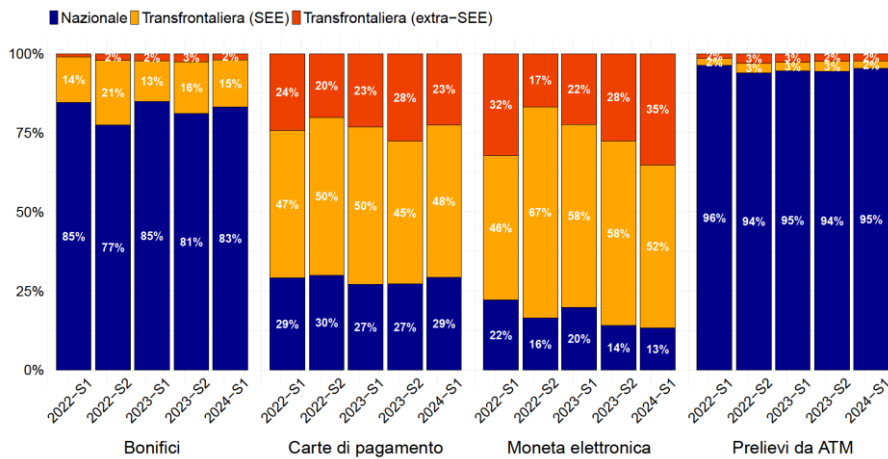
Figura 5. Composizione delle operazioni fraudolente per strumento di pagamento e prospettiva geografica

(quote percentuali)

a) Valore delle operazioni



b) Volume delle operazioni



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

Note: Per SEE si intende lo Spazio Economico Europeo che 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 con bonifico e con carta effettuate “a distanza” (internet, collegamenti telematici o telefonici) sono classificate come nazionali quando il PSP del beneficiario è situato in Italia mentre sono classificate come transfrontaliere all’interno del SEE (extra-SEE) quando il PSP del beneficiario è situato in un altro Stato all’interno del SEE (al di fuori del SEE). Le operazioni con carta “non a distanza” (pagamenti al punto vendita fisico e prelievi da ATM) sono classificate come nazionali quando il PSP del beneficiario (soggetto che convenziona l’esercente o che gestisce lo sportello automatico) e il punto vendita fisico e lo sportello automatico sono situati in Italia; sono classificate come transfrontaliere all’interno del SEE (extra-SEE) quando il PSP del beneficiario (soggetto che convenziona l’esercente o che gestisce lo sportello automatico) e/o il punto vendita fisico e/o lo sportello automatico è situato in un altro Stato all’interno del SEE (al di fuori del SEE).

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

In questa sezione viene fornita un’analisi delle transazioni fraudolente per canale di pagamento utilizzato dall’utente, distinguendo tra operazioni avviate “a distanza” che si riferiscono ai pagamenti via internet e tramite dispositivi mobili e quelle “non a distanza”, riconducibili ai pagamenti in prossimità del punto vendita fisico e ai prelievi allo sportello automatico.

Nel caso delle carte di pagamento, le operazioni “a distanza” risultano più rischiose di quelle al punto vendita fisico (Fig. 6). Nel 2024.S1 l’incidenza delle operazioni fraudolente nei pagamenti con carte su internet (es: sui siti e-commerce) rappresentava infatti il 68% del valore e il 78% dei volumi delle frodi

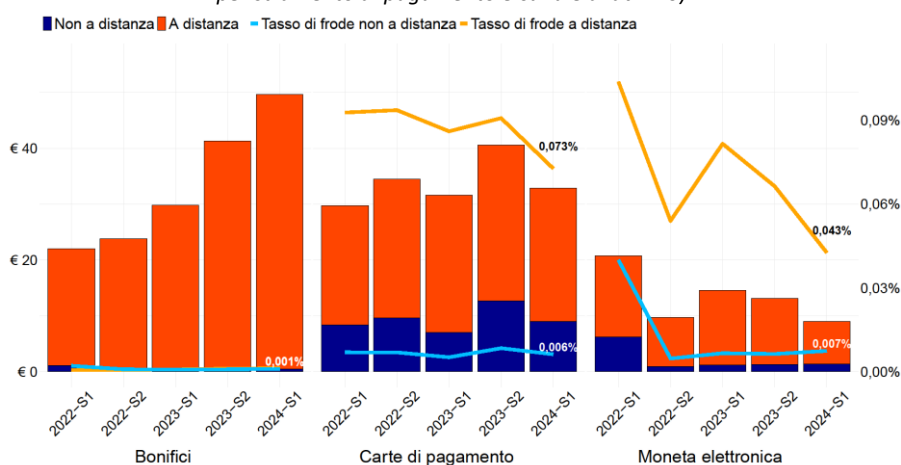
complessive, nonostante la maggior parte delle operazioni venga effettuata dagli utenti al punto vendita fisico (83% in termini di valore totale delle operazioni, 86% in termini di volumi). Il tasso di frode per le operazioni “a distanza” (0,072% in valore; 0,052% in volume) risultava pertanto pari a oltre dieci volte quello per le operazioni “non a distanza” (0,006% in valore; 0,003% in volume).

Anche per la moneta elettronica l'incidenza delle frodi è relativamente maggiore nelle operazioni “a distanza”. In particolare, nel 2024.S1 il 54% del valore delle operazioni era “non a distanza” (62% sui volumi) mentre il 90% del valore delle frodi interessava le operazioni “a distanza” (93% sui volumi).

Figura 6. Operazioni fraudolente “a distanza” vs. “non a distanza”

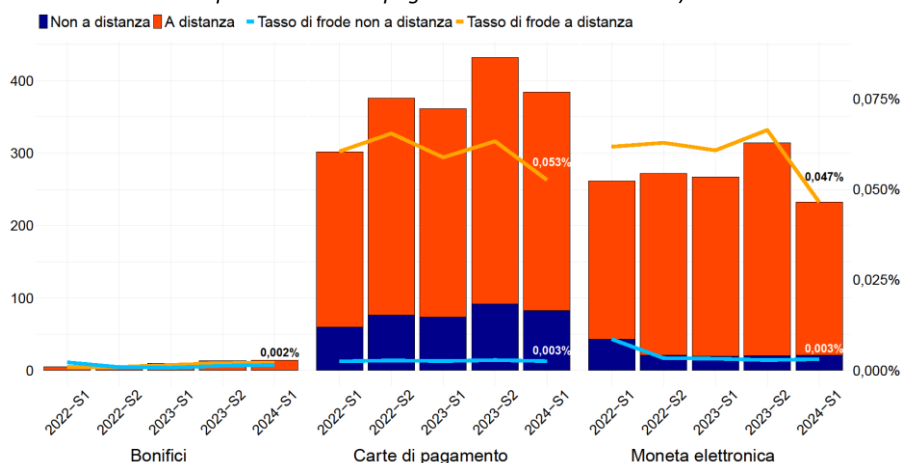
a) Valore delle operazioni

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



b) Volume delle operazioni

(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.

La rischiosità dei bonifici risulta molto contenuta, nonostante la quasi totalità di quelli elettronici sia avviata “a distanza”. In coerenza con i casi d’uso che caratterizzano questo strumento di pagamento, sebbene le transazioni fraudolente siano associate per il 99% a operazioni “a distanza” (sia in valore sia in volume), il rispettivo tasso di frode era pari nel 2024S1 allo 0,001%.

3. Le principali tipologie di frode

In questa sezione vengono fornite alcune evidenze sulle principali categorie di operazioni fraudolente per i diversi strumenti di pagamento, distinguendo anche tra operazioni “a distanza” e “non a distanza”. I casi d’uso dei diversi strumenti nonché il canale di utilizzo, infatti, sono all’origine delle nuove tecniche adottate dai frodatori, che si avvalgono soprattutto dello studio e della manipolazione dei comportamenti delle persone (cd. *social engineering*). La normativa regolamentare pone l’attenzione soprattutto sulla distinzione tra operazioni fraudolente effettuate senza il consenso del legittimo titolare (cd “non autorizzate” o sconosciute) e quelle dove il cliente stesso viene indotto a fare un pagamento dal frodatore. In tale ambito, sono distinguibili tre principali categorie di frodi:

1. **“emissione di un ordine di pagamento da parte di un frodatore”**: il frodatore si appropria illecitamente di informazioni confidenziali e dati riservati quali numeri di carta di credito, PIN e credenziali d’accesso (*username, password*) ai conti bancari, contattando gli utenti tramite email (*phishing*), SMS (*smishing*), WhatsApp o telefonate (*vishing*) per poi emettere ordini di pagamento. Per le operazioni con carte di pagamento, questa categoria è ulteriormente disaggregata in casistiche quali lo smarrimento, la contraffazione (*skimming*), la mancata ricezione, il furto della carta e quello dei dati ad essa associati.
2. **“modifica di un ordine di pagamento da parte del frodatore”**: 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 che consentono di intercettare la comunicazione tra due *host*) oppure il frodatore modifica l’istruzione di pagamento nel sistema del PSP prima che il relativo ordine sia autorizzato e liquidato.
3. **“manipolazione del pagatore”**: l’utente pagatore viene indotto dal frodatore a impartire un’istruzione di pagamento al PSP, in buona fede, su un conto che egli ritiene appartenere a un beneficiario legittimo (parente, amico, socio in affari, etc.).

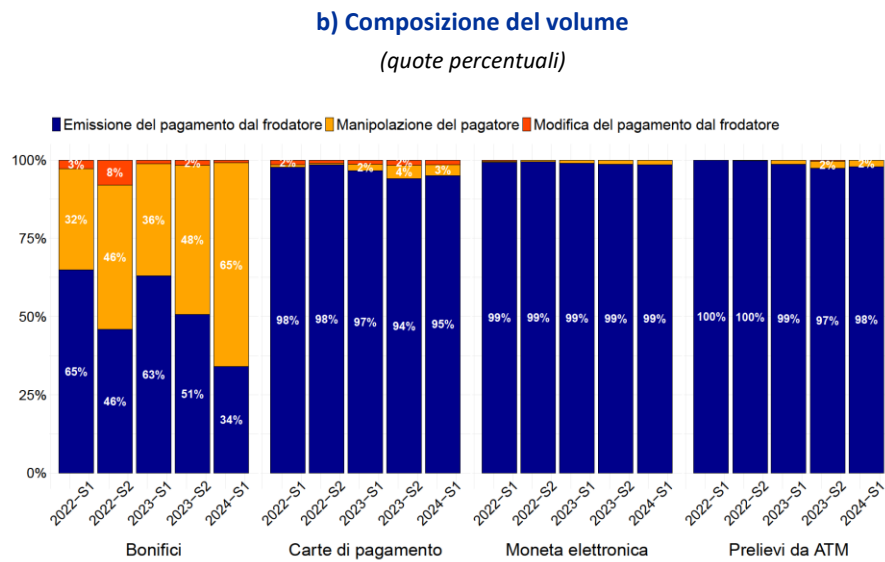
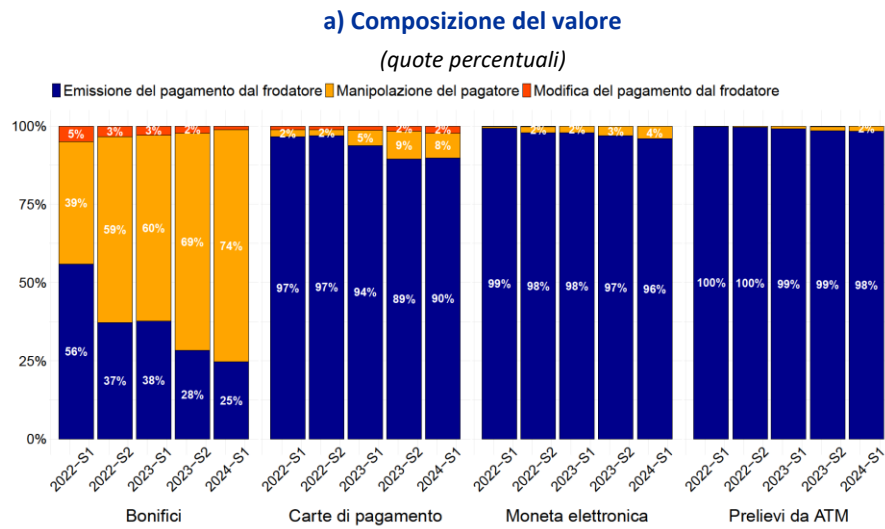
La “manipolazione del pagatore” è la tipologia di frode prevalente nel caso dei bonifici (Fig. 7). Questa categoria, in crescita nel tempo, rappresentava il 74% del valore totale delle frodi nel 2024.S1 (il 65% del numero di operazioni). La rimanente parte delle frodi era invece riconducibile all’emissione del pagamento da parte del frodatore (25% in valore e 34% in volume).

Le frodi con carte di pagamento, moneta elettronica e prelievi da ATM avvengono invece in larga parte a causa della cd. “emissione del pagamento da parte del frodatore”. Nel 2024.S1, così come nei periodi precedenti, almeno il 90% del valore e del volume totale delle operazioni fraudolente derivava da questa tipologia; la seconda causa di frode per le carte di pagamento era la cd. “manipolazione del pagatore”, sebbene ancora limitata in termini di incidenza percentuale (8% e 3%, rispettivamente, in valore e in volume).

Gran parte delle frodi nelle operazioni di pagamento “non a distanza” con carte avviene per “furto o smarrimento” (Fig. 8). Nel 2024.S1 questa tipologia rappresentava il 47% delle operazioni fraudolente in valore (69% in volume), seguita dalla categoria “altra emissione di pagamento dal frodatore” (21% in valore e 14% in volume) che rappresenta ad esempio i casi di “furto di account” o “furto di identità”. L’incidenza delle frodi da contraffazione (i.e. clonazione della carta) rimaneva invece modesta nelle operazioni “non a distanza”, grazie anche alla diffusione delle carte a microchip più difficili da duplicare.

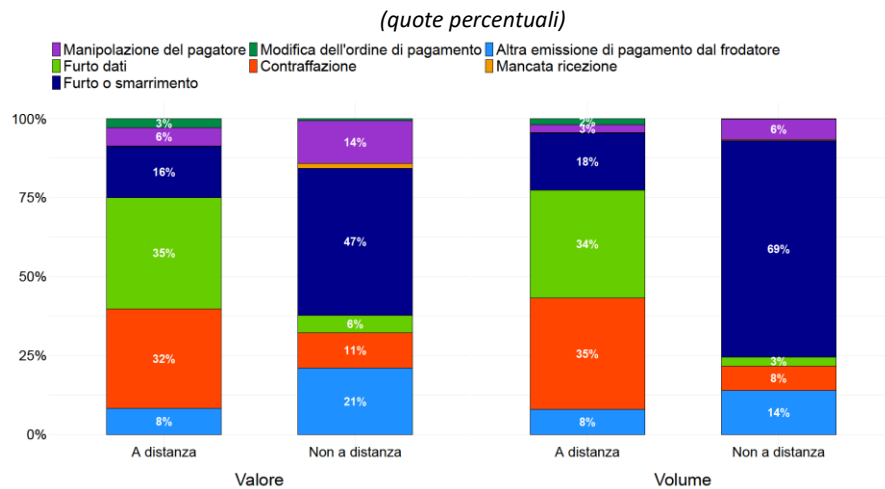
Per contro, la “contraffazione” e il furto di dati rappresentano la tipologia principale di frode nelle operazioni “a distanza”. Il “furto di dati” rappresentava nel 2024.S1 il 35% del valore delle operazioni fraudolente (il 34% del volume). La quota di contraffazione era pari al 32% in valore e al 35% in volume e rappresentava la tipologia di frode prevalente nelle operazioni “a distanza”. La categoria “altra emissione di pagamento dal frodatore” (i.e. “furto di account”) rappresentava invece solo l’8% delle frodi sia in valore sia in volume.

Figura 7. Operazioni fraudolente per tipologia di frode



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

Figura 8. Valore e volume delle operazioni fraudolente con carte di pagamento per canale di utilizzo e tipologia di frode nel 2024.S1



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

4. Il ruolo dell'autenticazione forte del cliente

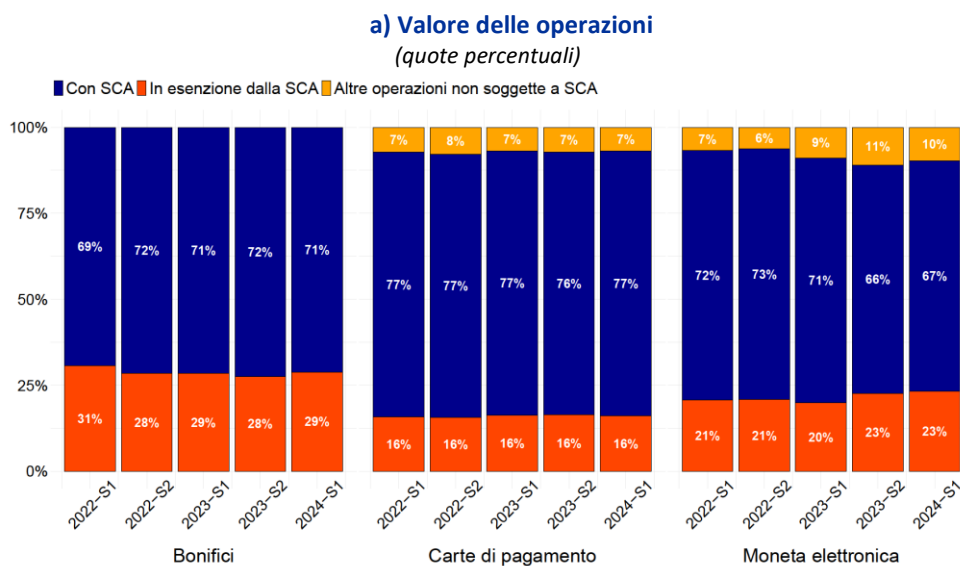
Questa sezione analizza l'utilizzo dell'autenticazione forte del cliente (*Strong Customer Authentication, SCA*)⁴ nei pagamenti elettronici con i diversi strumenti e i corrispondenti tassi di frode, effettuando un confronto del grado di sicurezza delle operazioni con SCA rispetto a quelle ritenute intrinsecamente poco rischiose dalla normativa vigente sulla base delle caratteristiche della transazione o della clientela (cd. "in esenzione dalla SCA") e alle "altre operazioni non soggette a SCA" ove rilevano, nel caso delle operazioni con carta, le cd. *Merchant Initiated Transaction, MIT*⁵.

4.1 Utilizzo della SCA nei pagamenti elettronici

La maggioranza dei pagamenti elettronici avviene con autenticazione forte del cliente oppure con altri presidi di sicurezza (Fig. 9). Nel 2024.S1 il valore delle operazioni "con SCA" rappresentavano il 71% e il 77%, rispettivamente, dei bonifici e delle operazioni con carte di pagamento, contro il 67% per la moneta elettronica.

Considerando i volumi, tale incidenza era ancora molto elevata nel caso dei bonifici (84%), mentre significativamente più bassa per le carte di pagamento e la moneta elettronica (54% e 37%, rispettivamente), dove sono più frequenti le operazioni "in esenzione dalla SCA" e l'adozione di altri presidi di sicurezza, tipici delle operazioni di modico valore.

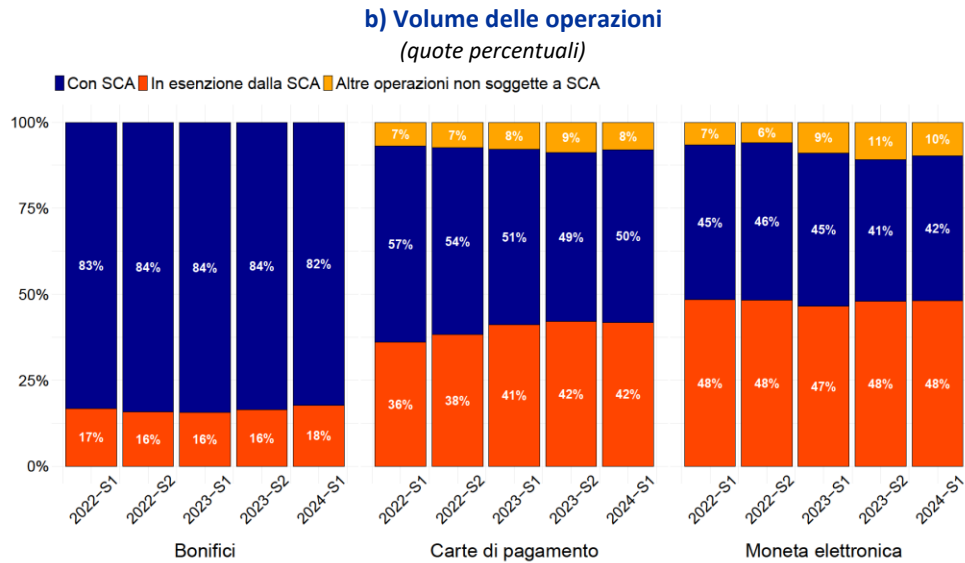
Figura 9. Operazioni di pagamento per canale di autenticazione



⁴ 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.

⁵ 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 canale di autenticazione (continua)



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

4.2 Tassi di frode nelle operazioni con e senza SCA

I tassi di frode nelle operazioni “con SCA” risultano generalmente inferiori quelli delle “altre operazioni non soggette a SCA” (Fig.10). Per le carte di pagamento questa evidenza è confermata per le operazioni transfrontaliere sia intra-SEE sia extra-SEE, con riferimento sia ai valori che ai volumi delle operazioni. Nel caso della moneta elettronica, la minore rischiosità delle operazioni “con SCA” risultava più evidente nelle operazioni verso PSP di giurisdizioni extra-SEE.

Le operazioni cd. “esenti da SCA” garantiscono un livello di sicurezza analogo alle operazioni “con SCA”. Questa evidenza rilevava per tutti gli strumenti di pagamento. Per i bonifici in particolare, nel 2024.S1 si registrava un basso livello dei tassi di frode, anche per le “altre operazioni non soggette a SCA” secondo la normativa, in quanto si tratterebbe verosimilmente di transazioni relative a casi d’uso particolari.

Figura 10. Tassi di frode per strumento di pagamento, canale di autenticazione e prospettiva geografica

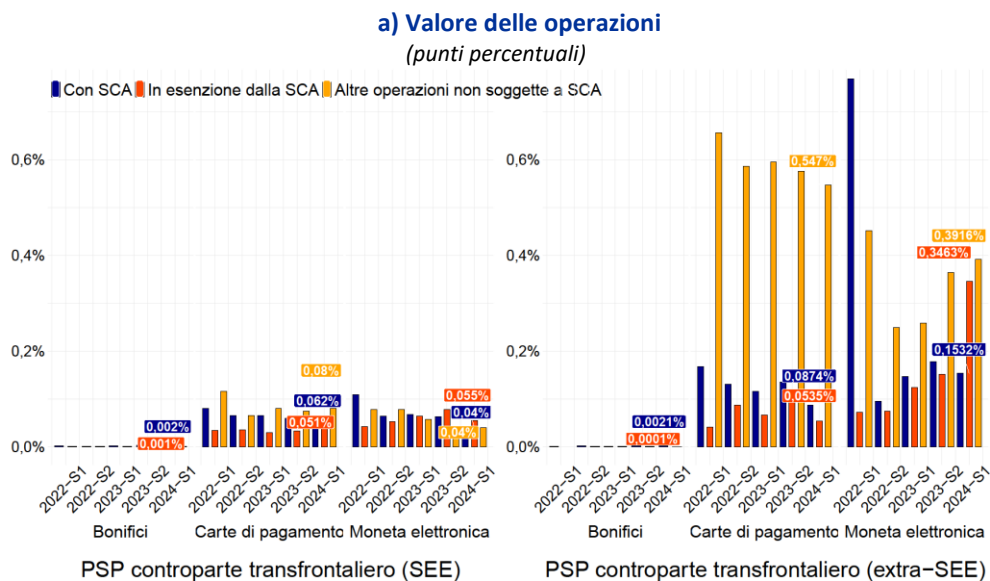
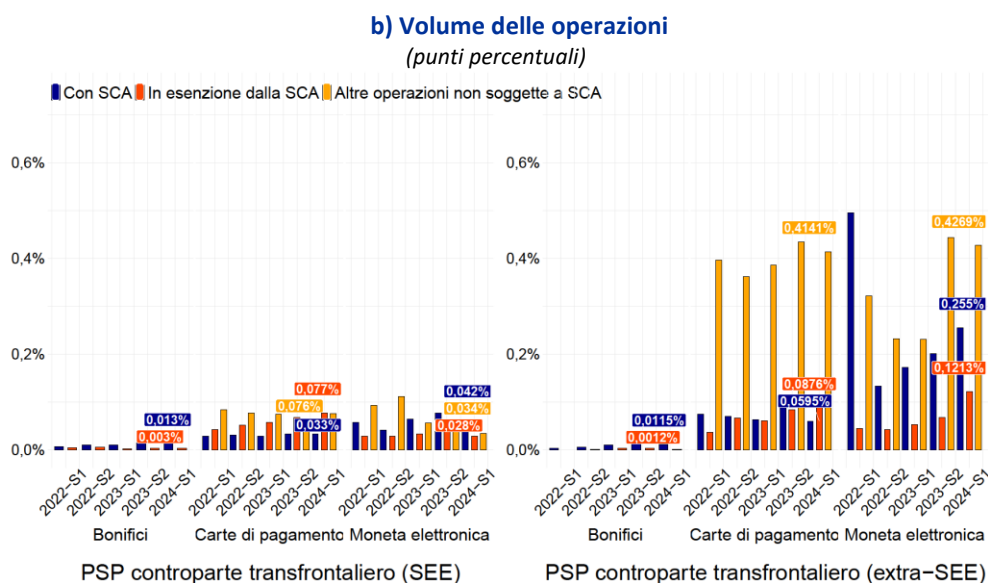


Figura 10. Tassi di frode per strumento di pagamento, canale di autenticazione e prospettiva geografica (continua)



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

4.3 Utilizzo delle “esenzioni dalla SCA”

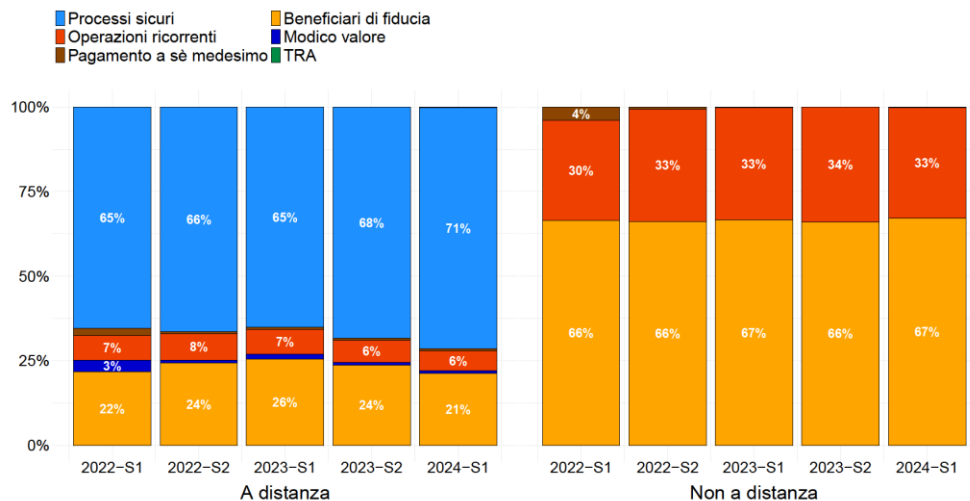
Le tipologie di esenzione dalla SCA si differenziano per strumento di pagamento e per canale di utilizzo (“a distanza” o “non a distanza”). Le esenzioni sono state introdotte dalla normativa regolamentare per bilanciare il *trade-off* esistente tra utilizzo della SCA e facilità d’uso dello strumento per il cliente soprattutto per le operazioni avviate a distanza. Le esenzioni sono definite sia sulla base delle caratteristiche della transazione quali l’importo, la ricorrenza e il canale di utilizzo del pagamento, sia sulla base della clientela. In particolare, la normativa regolamentare identifica le seguenti tipologie di esenzione:

a) “modico valore” che si riferisce a transazioni di importo contenuto, sia a distanza sia 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 l’autenticazione forte del cliente non risulta sempre 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 autorizzazione forte del cliente. Nel pagamento associato ai “beneficiari di fiducia” il ricevente appartiene a una lista di persone di fiducia precedentemente creata dal pagatore mentre nel caso delle “operazioni ricorrenti” il pagamento si ripete a favore dello stesso beneficiario con gli stessi parametri precedentemente impostati dal pagatore attraverso il ricorso all’autenticazione forte del cliente (es. registrazione presso una piattaforma online ove effettuare acquisti ricorrenti oppure per abbonamenti a servizi periodici); d) “processi e protocolli di pagamento sicuri per le imprese”, dove la procedura di esenzione si applica solo a pagamenti tra imprese che garantiscono livelli di sicurezza almeno equivalenti a quelli previsti dalla SCA; e) operazioni a distanza ritenute a basso rischio a seguito di analisi “*real time*” delle informazioni disponibili sul comportamento del cliente e sul tipo di pagamento effettuato (cd. “*transaction risk analysis*”, TRA), f) “pagamento a sé medesimo”, per le operazioni con bonifici per cui il pagatore e il beneficiario sono la stessa persona fisica o giuridica ed entrambi i conti di pagamento sono detenuti dallo stesso PSP.

Le tipologie di esenzione prevalenti nel caso dei bonifici “a distanza” sono connesse a “processi sicuri” e a “beneficiari di fiducia” (Fig.11) mentre per i bonifici “non a distanza” (i.e. presso ATM) sono associate a operazioni con “beneficiari di fiducia” e “operazioni ricorrenti”. Nel 2024.S1, il 71% delle operazioni a

distanza esenti dalla SCA erano operazioni tramite processi e protocolli riservati alle imprese, il 21% per beneficiari di fiducia. Questa tipologia era prevalente anche nelle operazioni presso ATM e pari al 67%, mentre il 33% erano operazioni ricorrenti.

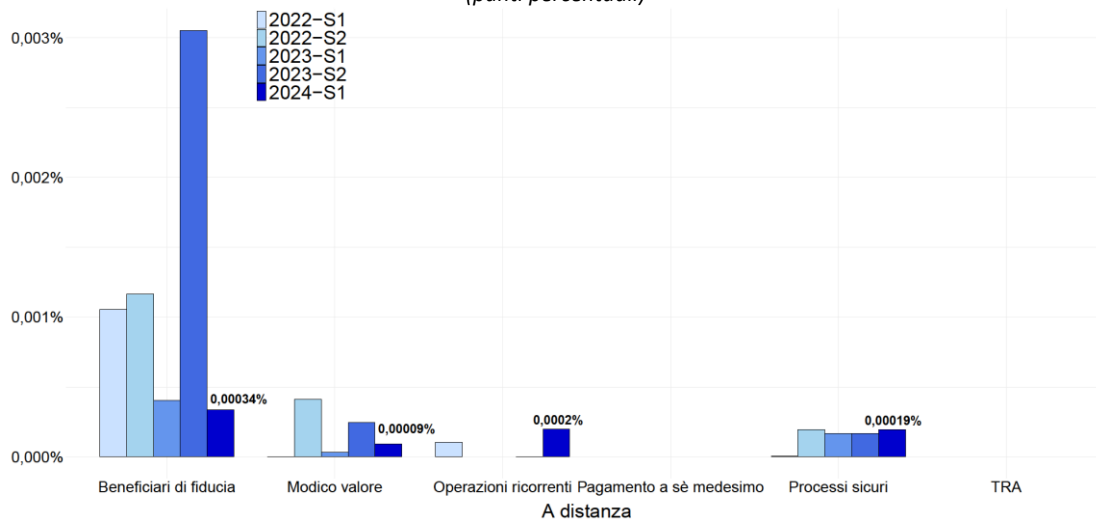
Figura 11. Composizione del numero di bonifici “in esenzione dalla SCA”
(quote percentuali)



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

I tassi di frode più elevati per i bonifici “in esenzione dalla SCA” sono per “beneficiari di fiducia” e operazioni di “modico valore” (Fig. 12). La tipologia prevalente di esenzione a distanza, i processi e protocolli sicuri per le imprese, mostrano tassi di frode pressoché nulli.

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

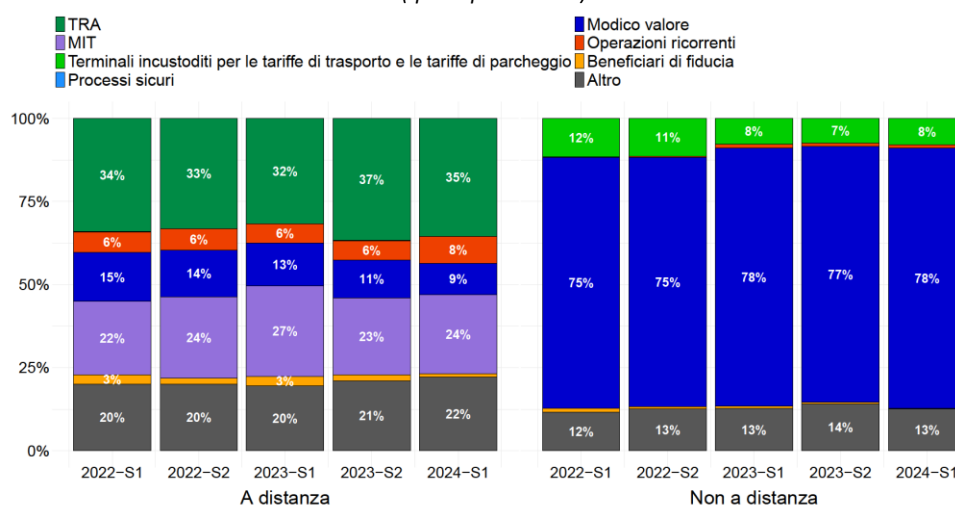


Fonte: Elaborazioni su dati di matrice dei conti forniti dai PSP italiani.

Nel caso delle operazioni al punto vendita fisico con carte di pagamento e moneta elettronica, la tipologia di esenzione dalla SCA più frequente è quella per “modico valore” (Figg. 13 e 14). Nel 2024.S1 questa tipologia di esenzione rappresentava il 78% delle operazioni “non a distanza” con carte e il 94% di quelle con moneta elettronica. Altre tipologie rilevanti di esenzione da SCA sono la *Transaction Risk Analysis* (TRA) per operazioni a distanza con carte di pagamento (35%) e moneta elettronica (18%). Apprezzabile risulta anche la quota di operazioni non soggette a SCA cd. “MIT” nel caso delle operazioni a distanza con carte (24%) e moneta elettronica (18%).

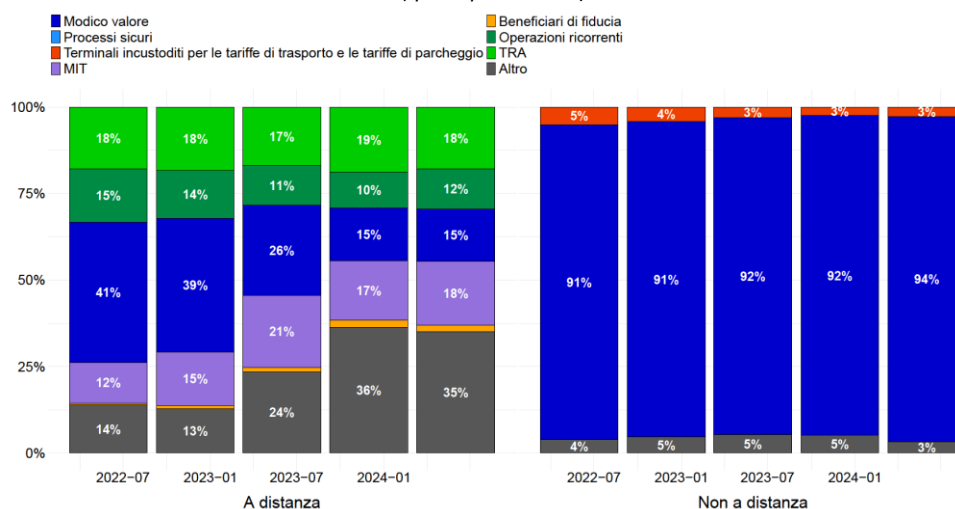
Con riferimento ai tassi di frode in valore calcolati per le diverse tipologie di esenzione, i livelli di rischio delle transazioni con carte e moneta elettronica “a distanza” sono superiori rispetto a quelli “non a distanza” (Figg. 15 e 16).

Figura 13. Composizione del numero di operazioni con carte di pagamento senza autenticazione forte del cliente (quote percentuali)



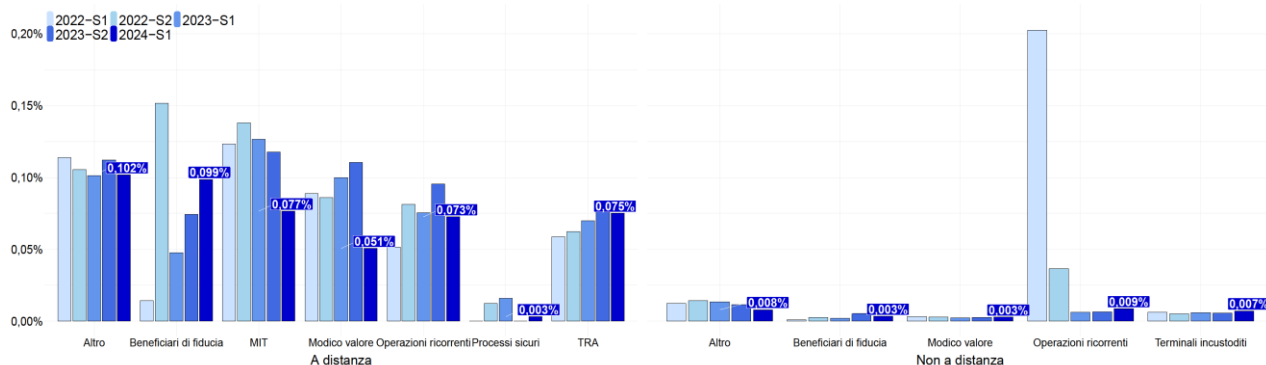
Fonte: Elaborazioni su dati di matrice dei conti forniti dai PSP italiani.

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



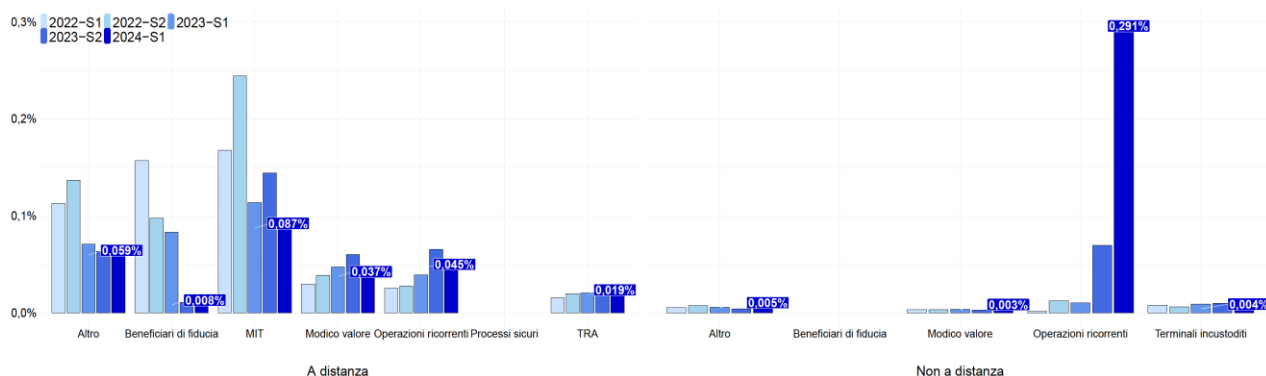
Fonte: Elaborazioni su dati di matrice dei conti forniti dai PSP italiani.

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.

5. Le perdite da frode per portatore di responsabilità

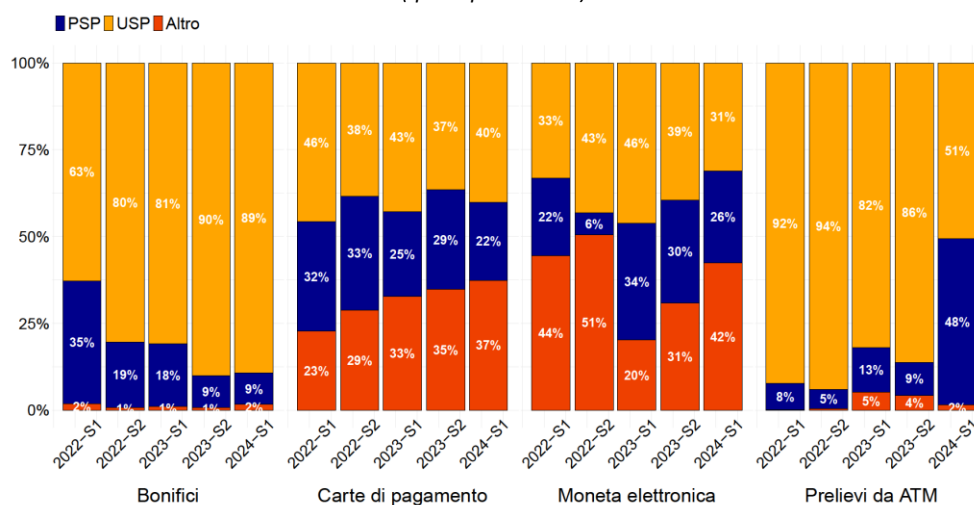
Le informazioni disponibili sulle frodi consentono anche di analizzare la ripartizione delle perdite tra i diversi attori coinvolti nell'operazione di pagamento. In particolare, gli oneri associati alle frodi sono riportati per portatore di responsabilità, distinguendo tra quelli a carico del PSP, dell'utente del servizio di pagamento (USP) o di altri soggetti (e.g. altri intermediari finanziari).

La maggior parte delle perdite da frode viene sostenuta dagli utenti nel caso dei bonifici mentre dal PSP o da altri intermediari finanziari nel caso delle carte di pagamento e della moneta elettronica (fig. 17). Nel 2024.S1 la quota delle perdite da frode a carico dell'USP era pari al 90% nel caso dei bonifici. Di contro, nel caso delle carte di pagamento e della moneta elettronica, l'onere che ricadeva al PSP era più elevata e pari al 37% e 42% rispettivamente; la quota a carico dell'USP rimaneva tuttavia di entità non trascurabile (40% e 31%, rispettivamente). Per i prelievi da ATM l'onere risultava pressoché ripartito in parti uguali tra USP e PSP.

La quota di ripartizione degli oneri tra i soggetti coinvolti nel pagamento è influenzata dalle caratteristiche intrinseche dei singoli strumenti di pagamento, dal contesto in cui i pagamenti vengono effettuati e dalla tipologia di frode prevalente per ciascuno strumento. Nel caso dei bonifici, ove prevale la "manipolazione del

pagatore”, non è infatti possibile per l’utente attivare tutti i meccanismi di tutela previsti invece per le “transazioni non autorizzate” che sono prevalenti nelle operazioni fraudolente con carta.

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.

6. L’Italia nel confronto europeo

I tassi di frode sui diversi strumenti di pagamento in Italia sono pressoché in linea con quelli delle principali giurisdizioni europee. Le tabelle 1 e 2 mostrano una panoramica del valore e del volume totale delle frodi e del tasso di frode nei principali Paesi europei per il periodo di riferimento 2023.S1, che costituisce l’ultimo dato disponibile per il confronto europeo nel Rapporto EBA-BCE (2024).

Per quanto riguarda i **bonifici**, i tassi di frode erano generalmente contenuti nei diversi Paesi (intorno allo 0,01% e 0,03%, rispettivamente per il valore e il volume di operazioni).

Con riferimento alle **carte di pagamento**, l’Italia riportava un tasso di frode inferiore a quello dei principali Paesi europei sia in valore che in volume, rispettivamente 0,019% (0,031% per la UE) e 0,010% (0,015% per la UE).

Nel caso della **moneta elettronica**, che nel nostro Paese ricomprende in larga parte le carte prepagate tradizionali⁶ per le quali è pertanto maggiore l’incidenza delle operazioni a distanza, il tasso di frode risultava maggiore in Italia sia in valore sia in volume (0,042% e 0,026%, rispettivamente) rispetto alla media UE (0,022% e 0,012%, rispettivamente). Il dato più recente per l’Italia (0,025% e 0,021%, in valore e in volume, rispettivamente al 2024.S1), tuttavia, è in riduzione e sembra suggerire una convergenza verso il dato medio europeo anche in questo comparto.

I **prelievi da ATM** mostravano generalmente tassi di frode contenuti in tutti i Paesi (inferiore allo 0,01%), in linea con il dato italiano, sia in volume sia in valore.

⁶ Per "moneta elettronica" si intende 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 (cfr. art. 2 Direttiva (CE) n. 110/2009, c.d. EMD2). In Italia la moneta elettronica si è diffusa in larga parte attraverso strumenti di pagamento prepagati basati su schema di carta "a quattro parti", mentre in altri paesi, soprattutto dell'Europa continentale, la moneta elettronica si è sviluppata soprattutto nell'ambito di schemi di pagamento cd. "closed loop", dove gli utenti effettuano e ricevono pagamenti presso conti (o wallet digitali) radicati all'interno di una rete autonoma rispetto a quella bancaria, in cui il gestore dell'infrastruttura, l'emittente dello strumento e l'acquirer che ne garantisce l'accettazione sono generalmente la stessa entità (es. PayPal).

Tabella 1. Operazioni fraudolente e tassi di frode in valore nel 2023.S1

Paese	Carte di pagamento		Prelievi da ATM		Bonifici		Moneta elettronica	
	Valore delle operazioni fraudolente (in €)	Tasso di frode	Valore delle operazioni fraudolente (in €)	Tasso di frode	Valore delle operazioni fraudolente (in €)	Tasso di frode	Valore delle operazioni fraudolente (in €)	Tasso di frode
IT	31.651.0564	0,019%	8.345.1255	0,009%	29.786.129	0,001%	14.571.868	0,042%
GE	64.755.673	0,025%	13.743.048	0,008%	146.516.621	0,000%	32.323	0,015%
SP	60.191.062	0,037%	2.336.667	0,004%	52.994.617	0,001%	1.025.153	0,025%
FR	211.361.921	0,054%	19.747.278	0,029%	155.903.705	0,001%	104.844	0,016%
GR	10.006.456	0,030%	1.911.448	0,013%	19.868.324	0,004%	178.344	0,035%
PB	32.029.596	0,036%	7.790.217	0,047%	162.487.711	0,001%	7.228	0,001%
UE	632.699.092	0.031%	62.222.205	0.008%	1.131.250.786	0.001%	53.052.802	0.022%

Tabella 2. Operazioni fraudolente e tassi di frode in volume nel 2023.S1

Paese	Carte di pagamento		Prelievi da ATM		Bonifici		Moneta elettronica	
	Volume delle operazioni fraudolente	Tasso di frode	Volume delle operazioni fraudolente	Tasso di frode	Volume delle operazioni fraudolente	Tasso di frode	Volume delle operazioni fraudolente	Tasso di frode
IT	361.099	0.010%	17.332	0.004%	9.812	0.0015%	267.392	0.026%
GE	638.036	0,011%	32.151	0,004%	75.163	0,002%	268	0,003%
SP	1.146.976	0,023%	7.340	0,002%	27.400	0,002%	23.007	0,024%
FR	3.047.131	0,032%	53.641	0,010%	44.577	0,002%	1.263	0,003%
GR	150.606	0,016%	2.875	0,004%	9.231	0,003%	4.801	0,020%
PB	377.663	0,012%	25.439	0,029%	275.786	0,014%	112	0,001%
UE	7.306.767	0.015%	173.639	0.005%	616.479	0.003%	541.432	0.012%