BANCA D'ITALIA
EUROSISTEMA

Le frodi e le misure di mitigazione del rischio nei servizi di pagamento: previsioni della PSD2 ed evidenze emerse nella sua applicazione

Andrea De Vendictis
Servizio Rapporti Istituzionali di Vigilanza
Banca d'Italia

Roma, 11 novembre 2024

Agenda

- Le frodi nei servizi di pagamento
- L'autenticazione forte del cliente (Strong Customer Authentication – SCA)
- Le esenzioni dalla SCA
- Il monitoraggio delle transazioni
- Conclusioni

Le frodi nei servizi di pagamento

- «Tutti i servizi di pagamento offerti elettronicamente dovrebbero essere prestati in maniera sicura, adottando tecnologie in grado di **garantire l'autenticazione sicura dell'utente e di ridurre al massimo il rischio di frode**.» [cit. PSD2]

- Tipo di frodi:
  - **Sulle carte**: carta persa e rubata, contraffatta, non ricevuta, non presente.
  - Manipolazione del cliente / Social engineering / campagne di social network
  - Phishing, vishing, smishing, spoofing (via e-mail, sms, search engine, siti web clonati)
  - Malware
  - Attacco "Man-in-the-middle" (es. dispositivi NFT)
  - Attacchi basati su vulnerabilità di processo (es. "sim swap", non corrispondenza tra iban e nome beneficiario)
  - AI? (es. video *fake* del CFO)

Strong Customer Authentication

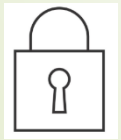
Art.97 PSD2: tutti i prestatori di servizi di pagamento (PSP) sono obbligati ad applicare la SCA quando l'utente dei servizi di pagamento (PSU):

- accede al conto *online*
- dispone un'operazione di pagamento elettronico
- esegue un'azione da remoto che può comportare un rischio di frode nei pagamenti o altri abusi (ad esempio, sottoscrizione di un mandato per addebiti ripetitivi, associazione carta al wallet).

La procedura SCA è un'autenticazione a **due** fattori per l'identificazione del PSU → a partire da almeno due elementi tra loro **indipendenti*** scelti tra le classi della conoscenza, possesso e inerenza viene generato un *codice di autenticazione non riutilizzabile*, per identificare univocamente il PSU nell'accesso informativo/dispositivo ai servizi di pagamento

Conoscenza

Qualcosa che solo l'utente conosce



Possesso

Qualcosa che l'utente possiede

Inerenza

Qualcosa che l'utente è

*** Indipendenza** = la violazione di un fattore non compromette l'affidabilità degli altri

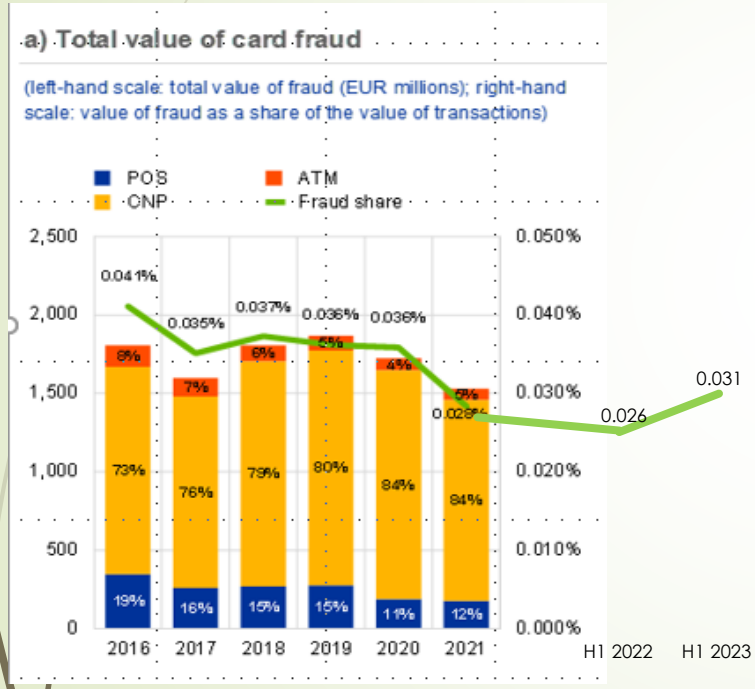
Dynamic linking

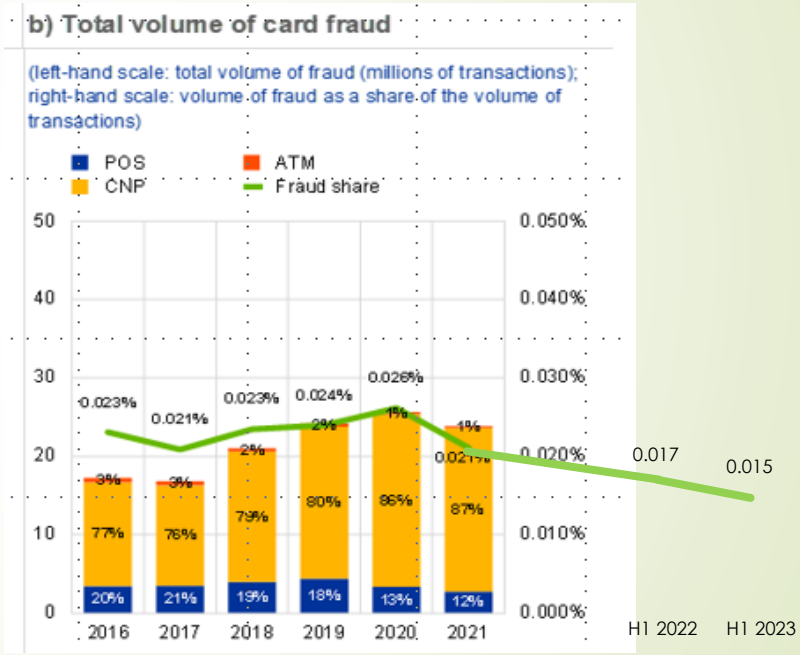
I pagamenti elettronici sono maggiormente esposti al rischio di frode e richiedono presidi di sicurezza rafforzati → **art. 5 RTS**: nelle operazioni dispositive il codice di autenticazione generato nel processo di SCA deve includere inoltre elementi collegati all'importo e al beneficiario dell' operazione di pagamento (*dynamic linking*).

L'importo totale e i riferimenti del beneficiario vengono mostrati al PSU prima di perfezionare l'autenticazione forte

Benefici della SCA

ECB REPORT (Maggio 2023) ON CARD FRAUD IN 2020 AND 2021
(integrato con dati aggiornati)

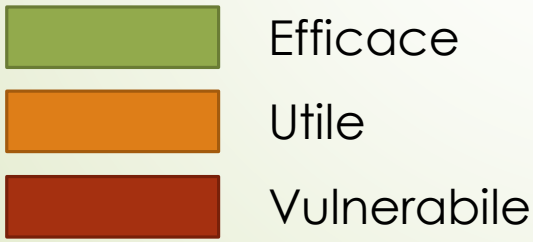




Inoltre: tasso di frode delle **MIT** (transazioni avviate dagli esercenti) e **MOTO** (transazioni per ordini postali e telefonici) **0.1%** (value)

Robustezza della SCA

- Tipo di **frodi**:
  - Carte: carta persa e rubata; contraffatta; non ricevuta; non presente
  - Manipolazione del cliente / Social engineering / campagne di social network
  - Phishing, vishing, smishing, spoofing (via e-mail, sms, search engine, siti web clonati)
  - Malware
  - Attacco "Man-in-the-middle" (es. dispositivi NFT)
  - Attacchi basati su vulnerabilità di processo (es. "sim swap")
  - AI? (es. video fake del CFO)



Esenzioni dalla SCA (1/2)

Le esenzioni dalla SCA - previste nella Sezione 2 degli RTS - sono una facoltà e non un obbligo per i PSP

Criteri di applicazione: in base al livello di rischio

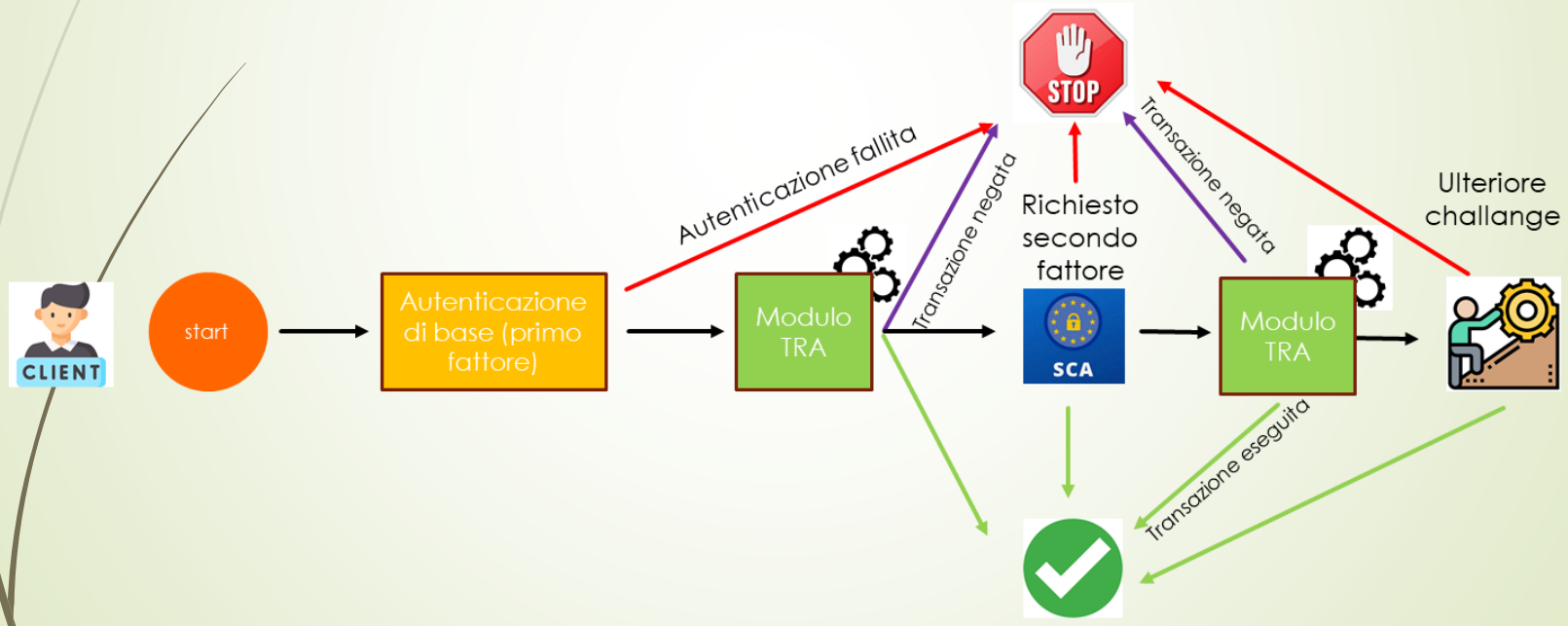
- **Art. 10 RTS** - esenzione dalla SCA per 90 giorni per l'accesso informativo al conto online
- **Art. 11 RTS –** pagamenti senza contatto fisico al punto vendita (<50 Eur e cum<150 Eur; <5 transazioni)
- **Art. 12 RTS -** terminali incustoditi per le tariffe di trasporto e le tariffe di parcheggio
- **Art. 13 RTS** - beneficiari di fiducia ovvero *white list* precedentemnete predisposta dal cliente
- **Art. 14 RTS** - operazioni ricorrenti di stesso importo e stesso beneficiario
- **Art. 15 RTS** - bonifici tra conti detenuti dalla stessa persona fisica o giuridica (giroconti)
- **Art. 16 RTS** - operazioni di modesta entità per pagamenti elettronici **a distanza** (max 30 euro, importo cumulativo max 100 euro, max 5 operazioni consecutive)
- **Art. 17 RTS** - processi e protocolli di pagamento sicuri per le imprese (a condizione che i presidi di sicurezza siano equivalenti alla SCA)
- **Art. 18 RTS** - analisi dei rischi connessi alle operazioni **in tempo reale** – transaction risk analysis (TRA)

Art. 74.2

Se il prestatore di servizi di pagamento del pagatore non esige un'autenticazione forte del cliente, **il pagatore non sopporta alcuna conseguenza finanziaria salvo qualora abbia agito in modo fraudolento**.

Procedure di monitoraggio delle transazioni

- Gli algoritmi di Monitoraggio delle transazioni (Transaction Risk Analysis - TRA) attribuiscono uno score alla transazione e, in base a regole calibrate su specifiche soglie di rischio, ne determinano la genuinità restituendo come output il blocco o l'approvazione (con eventuale *challange*) dell'operazione;



Monitoraggio delle transazioni – Criteri di valutazione

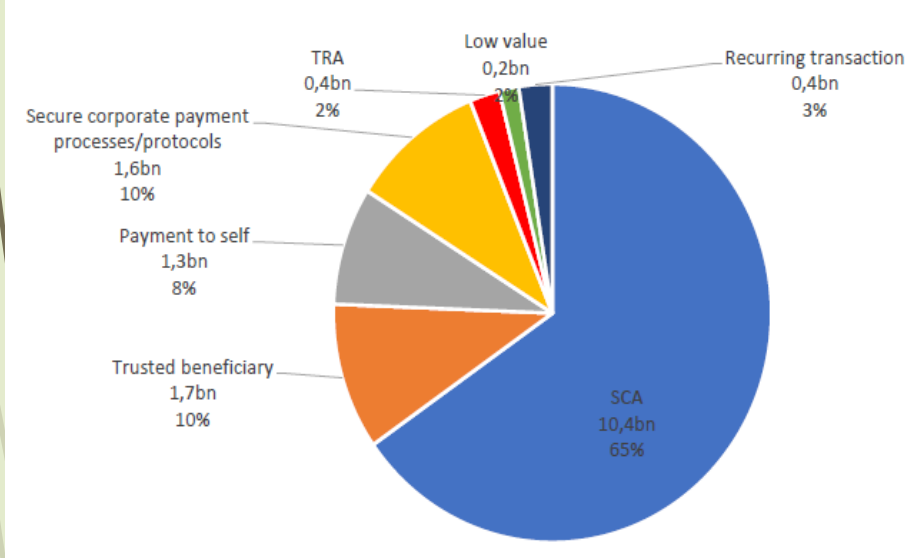
- Uno schema di spesa o di comportamento anomalo del pagatore;
- Informazioni insolite sull'utilizzo del dispositivo o del software del pagatore a fini di accesso;
- La presenza di *malware* in una qualsiasi delle sessioni della procedura di autenticazione;
- Uno scenario di frode noto nella prestazione dei servizi di pagamento;
- Localizzazione anomala del pagatore;
- Localizzazione ad alto rischio del beneficiario.

Monitoraggio delle transazioni – Punti di attenzione

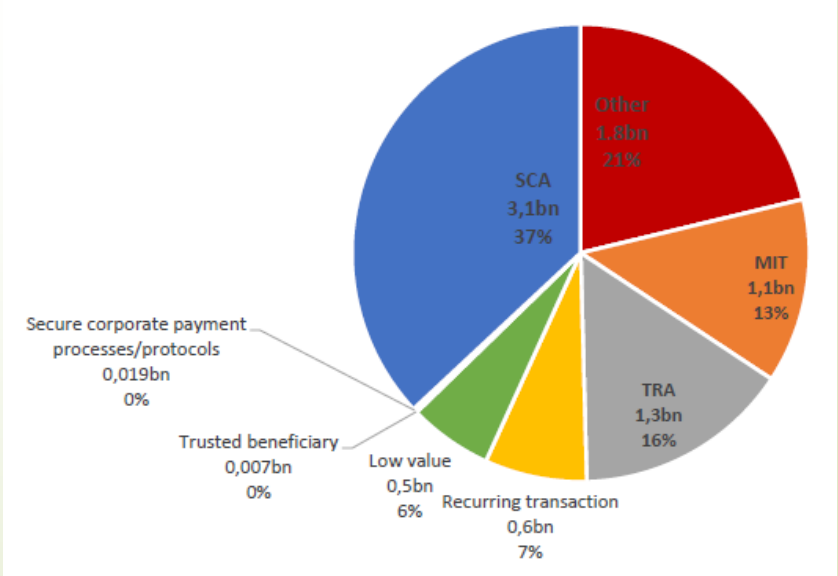
- **Sicurezza pagamento vs usabilità**
  - Algoritmi più «prudenti» implicano più falsi positivi e riducono la «user experience»
- **Sicurezza pagamento vs privacy cliente**
  - Gli strumenti di monitoraggio accedono ad informazioni eterogenee del cliente che possono andare al di là dei dati connessi allo specifico servizio di pagamento
  - Gli strumenti di monitoraggio possono fare leva su banche dati accentrate e online in cui sono raccolti i dati dei clienti
- **Monitoraggio vs «spiegabilità»**
  - Algoritmi di rilevazione delle frodi basati su ML e AI possono non fornire risultati sempre «spiegabili»

Esenzioni dalla SCA (2/2)

Bonifici



Carte



Composizione delle perdite da frode

Chart 19

Composition of losses due to card payment fraud per country and by liability bearer (H1 2023)

(share in total reported losses due to card payment fraud with cards issued in the EU/EEA)

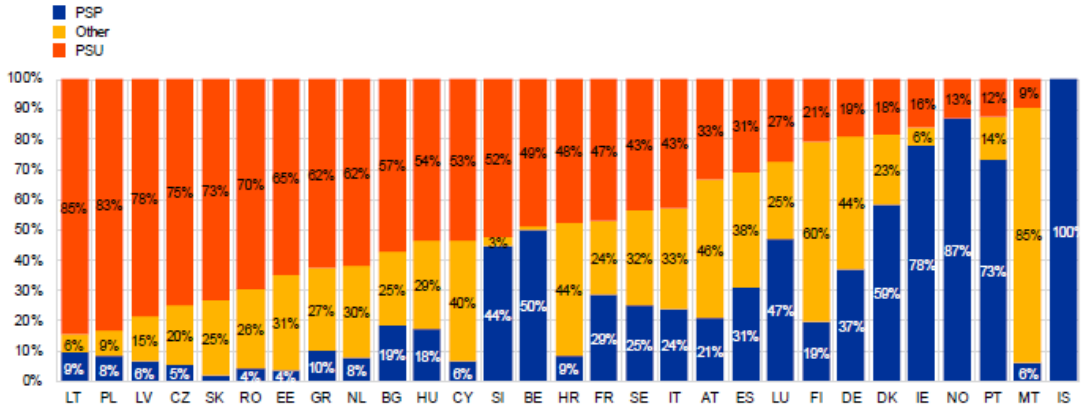
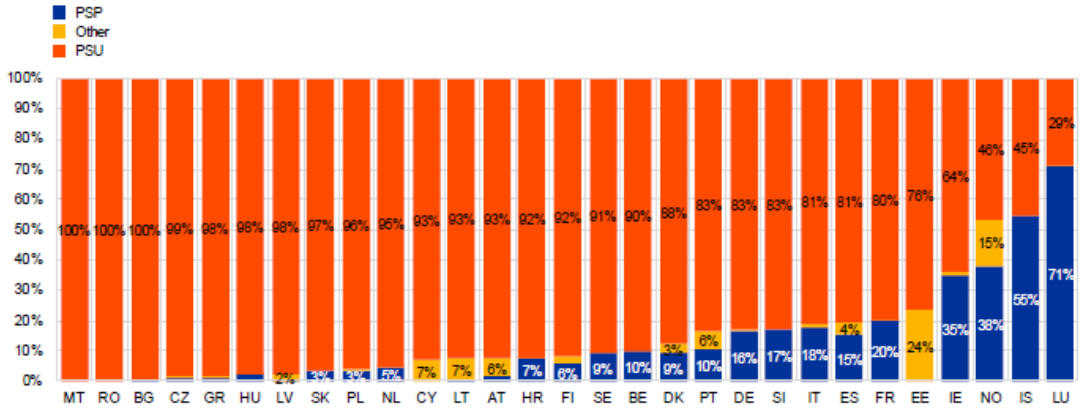


Chart 20

Composition of losses due to credit transfer fraud per country and by liability bearer (H1 2023)

(share in total reported losses due to credit transfer fraud)



PSR/PSD3 - Aspetti evolutivi

- **Rafforzamento dei:**
  - **presidi tecnologici**
    - **obbligo di soluzioni basate sul monitoraggio delle transazioni (Art. 83 PSR)**
      - Payment service providers shall have transaction monitoring mechanisms in place that: … enable payment service providers to prevent and detect potentially fraudulent payment transactions, including transactions involving payment initiation services.
      - Meccanismi di «Infosharing»
    - **Iban check (Art. 50 PSR)**
  - **presidi relativi all'educazione del cliente (Art. 84 PSR)**
    - "Payment service providers shall **alert their customers** via all appropriate means and media when new forms of payment fraud emerge..."

Fonti normative e approfondimenti

- DIRETTIVA (EU) 2015/2366 del Parlamento europeo e del Consiglio del 25 novembre 2015 (PSD2)
  Direttiva europea relativa ai servizi di pagamento nel mercato interno

- REGOLAMENTO DELEGATO (UE) 2018/389 della Commissione del 27 novembre 2017 (RTS)
  Norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri

- EBA Opinion on the elements of strong customer authentication under PSD2 (giugno 2019)
  Parere EBA contenente una lista non esaustiva di approcci di autenticazione riscontrati sul mercato (distinti in conformi alla PSD2 e non)

- Financial data access and payments package
  Proposta della CE relativa alla regolamentazione per l'accesso ai dati finanziari e i pagamenti

- NIST Special Publication 800-63B - Digital Identity Guidelines Authentication and Lifecycle Management (giugno 2017)
  Documento tecnico di riferimento per l'individuazione delle best practice di mercato sul tema delle procedure di autenticazione

- EBA Opinion on new types of payment fraud and possible mitigants (aprile 2024)
  Il documento illustra gli impatti dell'introduzione della SCA nel mercato dei pagamenti, descrive modalità di frode osservate recentemente, fornisce infine alcune proposte volte ad aumentare la protezione contro le frodi nel mercato europeo dei pagamenti (misure tecniche di sicurezza, policy di vigilanza, info-sharing, ecc.).

- EBA/ECB 2024 Report on payment fraud (luglio 2024)
  Dati sulle frodi nei servizi di pagamento nell'Unione Europe

Grazie per l'attenzione!

andrea.devendictis@bancaditalia.it

Backup – Fattori di autenticazione

Caratteristiche della SCA:

- **artt. 4-9 degli RTS**
- **Opinion EBA on the elements of SCA under PSD2**

Knowledge Element	Y/N
Password	Yes
PIN	Yes
Knowledge-based challenge questions	Yes
Passphrase	Yes
Memorised swiping path	Yes
Email address or user name	No
Card details (printed on the card)	No
OTP generated/received on a device (Hw/Sw token generator, SMS OTP)	No

Possession Element	Y/N
OTP generated/received on a device (Hw/Sw token generator, SMS OTP)	Yes
Signature generated by a device (hardware or software token)	Yes
QR code (or photo TAN) scanned from an external device	Yes
App or browser with possession evidenced by device binding	Yes
Card evidenced by a card reader	Yes
Card with possession evidenced by a dynamic card security code	Yes
App installed on the device *(no binding)*	No
Card with possession evidenced by card details (printed on the card)	No
Card with possession evidenced by a printed element (such as an OTP list)	No

Inherence Element	Y/N
Fingerprint scanning	Yes
Voice recognition	Yes
Vein recognition	Yes
Hand and face geometry	Yes
Retina and iris scanning	Yes
Keystroke dynamics	Yes
Heart rate/ body movement	Yes
The angle at which the device is held	Yes
Information via EMV® 3DS	No
Memorised swiping path	No