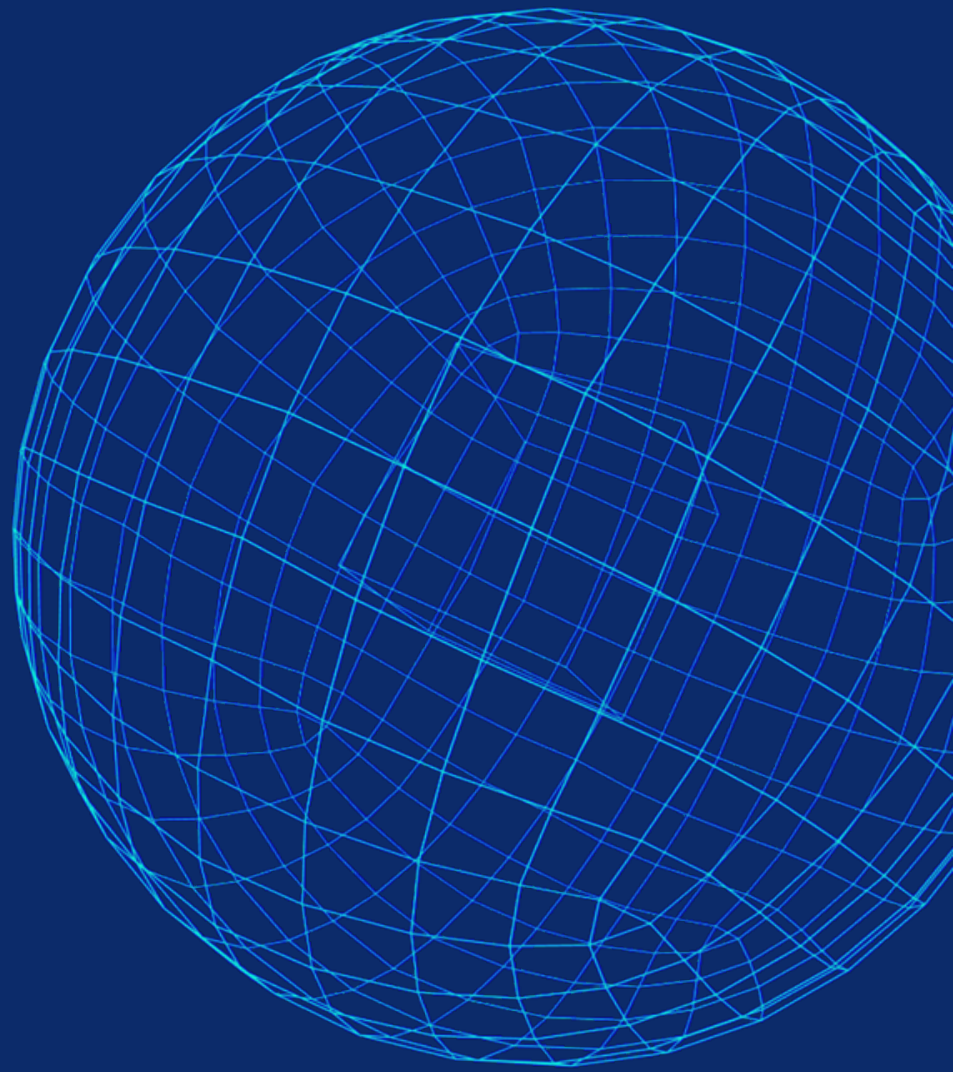
CERTFin

Sicurezza e Frodi in Banca Report 2026



KEY RESULTS

Gli analisti CERTFin di riferimento:

- **Mario Trinchera**
- **Simone Coltellese**
- **Maria Ferrucci**
- **Gabriele Gamberi**
- **Gabriele Patta**
- **Roberto Tordi**

La sfida del contrasto al cyber crime

CERTFin

Frodi bancarie 2026: il fattore umano resta il cuore del rischio

Il quadro 2026 conferma e amplifica la traiettoria tracciata lo scorso anno: il punto debole non è la tecnologia, ma la persona. La manipolazione del cliente è ormai la chiave di volta delle frodi andate a buon fine — **l'82% delle frodi effettive Retail nasce da social engineering** e il 96% delle transazioni fraudolente viene autorizzato dopo una SCA regolarmente completata.

Cambiano i canali: diminuisce il peso di telefonate e SMS (dal 60% al 46%), crescono social media e instant messaging app, mentre i falsi investimenti diventano la narrazione più efficace per attirare le vittime.

Il settore risponde: gli importi recuperati grazie alla collaborazione tra PSP (Payment Service Provider) passano da 23 a 35 milioni (+50%), mentre il ransomware sparisce dal campione e gli attacchi DDoS gravi si riducono a soli 2 casi. Cresce però l'attenzione su data breach indiretti, supply chain e rischio geopolitico, ambiti verso I quali le banche italiane stanno orientando i nuovi investimenti — più resilienza operativa, più Identity & Access Management, più presidio delle terze parti ICT.

La direzione è chiara: tecnologia solida, ma soprattutto awareness, cooperazione e cultura del rischio.

Le aree di rilevazione

Per favorire un'indagine il più possibile completa ed esaustiva, il monitoraggio esplora 5 aree ben distinte dalle cui analisi emergono diverse conferme e alcune sorprese:

1 SCENARIO, INVESTIMENTI E AWARENESS

OBIETTIVO: definire il contesto, monitorare il trend degli investimenti sostenuti nell'ambito della prevenzione e del contrasto alle frodi informatiche nonché le iniziative di formazione e sensibilizzazione del personale e della clientela intraprese dal settore.

EVIDENZE CHIAVE

- **La percentuale media di budget destinata dalle banche alla sicurezza IT** si prevede che dal 6,45% del 2025 passi all'8% nel 2026. La quota riservata al contrasto delle frodi cresce al **13,5%** (era il 12%).
- **L'81% delle banche prevede un aumento degli investimenti lato organizzazione** (di cui il 23% rilevante); il 71% prevede un aumento sui servizi rivolti alla clientela.
- **Nel prossimo biennio le priorità di investimento sono resilienza operativa digitale (87%)**, soluzioni anti-frode (84%) e Identity & Access Management (81%).
- **Il 100% del personale di filiale è coinvolto in iniziative di formazione**; il presidio si estende anche a Top Management (93%) e a Help Desk (92%).
- **Il 77% delle organizzazioni ha attivato iniziative di formazione verso i fornitori ICT (TPP)**, con focus crescente su Third Party Risk Management e continuità operativa.

Le Aree di Rilevazione

CERTFin

2 DIMENSIONAMENTO DELLE FRODI

OBIETTIVO: indagare i canali, i target, la numerosità e i volumi che caratterizzano le dinamiche fraudolente osservate.

EVIDENZE CHIAVE

- **Numero di accessi: oltre 7 mld Retail e 400 mln Corporate.** In merito agli importi economici relativi a transazioni anomale, emerge che, nel segmento Retail, l'82% viene preventivamente bloccato, il 4% recuperato e il 14% perso.
- **Forte aumento degli importi recuperati: da 23 a 35 milioni di euro (+50%)** grazie al protocollo di collaborazione antifrode tra PSP italiani.
- **Manipolazione utente:** nel Retail il 61% dei clienti manipolati subisce una perdita. Nel Corporate la manipolazione è efficace nel 68% dei casi.
- **Sul Retail il bonifico istantaneo nazionale concentra quasi il 50% delle frodi effettive** per numerosità, a seguire il bonifico ordinario nazionale che si assesta al 23%.
- **Le vittime con più di 45 anni rappresentano oltre il 70% del totale**, con gli over 60 al 43%. Nel Corporate le microimprese sono colpite nel 51% dei casi.
- **Malta è la nuova destinazione preferita dai frodatori nello SEE (61% delle indicazioni)**, superando la Lituania che per 4 anni ha guidato la classifica. Il controvalore delle transazioni anomale dirette all'estero passa da 53 a 115 mln di euro (+117%).

Le Aree di Rilevazione

CERTFin

3 MODALITÀ DI ATTACCO

OBIETTIVO: indagare i canali, i target, la numerosità e i volumi che caratterizzano le dinamiche fraudolente osservate.

EVIDENZE CHIAVE

- **L'81% delle frodi Retail effettive nasce da manipolazione del pagatore** (70% nel Corporate). Il cliente legittimo, raggirato dai criminali, spesso dispone di propria iniziativa l'operazione.
- **Il 96% delle transazioni fraudolente effettive è autorizzato con SCA correttamente completata**: l'autenticazione forte non viene "bucata", ma aggirata manipolando la vittima.
- **L'abuso dei canali telco scende al 46% (era il 60% nel 2024 e l'87,5% nel 2023)**; i social media salgono al 22% e le instant message app si attestano al 10%.
- **Nel Corporate torna a crescere il peso della Business E-mail Compromise (23% delle frodi effettive)** e delle compromissioni della casella e-mail (19% come vettore iniziale).
- **Il social engineering domina la finalizzazione delle frodi Retail (77%);** tra le diverse tipologie prevalgono i **falsi investimenti (36%)** e i **task scam (25%)**.
- **Identificati nel 2025 circa 17.000 conti correnti riferibili a money mule**, a conferma delle significative dimensioni della rete di riciclaggio criminale.

Le Aree di Rilevazione

CERTFin

4 MECCANISMI DI RILEVAZIONE

OBIETTIVO: monitorare e valutare con senso critico gli strumenti utilizzati dai PSP per identificare le operazioni fraudolente sia in prevention sia in detection.

EVIDENZE CHIAVE

- **Il transaction monitoring interno resta la prima fonte di segnalazione** sia per il Retail (57%) sia per il Corporate (58%).
- **Il 25% delle soluzioni di monitoraggio è basato su tecnologie di AI** (stabile); le organizzazioni utilizzano in media oltre 10 indicatori per valutare la legittimità delle operazioni.
- **Per autorizzare le operazioni Retail prevalgono Push notification (80%) e Passkey biometrica (66%)**; si registrano I primi casi di adozione del certificato digitale su smart card.

5 ATTACCHI RIVOLTI ALLA CONFIDENZIALITÀ, INTEGRITÀ E DISPONIBILITÀ DI DATI, INFORMAZIONI E SERVIZI

OBIETTIVO: fotografare trend, numerosità e incidenza delle tipologie di attacco che vedono come target ultimo i PSP italiani.

EVIDENZE CHIAVE

- **76 data breach rilevati (+27%);** il 31% delle organizzazioni rispondenti ha subito un breach diretto (era il 23%) e il 35% un breach indiretto da fornitori o supply chain.
- **Zero infezioni ransomware nel campione (era il 7%); attacchi DDoS gravi ridotti a 2 casi**, pur restando il 70% delle banche bersaglio di almeno un tentativo.
- **Il 56% delle organizzazioni ha integrato il rischio cyber geopolitico nei processi di risk assessment**; cloud provider (71%) e outsourcing IT (65%) sono le aree più vulnerabili nella supply chain.

Considerazioni finali

- **Le banche italiane confermano un quadro di investimenti solido e in crescita,** con priorità su resilienza operativa digitale (87%), antifrode (84%) e identity security (81%). L'awareness su personale, clientela e fornitori ICT diventa una componente strutturale della strategia di sicurezza.
- **La manipolazione del pagatore è ormai la cifra delle frodi che vanno a buon fine:** sia nel Retail sia nel Corporate la transazione anomala viene disposta direttamente dal cliente legittimo e il 96% è autorizzato con SCA regolarmente completata. Pur con una certa varietà di tecniche, è sempre la fiducia della vittima a essere sfruttata.
- **Cambiano i vettori di innesco:** cala progressivamente l'abuso dei canali telefonici in favore di outsider quali social media e instant messaging app. I falsi investimenti diventano la leva di social engineering più efficace (36%), seguiti dai task scam (25%).
- **La cooperazione tra PSP produce risultati misurabili:** aumenta ancora l'importo delle frodi "recuperate" (+50%). Restano però aree di vulnerabilità nei bonifici istantanei nazionali (~50% delle frodi effettive Retail) e nei flussi transfrontalieri, nell'ambito dei quali Malta diventa la nuova destinazione preferita dei frodatori.
- **Le minacce "classiche" perdono peso, ma cresce il rischio indiretto:** ransomware sostanzialmente assente, DDoS gravi ridotti a 2 casi ma data breach ancora in aumento con il 35% degli istituti colpito indirettamente attraverso proprie terze parti.

CERTFin

Thank you!

ricerca@certfin.it