CERTFin

# Report Sicurezza e Frodi in Banca

## KEY RESULTS

Maggio 2025


Gli Analisti CERTFin di riferimento:

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

# La sfida del contrasto al Cyber Crime

CERTFin

**Frodi bancarie 2025: il crimine è sempre più umano**

Nel panorama della sicurezza bancaria, c'è un fatto che non possiamo ignorare: il punto d'ingresso preferito dai frodatori non è un bug ma una persona.

Più di frequente, le frodi non si realizzano più "bucando" i sistemi ma convincendo il cliente a fare da solo.

Il phishing si è evoluto in arte persuasiva, i bonifici istantanei sono diventati l'arma perfetta e il social engineering è ormai la strategia dominante.

Anche l'AI entra in gioco, ma come alleato dei sistemi esistenti, non come sostituto.

Mentre calano minacce classiche come DDoS e ransomware, cresce un nuovo fronte: i data breach indiretti che colpiscono dalla filiera.

Le banche italiane reagiscono con forza: investimenti in crescita, tecnologie solide, modelli antifrode sempre più raffinati. Ma il salto di qualità passa dalle persone: awareness e collaborazione sono le nuove difese contro un crimine che fa leva su fiducia (mal riposta), velocità e disinformazione. La difesa si basa su più formazione e più cooperazione, perché oggi il rischio non è solo informatico ma umano, emotivo, relazionale.

E il settore risponde con lucidità, visione e unità.

# 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 destinato da ogni banca alla sicurezza IT**, rispetto al totale delle spese generali sostenute per l'IT, **si è attestata al 7%**.
- **Di tale budget, la quota destinata a interventi per la prevenzione e il contrasto delle frodi corrisponde al 12%.**
- **Il 77% delle banche rispondenti prevede un aumento degli investimenti sui servizi rivolti alla clientela** (su una scala di valori che va da aumento lieve ad aumento rilevante).
- **La formazione** rivolta al personale di filiale e ai contact center si focalizza in particolare **sul riconoscimento precoce delle frodi online e sulla sicurezza dei dispositivi**.
- **Il 62% delle banche rispondenti dichiara di aver utilizzato il materiale sviluppato dal CERTFin per iniziative di awareness**, sia in ambito Retail sia in ambito Corporate.

# 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**: 7,5 mld. Retail, 550 mln. Corporate.
- **Controvalore dei tentativi di frode**: circa 500 mln. €
  Il controvalore delle frodi recuperate nel 2024 ammonta a 22 mln di euro. Dall'introduzione del protocollo di collaborazione, il totale dei fondi recuperati attraverso la sola collaborazione tra PSP italiani supera i 100 milioni di euro.
- **Il 68% delle transazioni fraudolente** che vanno a buon fine (su clientela retail) avviene trasferendo il denaro **attraverso un bonifico istantaneo**.
- Ogni 100 transazioni anomale **21 diventano frodi effettive** (analisi su segmenti retail e corporate aggregati).
- La **Lituania** si conferma, in modo plebiscitario, il paese verso cui i frodatori preferiscono trasferire il denaro sottratto ai clienti italiani vittime di frode.

# 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**

- Quasi il **60% delle frodi effettive** è stato realizzato sfruttando come punto di contatto iniziale le **chiamate telefoniche e/o gli SMS** (lo scorso anno il dato era l'87,5%).
- Tra i vettori iniziali di frode, **social media** e **instant message app**, rispettivamente con il 20% e 14%, rappresentano un trend emergente.
- Su 100 transazioni fraudolente effettive, **99 avvengono assolvendo correttamente la SCA** (Strong Customer Authentication).
- **L'86% delle frodi è associato a casi di manipolazione** operati dal frodatore a danno del pagatore allo scopo di indurlo a emettere un ordine di pagamento.
- Le transazioni fraudolente effettive operate direttamente dal cliente legittimo sono circa **l'82% del totale**.

# Le Aree di Rilevazione

CERTFin

## 4 MECCANISMI DI RILEVAZIONE

**OBIETTIVO**: monitoraggio e valutazione critica degli strumenti utilizzati dai PSP per identificare le operazioni fraudolente, sia in *prevention* sia in *detection*.

**EVIDENZE CHIAVE**

- Il *transaction monitoring* interno rappresenta la **prima fonte di segnalazione** di operazioni sospette sia per la clientela Retail sia per la clientela Corporate.
- il **27%** delle soluzioni impiegate per il monitoraggio e la rilevazione degli attacchi rivolti alla clientela **è basato su tecnologie di AI**.
- Per autorizzare le operazioni da parte della clientela Retail, ai primi posti degli strumenti utilizzati dai PSP si confermano la **Push Notification** (81%) e **l'OTP tramite SMS** (62%).

## 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**

- Il **35%** dei PSP dichiara di aver rilevato almeno un **data breach indiretto** (per es., compromissione fornitore terzo o supply chain). In totale sono **60 i casi di data breach** rilevati (**+22%** rispetto al 2023).
- **Attacchi DDoS andati a buon fine: 286** (-83%) di cui solo 6 classificati come gravi.
- Solo il 7% delle banche ha subito **infezioni ransomware**, tutte con basso impatto.

# Considerazioni finali

CERTFin

- Le banche italiane confermano importanti volumi di investimenti nella sicurezza in generale e nel contrasto delle frodi in particolare. Preso atto degli attuali pattern utilizzati dai criminali, **le attività di awareness ricoprono sempre più un ruolo fondamentale**, tanto verso i dipendenti quanto verso i clienti.
- **L'SCT Instant si conferma il mezzo preferito dai frodatori**, i quali lo sfruttano ampiamente per trasferire denaro in modo illegittimo. I PSP stanno collaborando attivamente per definire nuove regole e approcci per mitigare il fenomeno.
- Le frodi, oggigiorno, accadono non perché i sistemi non riescono a intercettare le anomalie ma perché **è il cliente stesso a collaborare** (inconsapevolmente) alla riuscita della frode (le transazioni fraudolente effettive operate direttamente dal cliente legittimo sono l'82% del totale).
- **L'AI si integra (e non la sostituisce) con la componente core degli attuali sistemi antifrode**, basata principalmente su alberi decisionali capillari che si rivelano estremamente precisi e che, anche negli ultimi anni, attraverso indicatori come fraud rate, numero falsi positivi e numero falsi negativi, hanno confermato le proprie eccellenti capacità di intercettare transazioni anomale.
- Attacchi DDoS e ransomware sono in calo e al momento non rappresentano minacce particolarmente insidiose per le banche italiane. Preoccupa invece la **crescita dei data breach indiretti**, avvenuti cioè attraverso una compromissione di un fornitore.

CERTFin

ricerca@certfin.it