

Phishing e valore probatorio dei log informatici: il punto della Corte d'Appello di Milano

LUGLIO 2026

NUMERO 3/2026 – 56 SG

Le frodi informatiche, e in particolare il *phishing*, continuano a occupare una posizione centrale nel contenzioso bancario. Come noto, in base alla disciplina di derivazione PSD2 (D. Lgs. 11/2010 e successive modifiche) l'allocazione della responsabilità in caso di svuotamento del conto a seguito di truffe "online" si gioca sulla possibilità della banca di fornire la prova, oltre che della colpa grave del Cliente, del fatto che l'operazione contestata sia stata disposta nel rispetto dei **protocolli di c.d. autenticazione forte**, e dunque con il contestuale impiego di credenziali riferibili a due tra le categorie del possesso (la disponibilità di un dispositivo o di una carta), inerenza (es. il riconoscimento biometrico) e conoscenza (codici e password).

Sotto questo secondo profilo, assumono dunque indubbia rilevanza le evidenze offerte dalla Banca, in genere rappresentate da estrazioni dei propri sistemi informativi (c.d. **log informatici**), che registrano, in modo automatico, tutte le operazioni effettuate attraverso i sistemi bancari (accessi, autenticazioni, disposizioni di bonifico, utilizzo dei codici), consentendo di ricostruire ex post la sequenza degli eventi che hanno dato luogo alla realizzazione della frode ai danni del correntista.

Proprio sul valore probatorio delle **prove tecniche prodotte dalla banca** si è soffermata di recente la **Corte d'Appello di Milano**, con la **sentenza n. 696 del 13 marzo 2026**.

Nel caso di specie, nel valutare i presupposti della responsabilità dell'intermediario a fronte di operazioni di *home banking* ritenute fraudolente dal cliente, la Corte milanese chiarisce che non vi sono ragioni per dubitare, in via preventiva, dell'attendibilità e dell'utilizzabilità di tali registrazioni, trattandosi di dati generati in modo automatico dai sistemi informatici dell'istituto. I log, dunque, possono essere legittimamente prodotti in giudizio dalla banca per assolvere al proprio onere probatorio.

In tale contesto, la Corte perviene a qualificare i log come **riproduzioni informatiche ai sensi dell'art. 2712 c.c.**, precisando che, in assenza di una **specificata contestazione**, essi sono pienamente utilizzabili come prova delle effettive modalità di disposizione dell'operazione contestata.

La sentenza si sofferma anche sul profilo più generale dei parametri di valutazione della responsabilità della banca, adottando una posizione che rifugge da soluzioni automatiche. Pur riconoscendo l'elevato standard di diligenza richiesto agli intermediari, la Corte giunge infatti espressamente ad escludere che le banche debbano rispondere in via oggettiva di ogni truffa subita dalla clientela, evidenziando come

l'attuale contesto dei servizi di pagamento imponga anche agli utenti un **minimo dovere di attenzione e di autoresponsabilità**. Ritenere che ogni operazione disconosciuta dal cliente – seppur effettuata mediante l'uso dei suoi codici personali – debba essere automaticamente rimborsata dalla banca, significherebbe adottare una soluzione definita dalla Corte come “**manifestamente irrazionale**”, in contrasto con i principi che regolano la distribuzione dei rischi nei servizi di pagamento.

La decisione si inserisce in un filone giurisprudenziale che tenta di mantenere un equilibrio delicato: da un lato, la tutela del cliente vittima di frodi; dall'altro, il riconoscimento che la sicurezza dei sistemi di *home banking* passa anche attraverso un comportamento consapevole dell'utente, improntato al canone di ordinaria diligenza del cliente accorto.

Si tratta di principi tutt'altro che scontati in un panorama normativo e giurisprudenziale quale quello attuale, dove le – pur condivisibili – istanze di protezione del contraente “debole” si traducono talvolta in un'oggettivizzazione della responsabilità degli operatori bancari, ai quali viene ascrivita una funzione di tutela che travalica il mero rispetto degli obblighi informativi e la diligenza professionale per giungere alla salvaguardia del Cliente inadempiente o, addirittura, manifestamente negligente: si pensi alla tolleranza prima di avviare azioni esecutive nei confronti dei consumatori introdotta nel Testo Unico Bancario dall'attuazione della direttiva CCD2, o ad alcune pronunce in materia di *investment scam* (distrazione di fondi sul presupposto di improbabili schemi di investimento proposti dai malfattori) nei quali si porrebbe a carico degli intermediari l'onere di sorvegliare la complessiva operatività – pur consapevolmente e volontariamente disposta dal Cliente e di avvertirlo del pericolo di frode.

Anche in ragione di queste istanze, oltre che delle tempistiche ridotte imposte dal contenzioso, la tenuta della difesa giudiziale degli operatori risulta strettamente condizionata a rigorose policy di conservazione e reperimento delle evidenze, da strutturarsi con il necessario dialogo legali esterni.

Del resto, meglio prevenire ...

Linda Varanzano