

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(MI) RIZZO	Membro designato dalla Banca d'Italia
(MI) SANTARELLI	Membro di designazione rappresentativa degli intermediari
(MI) CESARE	Membro di designazione rappresentativa dei clienti

Relatore (MI) CESARE

Seduta del 10/03/2026

FATTO

Il cliente afferma di aver ricevuto in data 10 aprile 2025 una telefonata proveniente dal numero riferibile all'assistenza clienti della banca, nel corso della quale il presunto operatore la informava di tentativi di accesso al conto e la invitava a reinstallare l'app ufficiale, comunicandole contestualmente, via SMS dallo stesso numero, i codici necessari all'operazione. Contattava la banca per segnalare l'accaduto senza ricevere riscontro. In data 14 aprile 2025 veniva nuovamente contattata dallo stesso soggetto, il quale le comunicava che erano in corso operazioni sospette e che per bloccarle era necessario inserire ulteriori codici trasmessi via SMS; in tale contesto veniva eseguito un bonifico istantaneo di € 9.050,00 a favore di persona a lei sconosciuta, pari all'intera disponibilità del conto corrente, e veniva contestualmente richiesto a suo nome un prestito di € 6.500,00. Afferma di non aver mai rilasciato a terzi alcun codice di autenticazione personale, di aver operato sull'app ufficiale e di essere stata vittima di un attacco di ID caller spoofing di particolare sofisticatezza. Lamenta altresì che la banca non abbia previsto adeguate misure di sicurezza e abbia violato le disposizioni di cui al D.lgs. n. 11/2010 in materia di SCA. Chiede il rimborso di € 9.050,00, oltre interessi dalla domanda al saldo e le spese del procedimento.

Nelle controdeduzioni l'intermediario afferma che in data 10 aprile 2025 la cliente, comunicando i propri codici personali al truffatore, ha consentito l'attivazione dell'app su uno smartphone Samsung SM-A165F, successivamente utilizzato per eseguire l'operazione contestata; che l'enrollment è avvenuto nel pieno rispetto della SCA, mediante PIN quale elemento di conoscenza e codice OTP inviato al

recapito telefonico della cliente quale elemento di possesso; che il bonifico del 14 aprile 2025 è stato parimenti autenticato tramite smartcode e mobile token app nel rispetto della SCA; che la cooperazione attiva della cliente ha consentito la consumazione della truffa, integrandone la colpa grave; che la banca adotta un sistema di autenticazione forte nel pieno rispetto delle previsioni normative e non può ritenersi responsabile della manipolazione del numero chiamante da parte di terzi; che la cliente non ha prodotto evidenza della chiamata ricevuta, ha ignorato l'alert via e-mail inviatole e non ha utilizzato la funzione in app di verifica della chiamata messa a disposizione dall'intermediario. Chiede pertanto il rigetto del ricorso.

DIRITTO

La controversia riguarda un bonifico istantaneo di € 9.050,00 eseguito in data 14 aprile 2025, disconosciuto dalla ricorrente e riconducibile a un attacco di smishing misto a ID caller spoofing, nel corso del quale la cliente avrebbe comunicato al truffatore i codici di autenticazione necessari all'enrollment dell'app su un dispositivo di terzi.

Ai sensi dell'art. 10, D.lgs. n. 11/2010, il prestatore di servizi di pagamento è tenuto a fornire la prova dell'autenticazione e della regolare esecuzione dell'operazione, nonché a indicare gli elementi di fatto dai quali possa trarsi in via presuntiva la colpa grave dell'utilizzatore (Collegio di Coordinamento, decisione n. 22745/2019). Nel caso di specie, i log prodotti dall'intermediario documentano che l'enrollment dell'app sul dispositivo Samsung SM-A165F del 10 aprile 2025 è avvenuto mediante inserimento del PIN e del codice OTP inviato al numero di telefono della cliente, e che il bonifico del 14 aprile 2025 è stato autenticato tramite smartcode e mobile token app sul medesimo dispositivo, con SCA formalmente rispettata in entrambe le fasi. La prova di autenticazione deve ritenersi raggiunta.

Quanto alla **colpa grave** della ricorrente, la ricostruzione dei fatti — confermata dalla denuncia depositata agli atti — evidenzia che la cliente ha inserito o comunicato al truffatore il codice OTP ricevuto sul proprio cellulare durante la telefonata del 10 aprile 2025, consentendo così l'enrollment dell'app su un dispositivo a lei non riconducibile. È di comune conoscenza che le chiamate e i messaggi possono apparire come provenienti da un mittente attendibile attraverso tecniche di spoofing del numero chiamante, e tale consapevolezza è ormai diffusa tra il pubblico degli utenti bancari (Collegio di Milano, decisione n. 233/2025). La cliente, inoltre, non ha prodotto evidenza della chiamata ricevuta, non ha utilizzato la funzione di verifica della chiamata messa a disposizione dall'intermediario — la cui esistenza avrebbe consentito di sventare la frode — e ha ignorato gli alert di attivazione dell'app e di esecuzione del bonifico inviati dalla banca via e-mail e via SMS al suo recapito, come risulta dalla stessa denuncia agli atti (Collegio di Napoli, decisione n. 11053/2025; Collegio di Bari, decisione n. 9133/2025). La comunicazione dei codici OTP al truffatore costituisce condotta gravemente negligente, in quanto ha fornito il contributo causale determinante per la consumazione della frode, indipendentemente dalla sofisticatezza della tecnica impiegata.

Alla luce delle considerazioni che precedono, il ricorso non può trovare accoglimento.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE