

## COLLEGIO DI ROMA

composto dai signori:

|                |                                                           |
|----------------|-----------------------------------------------------------|
| (RM) SIRENA    | Presidente                                                |
| (RM) MARINARO  | Membro designato dalla Banca d'Italia                     |
| (RM) MAIMERI   | Membro designato dalla Banca d'Italia                     |
| (RM) CARATELLI | Membro di designazione rappresentativa degli intermediari |
| (RM) ONZA      | Membro di designazione rappresentativa dei clienti        |

Relatore MAURIZIO ONZA

Seduta del 24/02/2026

### FATTO

Con ricorso presentato il 1° agosto 2025, la ricorrente A. F di A. F e c. s.a.s., in persona della legale rappresentante *pro tempore*, (la "Ricorrente") ha domandato nei confronti della resistente (la "Resistente" e, assieme alla Ricorrente, le "Parti") il rimborso di Euro 928,00, in relazione a tre operazioni *on-line* effettuate con un carta di credito emessa dalla Resistente, che sarebbero state compiute all'esito di una frode commessa tramite *vishing* (e asserito *id spoofing*) in danno della Ricorrente.

Più nel dettaglio, la Ricorrente ha basato la propria domanda sul verbale di ricezione della denuncia e sul modulo di disconoscimento prodotti in atti, dai quali è emerso che la rappresentante legale della Ricorrente fosse titolare di una carta di debito emessa dalla Resistente.

Il 28 luglio 2025, intorno alle ore 17:55, la legale rappresentante della Ricorrente avrebbe ricevuto una chiamata telefonica proveniente dall'utenza \*\*\*317. Nel corso della conversazione, un sedicente operatore dell'ufficio antifrode della Resistente avrebbe segnalato l'esecuzione di alcuni movimenti insoliti che sarebbero stati effettuati a valere sulla citata carta di debito. Indotta in errore dalla messa in scena del truffatore, la legale rappresentante della Ricorrente avrebbe seguito le istruzioni impartite, autorizzando le operazioni proposte, nella ferma ma errata convinzione di procedere al relativo storno dei pagamenti sospetti.

Nonostante l'operatore avesse rassicurato la Ricorrente circa l'avvenuto blocco della carta, l'indomani, a seguito di un controllo diretto del rapporto di conto corrente, essa si sarebbe avveduta dell'effettiva esecuzione di tre operazioni per il complessivo importo di Euro 928,00. Essendo tali transazioni frutto di un'attività fraudolenta e non di una reale volontà negoziale, la Ricorrente ha chiesto dunque la condanna della Resistente alla restituzione della predetta somma.

La Resistente si è costituita in questo procedimento mediante il deposito di controdeduzioni, contestando integralmente le pretese della Ricorrente e domandando il rigetto della sua domanda.

In via preliminare, l'intermediario ha precisato che, a seguito di una procedura di *chargeback*, la Resistente avrebbe già ottenuto lo storno di una transazione pari a Euro 72,50; pertanto, tale importo è stato già rimborsato e deve essere scomputato dal totale originariamente richiesto.

Nel merito, la difesa della Ricorrente ha evidenziato che la carta di debito oggetto della truffa sarebbe stata bloccata solo il 30 luglio 2025, alle ore 14:37, ovvero due giorni dopo l'esecuzione delle operazioni contestate. La Resistente ha sottolineato come la Ricorrente abbia regolarmente ricevuto gli *alert* relativi alle transazioni effettuate, oltre che ai tentativi non andati a buon fine, sul numero telefonico indicato in sede di attivazione del servizio. Secondo la tesi della Resistente, la stessa Ricorrente avrebbe ammesso in sede di denuncia di aver autorizzato personalmente le operazioni, seppur nell'errata convinzione di stornarle, rendendo così inapplicabile la disciplina relativa alle disposizioni non autorizzate (si sarebbe realizzato, nella sostanza, il fenomeno della c.d. operazione sotto dettatura).

A supporto della propria posizione, l'intermediario ha prodotto i *log* di sistema, ritenuti idonei a comprovare la corretta autenticazione delle operazioni. Da tali evidenze è desunto che la frode non avrebbe comportato alcuna clonazione o sottrazione di credenziali, né l'associazione della carta su un dispositivo terzo. Al contrario, risulterebbe che il 28 luglio 2025, sul dispositivo della Ricorrente — sul quale l'app della Resistente era installata e utilizzata come canale di autenticazione forte (SCA) sin dal 7 giugno 2023 — sarebbero giunte le notifiche *push* per l'autorizzazione delle transazioni *on-line*, successivamente convalidate dalla Ricorrente stessa tramite fattore biometrico.

La Resistente ha dunque eccepito la colpa grave della Ricorrente per aver eseguito pedissequamente le istruzioni di un soggetto sconosciuto tramite una telefonata proveniente da un numero non riconducibile all'istituto. Inoltre, la Resistente ha rilevato che la Ricorrente, in quanto impresa commerciale ed esperta nell'uso dello strumento digitale da oltre due anni, avrebbe dovuto facilmente avvedersi della non originalità dei messaggi ricevuti, i quali presentavano errori nel contenuto e si svolgevano su una *chat* diversa da quella genuina. Infine, la Resistente ha escluso la presenza di anomalie o indici di rischio ai sensi del DM 112/2007, atteso che le transazioni non avrebbero esaurito il *plafond* disponibile.

Le Parti si sono ritualmente scambiate repliche e controrepliche.

Nelle proprie repliche, la Ricorrente ha insistito nella propria domanda, al netto degli importi rimborsati, ed ha chiarito, da un lato, che il rimborso di una delle operazioni in discorso implicherebbe il riconoscimento della natura fraudolenta di ciascuna di esse e, dall'altro, che, nelle operazioni sotto dettatura, mancherebbe il consenso consapevole dell'utente previsto dall'art. 10 d.lgs. 11/2010 ai fini dell'autenticazione e dell'esecuzione delle operazioni di pagamento.

Per parte propria, la Resistente ha richiamato le argomentazioni già rese con le proprie controdeduzioni.

## DIRITTO

Venendo alle ragioni della decisione, occorre procedere per gradi.

È bene perimetrare anzitutto l'oggetto del giudizio. Sul punto, si ritiene pacifico tra le Parti che l'oggetto della pretesa della Ricorrente sia ormai ridotto a Euro 855,50, per via dello storno operato dalla Resistente di Euro 72,50.

Tanto premesso, occorre anzitutto verificare se l'operazione materialmente compiuta dalla Ricorrente possa considerarsi, alla stregua della disciplina primaria e secondaria vigente, da questa effettivamente autorizzata.

Merita anzitutto evidenziarsi come dall'*app* bancaria della Ricorrente sia stato effettivamente seguito il percorso autorizzativo tramite notifiche *push*. Parimenti, è pacifico che la Ricorrente abbia eseguito le istruzioni ricevute dall'utenza privata \*\*\*317 del truffatore, essendosi convinta della loro genuinità. Utenza, questa, che non risulta in alcun modo riconducibile alla Resistente, ma neppure alla banca di radicamento del conto corrente.

Orbene, in casi simili questo stesso Collegio ha ritenuto che le condotte del cliente truffato integrassero gli estremi della colpa grave, essendosi prestato a richieste evidentemente anomale e rivelando a terzi

ignoti e non adeguatamente identificati credenziali e dati riservati. A titolo di esempio, è stato affermato che *«la ricostruzione dei fatti è tale da far emergere che parte attrice sia verosimilmente rimasta vittima di phishing telefonico (o vishing). Tuttavia, il carattere anomalo delle richieste avanzate avrebbe dovuto indurre la proponente a non seguire le indicazioni del falso operatore, rivelando a terzi ignoti i propri codici dispositivi. Ne deriva questo Arbitro, nel caso in esame, un contegno gravemente colposo della cliente nel proteggere le credenziali di sicurezza personalizzate (cfr., tra le altre, Collegio di Roma, decisione n. 12091/2021)»* (Collegio di Roma, decisione n. 6036/2022).

Indice di particolare rilievo in casi come quello di specie è quello dell'invio del messaggio-esca su di una *chat* o comunque in una sequenza di messaggi completamente estranea alla posizione dell'intermediario (cfr. Collegio di Roma, decisione n. 9667/2023, segnalando come tale circostanza evidenzi la grave negligenza della condotta del truffato).

Tutto quanto sopra è stato ammesso dalla Ricorrente, che dunque ammette di aver, sostanzialmente, causato il proprio danno con condotte gravemente colpose, per via della mancata adozione di minime regole di cautela.

A ciò va aggiunto che nella dinamica descritta dalle Parti e dai documenti in atti non risultino particolari vizi di autenticazione delle operazioni contestate. L'*app* della Ricorrente è sempre rimasta associata al medesimo dispositivo (dunque, soltanto i soggetti originariamente autorizzati hanno potuto operare tramite di essa) e su di essa è stata compiuta ciascuna fase della procedura autorizzativa delle operazioni.

Ne sono prova conclusiva i *log* depositati dalla Resistente, che permettono di ritenere rispettati tanto i fattori di possesso (tramite le notifiche *push*) quanto quelli di inerenza (tramite la biometria).

L'operazione risulta dunque debitamente autorizzata e autenticata, alcunché essendo imputabile alla Resistente nella truffa malauguratamente subita dalla Ricorrente.

### **PER QUESTI MOTIVI**

**Il Collegio respinge il ricorso.**

IL PRESIDENTE