

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) MASTROROSA	Membro di designazione rappresentativa dei clienti

Relatore MARCO MARINARO

Seduta del 14/01/2026

FATTO

Il ricorrente espone quanto segue:

- in data 20.01.2025, alle ore 19:00, riceveva una telefonata da un'utenza riconducibile al numero dell'intermediario così come memorizzato sul proprio device;
- nel corso dell'interlocuzione telefonica un sedicente operatore della banca lo informava dell'esecuzione di alcune operazioni "sospette" effettuate a valere sul conto di sua titolarità che andavano "immediatamente bloccate";
- il ricorrente, non potendo effettuare ulteriori verifiche trovandosi in auto, riponeva affidamento circa la genuinità delle richieste in quanto l'operatore si mostrava a conoscenza dei suoi dati;
- forniva, quindi, "i Token per effettuare le operazioni, ma...non gli altri dati per poter accedere, dalla app, alle operazioni dispositive";
- nel giro di dieci minuti venivano effettuati n. 3 bonifici istantanei ed un giroconto;
- successivamente, pervenivano messaggi con cui la banca lo informava di aver negato ulteriori operazioni di bonifico a favore di soggetti sconosciuti;
- non appena rientrato in albergo, il ricorrente si avvedeva della truffa subita e allertava la banca chiedendo il richiamo dei bonifici;
- la convenuta disponeva un parziale rimborso "conciliativo" per euro 4.933,00;
- il ricorrente aggiunge che, nei giorni precedenti alla truffa, aveva ricevuto ulteriori messaggi di allerta cui però non aveva dato peso in quanto provenienti da un numero sconosciuto.

Tanto ricostruito, rileva che:

- in sede di riscontro al reclamo, l'intermediario non ha dimostrato di aver agito con la diligenza qualificata richiesta dall'art. 1176, comma 2, cc, attraverso l'adozione delle misure di sicurezza idonee a prevenire il rischio di eventuali frodi;
- le operazioni sono avvenute "in orario di chiusura uffici", non potendo il ricorrente effettuare alcuna chiamata di "soccorso" pur nutrendo dei dubbi sulla genuinità della chiamata ricevuta;
- un sistema di sicurezza "forte" dovrebbe prevedere un presidio per evitare problemi legati alla modifica del numero chiamante;
- solo dopo la truffa, ovvero il 5 febbraio 2025, il ricorrente ha ricevuto una mail informativa rispetto alle frodi effettuate a mezzo telefonate;
- la fattispecie appare riconducibile al caller id spoofing;
- il ricorrente ha concorso ad effettuare le operazioni, ma il sistema era stato già abbondantemente violato posto che i dati personali erano già in possesso del truffatore.

Conclude chiedendo il rimborso del totale delle operazioni che, al netto della somma già riconosciuta "in acconto" dall'intermediario, risulta pari ad euro 9.867,00.

Il ricorso è stato inviato all'intermediario con nota prot. n. 1546494/25 del 4.8.2025, correttamente ricevuta.

Nonostante la rituale comunicazione del ricorso l'intermediario non ha presentato controdeduzioni.

In sede di interlocuzione preliminare al ricorso (e segnatamente nel riscontro del 05.03.2025) l'intermediario riferiva che:

- le operazioni in contestazione risultano autorizzate dal device del Cliente che, dando credito ad un contatto telefonico ricevuto da parte di un frodatore, ha pedissequamente seguito le istruzioni fornitegli fino ad autorizzare lui stesso le operazioni;
- senza la collaborazione del Cliente la frode non sarebbe stata possibile;
- le operazioni sono state correttamente autorizzate tramite c.d. autenticazione forte "a due fattori". Invero, con il mobile Token le operazioni possono essere autorizzate tramite inserimento dello smartcode o, nel caso in cui il cliente abbia attivato le funzioni biometriche, tramite fingerprint o face ID;
- allorquando la banca esegue correttamente l'operazione di pagamento in conformità all'identificativo unico fornito, alcuna responsabilità può esserle attribuita ai sensi dell'art. 24 del D. Lgs. 11/2010;
- la truffa, peraltro, si è protratta per oltre mezz'ora, lasso di tempo nel quale il cliente -che riceveva le notifiche di alert- avrebbe potuto prendere contatti con i canali ufficiali della banca per sincerarsi di quanto stesse accadendo (specie alla luce degli evidenti sospetti dallo stesso riconosciuti apertamente in denuncia);
- al fine di sensibilizzare la propria clientela in merito al fenomeno del phishing e alle diverse forme con cui esso si manifesta, trasmette ormai da tempo comunicazioni periodiche che contengono messaggi educativi anti-phishing volti proprio ad allertare il cliente, affinché lo stesso non dia seguito a certe richieste;
- ravvisando profili di colpa grave rinvenibili nella condotta del cliente, la banca ritiene congruo l'indennizzo già effettuato a mero titolo conciliativo e respinge la richiesta di rimborso integrale avanzata.

DIRITTO

Le operazioni di pagamento online disconosciute dalla parte ricorrente sono state eseguite in data 20 gennaio 2025. Risultano pertanto effettuate dopo l'emanazione della direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015, (c.d. PSD 2 - Payment Services Directive 2), recepita con il d.lgs. n. 218 del 15.12.2017, entrato in vigore in data 13.01.2018, che modifica in più punti il d.lgs. n. 11 del 2010. Si rileva che tali operazioni sono altresì successive alla data di entrata in vigore del Regolamento Delegato (UE) n. 2018/389 della Commissione.

Sulla base di quanto previsto dalla direttiva (art. 115, par. 4), l'art. 5, comma 6, d.lgs. n. 218/2017 prevede tuttavia che "le misure di sicurezza di cui agli articoli 5-bis, commi 1, 2 e 3, 5-ter, 5-quater e 10-bis del decreto legislativo 27 gennaio 2010, n. 11, si applicano decorsi diciotto mesi dalla data di entrata in vigore delle norme tecniche di regolamentazione di cui all'articolo 98 della direttiva (UE) n. 2015/2366". In particolare, la Commissione – delegata ad adottare tali norme tecniche di regolamentazione, ai sensi dell'art. 98, par. 4, della direttiva – ha emanato il 27.11.2017 il regolamento delegato (UE) n. 2018/389 che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri. Il regolamento, ai sensi dell'art. 38, par. 2, si applica a decorrere dal 14.09.2019 e cioè diciotto mesi dopo la pubblicazione sulla Gazzetta Ufficiale dell'Unione Europea, avvenuta in data 13.03.2018. Ne consegue che anche le norme del d.lgs. n. 11/2010 riferite alle misure di sicurezza, così come modificate dal d.lgs. n. 218/2017, hanno efficacia a partire dal 14.09.2019.

Esse risultano dunque applicabili alla vicenda oggetto del ricorso in esame.

In estrema sintesi, la nuova normativa fa ricadere sull'intermediario la responsabilità delle operazioni disconosciute laddove quest'ultimo non abbia predisposto un c.d. "sistema di autenticazione forte" (in inglese *strong customer authentication* o SCA). Un simile sistema deve essere applicato, stando alla previsione dell'art. 10-bis, dai prestatori di servizi di pagamento anche quando l'utente dispone un'operazione di pagamento elettronico ovvero effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi. Quanto alla responsabilità del pagatore, ai sensi del comma 2-bis dell'art. 12 d.lgs. n. 11/2010, come inserito dal d.lgs. n. 218/2017, "salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente. Il beneficiario o il prestatore di servizi di pagamento del beneficiario rimborsano il danno finanziario causato al prestatore di servizi di pagamento del pagatore se non accettano l'autenticazione forte del cliente".

Orbene, il concetto di "autenticazione forte" trova la propria definizione all'art. 1, comma 1, lett. q-bis), d.lgs. n. 11/2010 (lettera introdotta dal d.lgs. n. 218/2017): "un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione".

Il concetto è oggi ribadito e precisato, specie per quanto concerne la conformità di singole fattispecie concrete alle suddette categorie dell'autenticazione forte, dall'*Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2* del 21 giugno 2019.

L'EBA ha chiarito, per esempio, che, mentre l'OTP ricevuta tramite sms integra un elemento di possesso idoneo ai fini della strong customer authentication, i dati riportati sulla carta (numero, scadenza e CVV), non costituiscono né un valido elemento di possesso (par. 28), né un valido elemento di conoscenza (par. 33). Al par. 43 di tale documento si legge, in particolare, che "*a number of existing approaches within e-commerce, for card payments in particular, would not be compliant with SCA. This includes approaches in which card details printed in full on the card are used as stand-alone elements or used in combination with a communication protocol such as EMV® 3-D Secure or with only one compliant SCA element (such as SMS OTP)*".

Alla luce di un simile orientamento, con riguardo alle operazioni successive al 14.09.2019, questo Collegio ritiene che l'inserimento dei dati della carta, al fine di dar corso alle operazioni di pagamento, non integri un idoneo fattore di autenticazione (così, per esempio, Collegio di Roma, decisione n. 8493/2020, decisione n. 15221/2021 e decisione n. 21761/2021).

Il ricorrente chiede il rimborso dell'importo che asserisce essergli stato fraudolentemente sottratto all'esito di truffa perpetrata ai suoi danni tramite la tecnica del vishing.

Disconosce, nello specifico, tre bonifici istantanei, disposti il 20.01.2025, dal conto corrente radicato presso la resistente in favore di un rapporto acceso presso un intermediario terzo.

L'importo complessivamente sottratto risultava pari ad euro 14.800,00.

È pacifico che l'intermediario abbia riconosciuto al ricorrente l'importo di euro 4.933,00 quale rimborso "conciliativo".

La pretesa è stata, quindi, rideterminata nel ricorso in euro 9.867,00 residui.

Il ricorrente riferisce che, in data 20.01.2025, alle ore 19:00, veniva contattato telefonicamente da un soggetto qualificatosi come operatore della banca che lo informava dell'esecuzione di alcune operazioni "sospette" effettuate a valere sul conto di sua titolarità che andavano "immediatamente bloccate".

Pur non potendo effettuare ulteriori verifiche trovandosi in auto, il ricorrente riponeva affidamento circa la genuinità delle richieste, sia perché la chiamata proveniva da un'utenza riconducibile al numero dell'intermediario così come memorizzato sul proprio device, sia perché l'operatore si mostrava a conoscenza dei suoi dati.

Nel seguire le istruzioni impartite, il ricorrente forniva "i Token per effettuare le operazioni, ma...non gli altri dati per poter accedere, dalla app, alle operazioni dispositive".

Produce evidenza della chiamata ricevuta nella quale compaiono l'id dell'intermediario nonché alcuni numeri allo stesso riferibili.

Si rammenta che il Collegio equipara la chiamata proveniente da un numero apparentemente riconducibile all'intermediario (vishing caller id) all'sms spoofing, ravvisando un concorso di colpa.

La ricostruzione fornita coincide con quanto dichiarato in sede di denuncia.

Tanto ricostruito, l'intermediario eccepiva - solo in sede di interlocuzione preliminare al ricorso - che le operazioni sarebbero state disposte dal device in possesso del cliente con autorizzazione delle stesse mediante sistema mobile Token.

Lo stesso ricorrente ammette di aver generato, a più riprese, dei codici Token su richiesta del frodatore nell'errata convinzione di bloccare le operazioni fraudolente.

Al riguardo si osserva che, secondo gli orientamenti condivisi dei Collegi territoriali, l'applicazione del regime di responsabilità per le operazioni disconosciute previsto dalla predetta normativa è esclusa solo quando l'operazione sia stata eseguita per intero dal pagatore (con inserimento della disposizione di pagamento e di tutti i fattori di autenticazione).

Diversamente se il concorso causale dell'utente in fase dispositiva e/o autorizzativa è parziale (ad es. con l'inserimento di uno dei fattori di autenticazione), la transazione non deve intendersi, per ciò solo, autorizzata.

Ad avviso del Collegio nel caso di specie ricorre la seconda ipotesi e cioè il parziale concorso del cliente nella fase autorizzativa della transazione non essendo emersa evidenza diversa.

Come anticipato l'intermediario non si è costituito per cui nulla è stato acquisito in ordine all'autenticazione delle operazioni.

Soltanto in sede di riscontro al reclamo riferiva che le operazioni risultavano autorizzate mediante sistema mobile Token (inserimento dello smartcode o, nel caso in cui il cliente abbia attivato le funzioni biometriche, tramite fingerprint o face ID) senza fornire ulteriori dettagli.

Secondo l'orientamento condiviso dai Collegi, in tali ipotesi, il ricorso deve essere accolto integralmente "posto che la mancanza anche parziale della prova di autenticazione è risolutiva e dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili al cliente. La prova di autenticazione rappresenta infatti, in aderenza al dato normativo, un prius logico rispetto alla prova della colpa grave dell'utente".

In adesione a tale principio, in caso di mancata produzione di elementi idonei a dimostrare l'avvenuta autenticazione, registrazione e contabilizzazione dell'operazione, i Collegi accolgono il ricorso, ai sensi dell'art. 10, primo comma, del d.lgs. 11/2010 (Collegio di Roma, decisione n. 26738/2019; Collegio di Roma, decisione n.6964/24).

Per quanto sopra esposto il ricorso è meritevole di accoglimento e l'intermediario è tenuto a rimborsare alla ricorrente l'importo pari alla somma delle operazioni contestate, detratti gli importi eventualmente già rimborsati.

PER QUESTI MOTIVI

Il Collegio, in accoglimento del ricorso, dispone che l'intermediario corrisponda alla parte ricorrente la somma di euro 9.867,00.

Dispone, inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di euro 200,00 (duecento/00) quale contributo alle spese della procedura e alla parte ricorrente quella di euro 20,00 (venti/00) quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE