

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MARINARO	Membro designato dalla Banca d'Italia
(RM) DEPLANO	Membro designato dalla Banca d'Italia
(RM) BILOTTI	Membro di designazione rappresentativa degli intermediari
(RM) NOTARO	Membro di designazione rappresentativa dei clienti

Relatore DANIELA CONCETTA NOTARO

Seduta del 06/03/2026

FATTO

Con ricorso del 10 settembre 2025 (preceduto da rituale reclamo, negativamente riscontrato dall'intermediario) l'istante si è rivolto a codesto Collegio rappresentando che in data 11/04/2025 alle ore 15.10 circa riceveva diversi sms, "in perfetta consecutio" rispetto a precedenti già ricevuti dal sistema, nel contesto dei quali si avvisava di proseguire la configurazione della App con la esatta specifica "se non hai chiesto tu il codice contattaci". Alle ore 15.13 chiamava il servizio clienti per avere conferma del fatto che fosse necessario proseguire con la configurazione richiesta, ricevendo risposta affermativa dall'operatore.

Tale conferma da parte dell'Istituto bancario e le riferite circostanze, determinavano la certezza della necessità di configurare l'APP.

In data 13/04/2025 riceveva altro sms "sempre in perfetta consecutio" rispetto a precedenti già ricevuti dal sistema, nel contesto del quale veniva informato di un riaccredito di €. 570,00 dalla carta prepagata.

Il giorno successivo – 14/04/2025 – il ricorrente chiamava sempre il numero del servizio clienti per chiedere chiarimenti in merito al comunicato riaccredito e contestualmente l'operatore lo informava di un ordine bonifico eseguito nella stessa giornata del 14/04/2025 di €. 12.000,00 per saldo fattura", oltre ad una serie di numerosi altri pagamenti di importi pari a €. 95,00 ed €. 1,99.

In pari data – 14/04/2025 – chiamava il numero verde per provvedere al blocco di tutte le operazioni.

In data 14 aprile 2024 l'istituto bancario riaccreditava la somma di 4.206,41 quale "conciliazione per frode".

Ciò premesso, specificava di non avere mai fatto richiesta e/o eseguito la operatività di tutte tali operazioni di pagamento.

Inoltre, mai nessun sms di conferma operazioni è mai pervenuto, contrariamente a quanto è sempre avvenuto per precedenti pagamenti realmente eseguiti.

Rilevava che il giorno stesso 14/04/2025 aveva immediatamente provveduto a richiedere il blocco delle operazioni.

Inoltre, l'importo di €. 12.000,00 era relativo ad un bonifico ordinario eseguito in data 14/04/2025 dal malfattore quale "*RISTRUTTURAZIONE EDILIZIA art. 16-bis del DPR 917 del 22/12/1986*" e come tale pienamente revocabile nella stessa giornata e/o comunque richiedibile alla banca beneficiaria.

In conclusione, ha richiesto all'ABF le informazioni esatte dell'orario dei pagamenti e/o operazioni nonché bonifici avvenuti on line, la copia delle disposizioni di bonifico, le modalità di verifica per la regolarità della operazione ed i log delle operazioni svolte dall'utente con specifica evidenza del dispositivo da cui sono state eseguite.

Nel costituirsi con apposite controdeduzioni, l'intermediario ha precisato che in considerazione del rimborso di euro 4.206,41 tutte le operazioni di bonifico del 13/04/2025 e del 14/04/2025 – fatta eccezione per la sola operazione di bonifico di euro 12.000 del 14/04/2025 - pari ad euro complessivi 619,23, risultano interamente coperte dalla citata corresponsione.

Nell'esaminare, quindi, esclusivamente l'operazione compiuta il 14.4.2025, ha rilevato dalla ricostruzione fattuale una chiaramente cooperazione colpevole tra il Cliente e il presunto truffatore.

Risulta, invero, che alle ore 15:18:44 dell'11/04/2025, sia stata installata l'APP, necessaria per l'autorizzazione di disposizioni su un altro dispositivo (nello specifico trattasi del device del frodatore: samsung SM-**55F) tramite inserimento dei dati personali del Cliente (Codice Cliente, Data di nascita, Codice PIN e successivo inserimento del codice OTP ricevuto sul numero di cellulare appartenente al Cliente).

Si tratta, invero, del medesimo recapito telefonico indicato dal Cliente all'interno del Modulo di disconoscimento presentato.

Orbene, tale circostanza è stata resa possibile solo grazie alla cooperazione dell'odierno ricorrente con il frodatore.

In termini generali, invero, l'installazione della nuova APP su device di altro soggetto avviene tramite Strong Customer Authentication attraverso l'Accesso tramite app sul nuovo dispositivo con l'inserimento del Codice Cliente, data di nascita e Codice PIN (elemento di conoscenza). Inoltre si procede all'invio sms OTP sul recapito telefonico registrato sull'anagrafica del Cliente (elemento di possesso) con il seguente testo: "*Per proseguire la configurazione della tua App, inserisci il codice XXXXXXXX. Se non hai richiesto tu il codice, contattaci*".

Infine, l'APP richiede l'inserimento dell'OTP ricevuto sul recapito telefonico posseduto dal Cliente.

Nel caso in esame, la modifica del dispositivo è avvenuta senza anomalie e nel rispetto della "Strong Customer Authentication" (c.d. SCA): in assenza della comunicazione delle credenziali, nonché del

codice OTP ricevuto sul recapito telefonico, l'accesso alla posizione del Cliente e l'esecuzione delle operazioni oggi sconosciute dal Ricorrente non avrebbero potuto essere eseguite.

Il Cliente – con la propria, colpevole, rivelazione al frodatore dei propri codici – ha consentito l'installazione della nuova APP sul device del frodatore, violando il dovere di tenere un comportamento idoneo a garantire la sicurezza del dispositivo ed il suo utilizzo (art. 7 comma 2 d.lgs. n. 11/2010).

In sede di repliche parte ricorrente ha rilevato che, come si evince dagli atti, il ricorrente ha ricevuto gli sms in data 11/04/2025 in perfetta consecutio rispetto a precedenti già ricevuti dal sistema, nel contesto dei quali si avvisava di proseguire la configurazione della App con la esatta specifica “ se non hai chiesto tu il codice contattaci.

Ha provveduto a chiamare in data 11/04/2025 alle h. 15.13 il numero verde dell'assistenza.

Ed è stato esattamente il personale della banca a confermare la genuinità dei messaggi e la necessità di provvedere alla disinstallazione dell'app per la sua configurazione: pertanto ha provveduto a disinstallare l'app dal suo cellulare per espressa indicazione del personale.

Tutto ciò che è accaduto è piena ed esclusiva responsabilità della banca, per grave vulnus del sistema; peraltro, i truffatori già dal giorno 11/04/2025 avevano posto in essere numerosi tentativi per accedere al sistema (così si evidenzia dai log), ma la banca non ha provveduto a porre in essere alcun atto di blocco per tutelare il ricorrente.

La stessa banca fornisce il lungo elenco delle operazioni fraudolente che sono partite dal giorno 13/04/2025 e proseguite nel giorno 14/04/2025 (lunedì).

Pertanto non si comprende come la banca a partire dal giorno 13/04/2025 (domenica) non abbia riscontrato l'anomalia dei ben 24 bonifici eseguiti esattamente dopo i numeratissimi tentativi posti in essere dal truffatore a partire dal giorno 11/04/2025.

Dopo il cambio utente sull'app con la piena insinuazione del frodatore con il proprio device e dopo il cambio di numero di telefono dal quale sono partite le operazioni, la banca non provvedeva diligentemente in quel lasso temporale a bloccare l'operatività del conto.

I log depositati dalla banca convenuta non sono affatto trasparenti né tantomeno comprensibili

Infatti dai “dati” che fornisce la banca (epurati chirurgicamente da altri precedenti eseguiti) non emerge la disinstallazione dell'app dal cellulare, il cambio contestuale dell'uso dell'app in un nuovo cellulare, il nuovo numero di telefono che utilizza l'app che non appartiene al ricorrente, l'ID utente ed il cambio IP utente del giorno 11/04/2025 che deve essere avvenuto alle h. 15.18 quando si è inserito il frodatore, dopo i suoi numerosissimi tentativi.

Il ricorrente non ha mai ricevuto nessun sms di conferma di bonifici eseguiti dai malfattori, né mai ha ricevuto alcuna notifica push di OTP (perché la banca per facilitare la operatività utilizza un solo codice fisso sia per accedere all'app e sia per dare l'ordine di pagamento).

Il ricorrente tra l'altro non ha mai attivato un secondo dispositivo.

Nonostante tutti tali elementi la banca ha provveduto a restituire solo € 4.206,41 quale “conciliazione per frode”.

Inoltre la banca non fornisce la dovuta specifica informazione circa il bonifico di €. 12.000,00 eseguito il giorno 14/04/2025 dal malfattore (cioè il giorno dopo rispetto agli altri 23 eseguiti il giorno precedente), non spiegando se si tratti o meno un bonifico ordinario.

L'istante, infine, reitera la doglianza circa il mancato richiamo del bonifico eseguito dal malfattore in data 14/04/2025.

Nel controreplicare, l'intermediario ha rappresentato che nell'ambito delle controdeduzioni presentate, la Banca ha chiaramente dimostrato la corretta autenticazione della sola operazione che non è stata già oggetto di rimborso nonché la colpa grave del Cliente nella vicenda in esame che ha permesso l'installazione della app sul dispositivo del frodatore.

Ha rilevato di avere già rimborsato 1/3 delle somme complessivamente oggetto di contestazione.

Inoltre, ha segnalato che 21 operazioni delle 24 contestate, sono state effettuate in data 13/04/2025, mentre solo le ultime 3 operazioni (euro 1,99 – euro 1,95 – euro 12.000) sono state effettuate in data 14/04/2025.

Nel palesare l'invio delle e-mail di alert inviate al cliente in data 13/04/2025, ha specificato che se il cliente avesse preso atto delle comunicazioni ricevute via mail e avesse provveduto a contattare tempestivamente la Banca, il rapporto sarebbe stato bloccato in data 13/04/2025 evitando l'esecuzione dei bonifici del 14/04/2025, tra cui quello di euro 12.000.

DIRITTO

L'utilizzo fraudolento per cui è controversia è disciplinato dal d.lgs. 27 gennaio 2010, n. 11, modificato a seguito dell'entrata in vigore (il 13/01/2018) del D.lgs. 15 dicembre 2017, n. 218, di recepimento della direttiva (UE) 2015/2366 (c.d. PSD2) relativa ai servizi di pagamento nel mercato interno, nonché adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta.

In tale ambito si rammenta che, secondo la posizione consolidata dell'ABF, la disciplina sopra citata prevede un regime probatorio di favore per l'utente di strumenti e servizi di pagamento, essendo *“ispirata al principio del “rischio d'impresa”, e cioè all'idea secondo la quale è razionale far gravare i rischi statisticamente prevedibili legati ad attività oggettivamente “pericolose”, che interessano un'ampia moltitudine di consumatori o utenti, sull'impresa, in quanto quest'ultima è in grado, attraverso la determinazione dei prezzi di vendita dei beni o di fornitura del servizio, di ribaltare sulla massa dei consumatori e degli utenti il costo dell'assicurazione di detti rischi”* (così Collegio di coordinamento, decisione n. 3498/2012).

In particolare, l'art. 10 del d.lgs. 11/2010 prevede, in merito all'onere della prova gravante sul prestatore dei servizi di pagamento (PSP), una precisa e graduata sequenza, in base alla quale il PSP è tenuto a dimostrare:

1. l'autenticazione, la corretta registrazione e contabilizzazione della o delle operazioni contestate e l'assenza di malfunzionamenti delle procedure necessarie per la sua esecuzione o di altri inconvenienti.

In particolare, secondo gli orientamenti condivisi dei Collegi, la prova di autenticazione rappresenta, in aderenza al dato normativo, l'antecedente logico rispetto alla prova della colpa grave (o dolo) dell'utente;

2. il comportamento gravemente colposo (o fraudolento o doloso) dell'utilizzatore (anche per presunzioni).

Nel merito si rileva che parte ricorrente rappresenta di aver disconosciuto 24 operazioni, 21 delle quali effettuate in data 13/04/2025 mentre le ultime 3 (tra cui il bonifico di euro 12.000,00 oggetto del presente ricorso) sono state effettuate in data 14/04/2025.

Il totale delle operazioni ammonta a 12.619,23 (619,23 +12.000,00).

E' pacifico che l'intermediario ha rimborsato l'importo di euro 4.206,41 corrispondente a 23 operazioni oltre che a una parte del bonifico di 12.000,00 euro in contestazione. Parte ricorrente specifica di chiedere la restituzione di €. 8.392,82 ma l'importo ammonterebbe a 8.412,82 euro (12.000,0 - 4.206,41).

In ordine all'autenticazione, l'intermediario rappresenta che le operazioni sono state eseguite tramite il device utilizzato dai frodatori dopo che gli stessi frodatori hanno installato la app con le credenziali fornite dal ricorrente.

In proposito, la resistente fornisce evidenza della installazione della app sul nuovo device avvenuta alle ore 15:18 dell'11 aprile 2025, dopo aver inserito codice cliente, PIN e OTP.

Durante la configurazione della app viene scelto lo smartcode e vengono configurati eventualmente i dati biometrici.

L'OTP risulta inviato sul cellulare del ricorrente indicato in denuncia.

Risulta inviata, altresì, una mail di alert all'indirizzo indicato nel modulo di disconoscimento.

In ordine alla esecuzione del bonifico l'intermediario riferisce che alle ore 00:18 del 14.04.2025 l'accesso prodromico al bonifico è stato autorizzato dalla APP (possesso) digitando il Codice Segreto (SmartCode – conoscenza) a seguito di notifica push.

Il bonifico è stato poi eseguito tramite inserimento dello stesso Smartcode (conoscenza) in app (possesso).

In ordine agli elementi rilevanti del fatto, il ricorrente afferma di aver ricevuto in data 10 e 11 aprile 2025 due sms in apparenza riferibili alla banca contenenti un link per aggiornare la app. Ammette di aver cliccato il link per eseguire l'aggiornamento ma nega di aver comunicato i codici necessari a eseguire le operazioni disconosciute.

Afferma di aver contattato il servizio clienti della banca prima di "aggiornare la app" e che un operatore gli avrebbe confermato la genuinità di tale operazione.

Rileva di essersi accorto della truffa il 14.04.2025 e di aver bloccato immediatamente il conto.

I messaggi, nello specifico, risultano inseriti in una chat riferibile all'intermediario contenente messaggi genuini e non presentano errori grammaticali.

Il link truffaldino presenta riferimenti alla banca e risultano anche presenti gli sms con i codici OTP per configurare la app.

La chiamata dell'11.04.2025 alle ore 15:13 che il ricorrente afferma di aver effettuato al servizio clienti per avere certezza della genuinità dei messaggi non consente di individuare il mittente.

Orbene, secondo la consolidata giurisprudenza di codesto Collegio, le intrusioni truffaldine tramite “*sms spoofed*” sono riconducibili alle frodi sofisticate.

Si tratta di ipotesi di *smishing* in cui il messaggio reca, quale mittente, la denominazione dell'intermediario, in modo tale che il testo si inserisca, nei moderni *smartphone*, all'interno della conversazione contenente messaggi genuini (effettivamente provenienti dall'intermediario). In tale contesto, quando il cliente è vittima di questo tipo di truffa non può essere in genere ravvisata una sua colpa grave, salvo che il messaggio civetta presenti indici di evidente inattendibilità o anomalia che dovrebbero allertare l'utente avveduto; in quest'ultimo caso può essere riconosciuto un concorso di colpa per l'utente a causa della sua grave negligenza che agevola la truffa.

Ed è evidente che il messaggio contenente il link – che possiede riferimenti all'intermediario - risulta inserito in una chat riferibile alla resistente e risulta alternato a messaggi genuini, non presentando oltretutto errori grammaticali.

Aggiungasi le operazioni complessivamente considerate (24 operazioni eseguite tra il 13 e il 14 aprile 2025) possono apparire anomale, anche in considerazione del fatto che i principi del D.M. 112/2007 non hanno un valore precettivo diretto in materia di disconoscimento di operazioni non autorizzate ma sono espressione di un generale obbligo di monitoraggio delle operazioni, da utilizzare per valutare la condotta dell'intermediario. E la stessa giurisprudenza della Suprema Corte (Cassazione civile, sezione I, 3.11.2023 n. 30588) ha chiarito che nonostante la banca non abbia alcun dovere generale di monitorare la regolarità delle operazioni ordinate dal cliente, nondimeno, in presenza di circostanze anomale idonee a ledere l'interesse del correntista, questa, in applicazione dei doveri di esecuzione del mandato secondo buona fede, deve rifiutare l'esecuzione o almeno informare il cliente (Cass. 31 marzo 2010, n. 7956). Tale obbligo di protezione si attiva alla ricorrenza cumulativa di due presupposti: che l'operazione sia *ictu oculi* anomala e che non risponda agli interessi del cliente.

Dalle considerazioni sopra riferite, deriva l'accoglimento del ricorso.

PER QUESTI MOTIVI

Il Collegio, in accoglimento del ricorso, dispone che l'intermediario corrisponda alla parte ricorrente la somma di euro 8.392,82.

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