

COLLEGIO DI ROMA

composto dai signori:

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

Relatore DANIELA CONCETTA NOTARO

Seduta del 16/12/2025

FATTO

Con ricorso del 23 giugno 2025 (preceduto da rituale reclamo, negativamente riscontrato dall'intermediario) l'istante ha rappresentato che il 16.4.2025 ha ricevuto una chiamata da un numero riconducibile al servizio clienti della banca.

Il sedicente operatore lo ha avvisato di un bonifico di € 490,00 dal suo conto e che, pertanto, era necessario provvedere al relativo blocco.

Nel corso della telefonata, il truffatore ha riferito che occorreva aggiornare l'app per ultimare l'operazione di blocco del bonifico, che, tuttavia, non andava a buon fine. Pertanto, si rendeva necessario attendere il giorno successivo.

La mattina seguente, il ricorrente insospettito anche per un malfunzionamento dell'applicazione, chiamava il servizio clienti della banca per chiedere informazioni circa l'aggiornamento del giorno precedente. A questo punto scopriva che erano state effettuate undici operazioni, tra bonifici istantanei e ricariche telefoniche, per un totale di € 6.079,00.

Il 6.5.2025 la banca procedeva al rimborso di quota parte dei 6.079,00 € truffaldinamente sottratti da suo conto, per un totale di € 2.143,33 corrispondenti alle cinque ricariche telefoniche (€ 500 totali) e all'importo di € 1.643,33 per le operazioni di bonifico bancario disconosciute.

Apprezzando la volontà della Banca di definire bonariamente la controversia, ritiene tuttavia che la somma rimborsata non rifletta il pregiudizio subito.

Infatti, a fronte della frode sofisticata subita e della insussistenza di qualsivoglia colpa grave, ha richiesto il rimborso anche della restante parte pari ad € 3.935,67.

Nel costituirsi con apposite controdeduzioni, l'intermediario ha rilevato che le operazioni disconosciute risultano essere state eseguite senza anomalia alcuna.

Nel merito, ha riferito che le operazioni disconosciute sono avvenute in due date differenti; pertanto, il cliente avrebbe potuto impedire il perfezionamento di tutte le transazioni contestate.

In dettaglio, nella giornata del 16 aprile 2025 risultano impartite esclusivamente le operazioni di bonifico, mentre nella giornata del 17 aprile risultano disposte le cinque operazioni di ricarica telefonica e la transazione con Carta di Debito n. *301 di importo pari ad € 690,00.

Tutte le transazioni risultano autenticate mediante la nuova App installata il 16 aprile 2025 alle ore 18:00:10 su di uno smartphone al quale vengono inviate tutte le PUSH.

Per poter procedere all'installazione della nuova APP sul device prescelto, il cliente, accede all'APP e inserisce i seguenti dati in due sessioni separate:

- Codice Cliente (codice composto da 7 cifre che viene assegnato dalla Banca al Cliente al momento della conclusione del Contratto) e data di nascita;
- Tre cifre del codice segreto P.I.N. (elemento di conoscenza);

In seguito al corretto inserimento, il cliente sceglie il proprio S*Code;

Per procedere con l'attivazione della nuova App è prevista l'autenticazione con OTP (One Time Password) che viene inviato al numero di telefono del cliente registrato all'interno dell'anagrafica dei sistemi della banca (elemento di possesso).

A riprova che il numero di cellulare su cui è giunto l'OTP autorizzativo fosse in possesso del cliente, l'intermediario segnala che la stessa utenza è indicata dal ricorrente anche nei moduli di contestazione. Di tale installazione alle 18:00:11 è stato inviato apposito alert mediante notifica a mezzo e-mail.

Dopo avere effettuato l'accesso all'area riservata del cliente secondo le modalità sopra descritte, sono state impartite le disposizioni relative alle operazioni di pagamento e si è proceduto alla relativa autorizzazione con doppio fattore.

Per ciascuna delle operazioni eseguite, al cliente è stata inviata apposita notifica di alert.

In ogni caso, i bonifici disconosciuti sono bonifici istantanei e non è possibile annullarli.

Riporta il testo della comunicazione e-mail inviata al cliente al fine di informarlo dell'introduzione del nuovo servizio di bonifici istantanei nonché evidenza del caricamento del documento all'interno dell'Area Riservata del sito internet della Banca.

Ravvisa colpa grave del cliente che ha cooperato con il truffatore.

Inoltre, il Cliente non sembra aver utilizzato l'App di verifica del numero implementata dalla Banca proprio a tutela dei propri clienti nella prevenzione delle frodi. Se avesse verificato il contatto ricevuto, il sistema avrebbe fornito feedback che il Cliente non era al telefono con un operatore.

Pertanto, ha chiesto il rigetto del ricorso, ritenendo più che soddisfacente la somma di euro 2.143,33 già liquidata ai fini conciliativi.

In sede di repliche, parte ricorrente insiste per l'accoglimento del ricorso, poiché ha subito una frode sofisticata attuata tramite vishing callerID.

Nega di aver fornito le credenziali al truffatore e l'onere di fornire prova del dolo o della colpa grave incombe sull'intermediario (che deve altresì sopportare il rischio di impresa).

Ravvisa responsabilità della banca poiché non ha inviato nessun avviso in tempo utile relativo all'accesso da un dispositivo non autorizzato e comunque diverso da quelli usuali.

Nessuna segnalazione perveniva attraverso messaggi di alert di quanto stesse accadendo.

In tale contesto, ravvisa altresì responsabilità della banca per non aver custodito i dati dei clienti.

Evidenza che la banca non ha rilevato l'anomalia delle operazioni e, neanche di fronte a tale anomalia, la resistente ha chiesto conferma delle transazioni e/o ha sospeso le movimentazioni inconsuete, così acclarando l'inadeguatezza dei sistemi di allerta. In particolare, richiama l'art. 8, lett. a), punto 2, d.m. 112/2007. Nel caso di specie, sono stati effettuati sei bonifici; ne consegue che la succitata disciplina avrebbe potuto essere applicata per scongiurare la truffa subita o comunque per allertare il cliente circa il tentativo di truffa.

In sede di controrepliche, l'intermediario si è riportato alle controdeduzioni.

DIRITTO

Come noto, l'utilizzo fraudolento 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 contesto normativo, 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 – ex multis - 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 che si configura come 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).

Nello specifico, la controversia ha ad oggetto il disconoscimento di cinque bonifici istantanei disposti il 16.4.2025 e il disconoscimento di sei operazioni eseguite il 17.4.2025.

L'intermediario ha rimborsato 2.143,33 euro.

In particolare, risultano rimborsate tutte le ricariche telefoniche (per un totale di euro 500,00) e, per spirito conciliativo, la somma di euro 1.643,33 per i bonifici disconosciuti.

In ordine alle modalità di autenticazione, l'intermediario afferma di aver adottato un sistema di autenticazione forte.

In particolare, rispetto all'enrollment su nuovo device, dopo averla scaricata ed installata il cliente avvia la nuova App. Successivamente, digita il codice cliente e la data di nascita nonché – all'esito – inserisce le tre cifre del PIN richieste.

Il cliente medesimo, sceglie il proprio S*Code e conferma cliccando sul bottone "Scegli lo S*Code". Per procedere con l'attivazione della nuova App è prevista l'autenticazione con OTP (One Time Password) e alle ore 17:59:04 la banca ha inviato un SMS OTP al numero di telefono del ricorrente (corrispondente a quello indicato in denuncia).

Quanto ai bonifici, gli stessi risultano essere stati effettuati tramite autenticazione forte: infatti, secondo l'intermediario il cliente ha ricevuto la PUSH sullo smartphone e ha autorizzato le operazioni attraverso S*Code.

In ordine all'operazione online, la resistente produce i log relativi alla transazione del 17.4.2025 di euro 649,00 eseguita su un sito di e-commerce. In particolare la banca riceve i dati della transazione, li elabora e invia la notifica PUSH allo Smartphone Operativo (primo fattore SCA: possesso) e attende che il cliente autorizzi l'operazione.

Il Titolare autorizza l'operazione facendo Tap sulla PUSH ricevuta sul suo Smartphone Operativo e digitando lo s***code oppure facendosi riconoscere dalla impronta digitale o dal volto (secondo fattore SCA: conoscenza o inerenza).

La banca riceve dalla App la conferma dell'autorizzazione e comunica al sistema che la transazione è stata autorizzata.

Orbene, anche in considerazione dei log prodotti (e delle relative legende), l'operazione in questione è stata correttamente autenticata secondo i requisiti richiesti per la strong customer authentication, nel caso di specie mediante un fattore di conoscenza noto solo al cliente (smart code/codice biometrico) e un fattore di possesso (App generatrice del mobile token).

Quanto, poi, agli elementi rilevanti del fatto risulta che il 16.4.2025 il ricorrente ha ricevuto una chiamata da un numero apparentemente riconducibile alla banca.

Effettivamente, il numero sembra apparentemente riconducibile a uno dei recapiti della banca.

In tale contesto, il Collegio di Coordinamento, con la decisione n. 22745/2019, ha precisato che "la previsione di cui all'art. 10, comma 2, del d. lgs. n.11/2010 in ordine all'onere posto a carico del PSP della prova della frode, del dolo o della colpa grave dell'utilizzatore, va interpretato nel senso che la produzione documentale volta a provare l'"autenticazione" e la formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere probatorio, essendo necessario che l'intermediario provveda specificamente a indicare una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente". Inoltre, ha chiarito che, "nel caso in cui l'intermediario si sia costituito nel procedimento, fornendo prova dell'autenticazione e della regolarità formale dell'operazione, ma nulla abbia dedotto in merito alla colpa grave dell'utente, il Collegio possa comunque affermarne l'accertamento se palesemente emergente dalle dichiarazioni rese dal ricorrente in sede di denuncia all'autorità giudiziaria e/o nel ricorso".

Codesto Collegio, allorquando si verta in ipotesi caratterizzate dalla presenza di artifici e raggiri della medesima tipologia di quelli di cui è rimasto vittima la ricorrente (meglio note con l'espressione di vishing e sostanzialmente valutabili alla stessa stregua delle ipotesi di smishing), l'utente del servizio di pagamento che dà corso all'operazione versi in colpa grave. Si giunge a una simile conclusione sulla base della constatazione dell'ampia diffusione di tali fenomeni, nonché della considerazione che l'impiego da parte dell'utente di una media diligenza risulti sufficiente a scongiurare tale pericolo e quindi a evitare la truffa (cfr., ex multis, Collegio di Roma, decisione n. 8749/2024).

Ed infatti, con particolare riferimento al fenomeno del vishing, la comunicazione per telefono, da parte dell'utente, dei codici dispositivi – ove evidentemente non sussista una frode più sofisticata, in combinazione con altre forme di captazione fraudolenta dei dati sensibili – è considerata quale indice di colpa grave della vittima della frode.

Nella ipotesi sottoposta alla odierna disamina, è la stessa ricorrente a dichiarare di aver ricevuto una chiamata apparentemente proveniente dalla banca resistente che comunicava del tentativo di un bonifico, rispetto al quale sarebbe stato necessario il blocco. Ed il ricorrente, seppure indotto, avviava le procedure ed i dati occorrenti per l'esecuzione delle operazioni poi disconosciute.

Appare significativa, al riguardo, la circostanza per cui la frode sembra essersi configurata alla stregua di un'ipotesi, più specifica, di c.d. vishing caller ID. In particolare, la ricorrente ha comprovato (producendo lo screenshot della schermata dello smartphone contenente i riferimenti della chiamata truffaldina) che il numero di telefono è riferibile a quelli appartenenti all'intermediario.

In simili fattispecie, l'orientamento prevalente tra i Collegi territoriali dell'ABF ravvisa un concorso colposo delle parti, imputando all'intermediario la colpa di "non avere adottato tutti i presidi di sicurezza necessari a impedire che il truffatore potesse chiamare la cliente con un numero riferibile all'intermediario medesimo", richiedendosi l'allegazione da parte del ricorrente della lista delle chiamate ricevute, onde poter verificare la corrispondenza del numero utilizzato dal truffatore con i numeri riferibili all'intermediario. Tale frode è certamente sovrapponibile alle ipotesi di "spoofing", ossia allo smishing in cui il messaggio "esca" 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). E, secondo la più recente posizione dell'ABF, nelle fattispecie di spoofing è al più ravvisabile "un concorso di colpa tra le parti in relazione, da un lato, alla negligenza grave dell'utente che agevola il compimento della truffa, similmente a quanto avviene negli episodi di phishing e, dall'altro lato, alle criticità organizzative del servizio di pagamento offerto dall'intermediario" (in questi termini, Collegio di Roma, decisione n. 8749/2024).

Va chiarito – secondo la stessa eccezione dell'intermediario - che il cliente non sembra aver utilizzato l'App di verifica del numero implementata dalla Banca proprio a tutela dei propri clienti nella prevenzione delle frodi. In particolare, se fosse stato verificato il contatto ricevuto, il sistema avrebbe fornito feedback che il Cliente non era al telefono con un operatore.

Ulteriormente, il cliente ravvisa responsabilità della banca per non aver inviato messaggi di alert prima dell'esecuzione delle operazioni.

La banca afferma che per ciascuna delle operazioni eseguite, al Cliente è stata inviata apposita notifica di alert. Poiché le operazioni sono avvenute in due date differenti, il cliente avrebbe potuto impedire il perfezionamento di tutte le transazioni contestate.

Purtuttavia, la mail pretesamente inviata (e risultante dai log) è differente rispetto a quella inserita nel modulo di disconoscimento.

Va chiarito come non sia possibile parificare il sistema di alert a mezzo SMS a quello via email, perché i due mezzi di comunicazione non offrono lo stesso grado di immediatezza. Se è vero che anche l'SMS può esser conosciuto anche dopo svariate ore dall'invio, e che oggi è ampiamente diffusa la gestione della posta elettronica da smartphone, il telefono cellulare resta uno strumento capace di assicurare un più alto livello di raggiungibilità del destinatario attraverso le comunicazioni via SMS, le quali tra l'altro non hanno bisogno di una connessione internet.

L'ABF, nell'affrontare la questione, ha affermato che l'alert via email (e non SMS) può ritenersi idoneo purché l'intermediario dia prova della ricezione della email, o il ricorrente non ne contesti la ricezione. Il ricorrente, poi, contesta l'esecuzione di cinque bonifici istantanei e ravvisa responsabilità dell'intermediario per non aver rilevato l'anomalia delle operazioni. Sul punto, l'art. 2 del Regolamento Delegato n. 2018/389 prevede un monitoraggio ex post sulle operazioni di pagamento mentre non prevede, di contro, un obbligo di monitoraggio delle operazioni in tempo reale (se non nei casi in cui l'intermediario voglia avvalersi della esenzione SCA), come chiarito dalla Q&A dell'EBA n. 4090/2018. In considerazione delle tematiche compiutamente affrontate e tenuto conto di tutti suddetti elementi di fatto e delle previsioni richiamate del d.lgs. n. 11 del 2010, il Collegio accerta una responsabilità dell'intermediario resistente, in concorso con il comportamento gravemente negligente della cliente, per i danni derivanti dal compimento delle operazioni di pagamento non autorizzate e dispone che, in

aggiunta alle restituzioni già eseguite, l'intermediario corrisponda alla parte ricorrente l'ulteriore importo di euro 800,00, a titolo di risarcimento del danno determinato in via equitativa.

PER QUESTI MOTIVI

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda alla parte ricorrente la somma ulteriore di euro 800,00, determinata in via equitativa.

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