

COLLEGIO DI PALERMO

composto dai signori:

(PA) MAUGERI	Presidente
(PA) PIRAINO	Membro designato dalla Banca d'Italia
(PA) FORGIONE	Membro designato dalla Banca d'Italia
(PA) IMBURGIA	Membro di designazione rappresentativa degli intermediari
(PA) CLEMENTE RUIZ	Membro di designazione rappresentativa dei clienti

Relatore REBECA CLEMENTE RUIZ

Seduta del 29/01/2026

FATTO

La ricorrente riferisce che:

- in data 20 giugno 2024 veniva contattata alla propria utenza mobile dal numero 06-**0 alle ore 10:19 e sul display del proprio dispositivo appariva il logo dell'intermediario;
- l'interlocutore si presentava come consulente dell'ufficio antifrode della Banca e riferiva di aver notato degli anomali movimenti sul suo conto corrente;
- in particolare, vi erano due movimenti, pre-autorizzati, degli importi rispettivamente di euro 250,00 e di euro 400,00 riferiti ad acquisto di criptovalute;
- il sedicente consulente chiedeva invano alla odierna esponente la disponibilità economica residua nel proprio conto corrente nonché gli ultimi movimenti sullo stesso, senza ottenere al riguardo, alcuna risposta;
- l'interlocutore comunicava altresì che la polizia postale l'avrebbe contattata al fine di ricevere informazioni in ordine al blocco delle operazioni;
- dopo alcuni minuti, l'odierna ricorrente veniva raggiunta telefonicamente dal sedicente Ispettore della Polizia Postale tramite l'utenza 091***304;
- quest'ultimo riferiva che era in corso un bonifico in pre-autorizzazione per un importo di euro 13.000,00 che sarebbe stato eseguito intorno alle ore 13.30 dello stesso giorno;

- il presunto ispettore la invitava a recarsi presso la filiale dell'intermediario al fine di distrarre la somma di euro 13.000,00 a mezzo bonifico bancario urgente al fine di mettere in sicurezza i fondi del proprio conto corrente;
 - si recava quindi presso la propria agenzia e, per l'effetto, procedeva all'esecuzione del bonifico urgente presso lo sportello dedicato, utilizzando le coordinate bancarie e la causale che tramite sms (dove figurava il logo dell'intermediario) le venivano indicate dal sedicente consulente;
 - perfezionata l'operazione, veniva inviata la ricevuta del bonifico al sedicente consulente, il quale ne raccomandava la massima riservatezza ed al contempo invitava la ricorrente a non informare i dipendenti dell'agenzia dell'operazione effettuata;
 - successivamente la ricorrente veniva nuovamente contattata dal sedicente consulente, il quale le consigliava di recarsi presso la Polizia postale per sporgere denuncia e ripristinare l'operatività del conto corrente;
 - recatasi presso i vicini uffici della Polizia postale, realizzava che, nella specie era stata vittima di una truffa perpetrata ai suoi danni;
 - nel caso di specie la tecnica di approccio si è sviluppata attraverso una conversazione telefonica tra il cliente ed il truffatore che si finge un operatore bancario;
 - per dare conferma della autenticità del chiamante si è fatto ricorso al camuffamento (spoofing) realizzato attraverso la comparsa sul display del dispositivo mobile, in uso al cliente, del logo della Banca, rendendo così verosimile quanto riferito dall'interlocutore/truffatore;
 - non v'è dubbio che la telefonata dal contenuto allarmistico abbia indotto la ricorrente a mettere in atto quanto alla stessa indicato, al fine di salvaguardare i suoi risparmi;
 - la circostanza che il destinatario di tali avvertimenti sia affetta da "depressione endogena reattiva" in corso di trattamento consentiva al truffatore di realizzare con facilità e successo la truffa;
 - la fattispecie oggetto del presente scrutinio non rientra nella categoria delle cosiddette "operazioni autorizzate";
 - nel caso in specie, non può non rilevarsi una responsabilità concorrente secondo le norme di diritto comune, considerato che la banca ha omesso di adottare adeguate misure di sicurezza volte a prevenire e contrastare l'accesso fraudolento alle informazioni riservate della cliente, posto che un soggetto terzo è riuscito ad acquisire dati sensibili, quali l'esistenza e i dettagli del conto corrente intestato alla ricorrente, circostanza, questa, che denota una falla nel sistema di protezione delle informazioni personali;
 - in tale segmento argomentativo, pertanto, non può che riconoscersi in capo all'istituto bancario la concausa nella verifica dell'evento;
 - nel caso in specie, appare evidente la responsabilità dell'intermediario, nell'area del rischio di impresa, che non ha approntato gli strumenti elettronici necessari al fine di prevenire la possibilità di utilizzo di informazioni circa le posizioni bancarie dei clienti;
 - la "diligenza uomo medio" nel contesto di un correntista si riferisce al comportamento di un individuo di media avvedutezza e accortezza che impiega un adeguato impegno di energie e mezzi nel soddisfare i propri obblighi, sia che si tratti della gestione di un conto corrente che di altre obbligazioni contrattuali;
 - si trovava in una condizione di particolare vulnerabilità psicologica e di ridotta capacità di difesa e detta circostanza ha sicuramente facilitato il successo del piano fraudolento;
 - la truffa si è inoltre avvalsa dell'utilizzo di tecniche di camuffamento del numero telefonico, noto come caller ID spoofing e, tale modalità, ha reso particolarmente insidioso il raggirò, poiché ha creato un'illusione di assoluta veridicità del contatto telefonico;
 - la condotta fraudolenta dei truffatori ha potuto trovare terreno fertile anche per la mancanza di un sistema efficace di verifica da parte della banca che non ha protetto la sua cliente da un uso illecito incluso l'indirizzamento verso la complicità "forzata" del trasferimento di denaro.
- Parte resistente eccepisce che:

- la ricorrente, in data 20/06/2024, disponeva in agenzia e de visu l'ordine di pagamento, con apposizione della propria firma e richiedeva che l'operazione fosse effettuata con modalità "bonifico urgente" al fine di rendere l'importo bonificato immediatamente disponibili sul conto del beneficiario, rendendo quindi lo stesso non revocabile;
- nella denuncia depositata in atti, la ricorrente ha confermato e confessato la volontarietà della sua azione dispositiva che si è concretizzata nella richiesta di esecuzione dell'operazione;
- essendovi la confessione in denuncia, la colpa non ha necessità d'esser provata ma va assunta tal qual è;
- poiché si tratta di una disposizione di pagamento espressamente richiesta dalla ricorrente, essa deve considerarsi autorizzata e pertanto è esclusa dal regime di protezione previsto dal d.lgs. n. 11 del 2010,
- per quanto attiene al canale di provenienza della telefonata occorre sottolineare che il numero 060060 non costituisce la modalità comunicativa ordinaria della Banca in uscita;
- come più volte segnalato dalla Banca alla propria clientela tramite gli avvisi sulla sicurezza, non si deve riporre troppa fiducia nel "caller ID" che appare su telefono fisso o mobile, in quanto è risaputo che esso non garantisce che la chiamata sia effettivamente partita dall'utenza indicata sul display;
- il contenuto della telefonata, sulla base di quanto dichiarato in denuncia, avrebbe dovuto mettere in allarme la ricorrente in considerazione delle richieste del sedicente operatore;
- nello specifico quest'ultimo chiedeva la disponibilità economica del conto corrente, nonché, gli ultimi movimenti del proprio conto. Questo è un evidente indice di anomalia, che la persona accorta avrebbe dovuto riscontrare;
- l'esame della denuncia, riporta una situazione oggettiva, diversa da quella descritta nel ricorso;
- la cliente ha risposto alle richieste del sedicente operatore, consentendogli, così, di venire a conoscenza di informazioni sensibili attinenti al proprio conto corrente;
- il sedicente operatore gli preannunciava, anche, un contatto a breve da parte della polizia postale per avere maggiori informazioni su come poter bloccare le operazioni che a detta dello stesso erano "pre-autorizzate";
- in verità, l'"ispettore" della Polizia Postale nel successivo contatto non provvedeva a dare alla cliente le informazioni necessarie per procedere al blocco delle stesse, ma, la informava di un'altra operazione in "pre-autorizzazione" della somma di euro 13.000,00. Questo rappresenta un evidente indice di anomalia che la ricorrente non poteva non riscontrare;
- sulla base di tutte queste informazioni contraddittorie la ricorrente avrebbe dovuto avvedersi del tentativo di truffa ai suoi danni;
- posto che in pre-autorizzazione vi erano anche, altri due movimenti di € 250,00 ed € 400,00, non si comprende perché vi fosse l'esigenza di mettere al sicuro solo il movimento di 13 mila euro e non anche gli altri;
- è evidente, che la ricorrente ha "creduto" ad una ricostruzione illogica, paradossale e assurda; ha infatti "creduto" alla necessità – comunicata da un soggetto a lei sconosciuto - di mettere in sicurezza la propria disponibilità di conto; ha creduto alla necessità di trasferire altrove le proprie disponibilità, non su di un altro conto corrente a sé intestato (come sarebbe stato quanto meno logico e naturale) ma su di un conto corrente intestato ad un soggetto terzo a lei sconosciuto e con una causale "acquisto auto 500 X" che la stessa ricorrente sapeva non essere corretta;
- se la ricorrente avesse usato la diligenza media del buon padre di famiglia, ovvero quella diligenza che è richiesta a ciascuno nelle vicende della vita quotidiana, si sarebbe agevolmente resa conto del tentativo di frode ai suoi danni;
- in tema di misure di sicurezza adottate per la salvaguardia della propria clientela dal rischio frode, la scrivente Banca ha inviato a tutti i clienti una comunicazione contenente "REGOLE E COMPORTAMENTI PER OPERARE IN SICUREZZA" che nel caso di specie sono stati disattesi dalla ricorrente;

- il legale della ricorrente ha allegato, al ricorso, documentazione clinica della ricorrente. Tale situazione clinica non potrebbe comunque costituire argomentazione per imputare alla Banca una “non adeguata considerazione della condizione di vulnerabilità psicologica della ricorrente che ha determinato l’esposizione al rischio di truffa”;
 - la ricorrente ha espressamente dichiarato in denuncia che “Voglio precisare che quanto sono entrato in *** di Via Libertà per effettuare il bonifico io ero al telefono con i truffatori, i quali mi riferivano che io non dovevo far capire nulla all’operatore della Banca in quanto a loro dire erano tutti sotto indagine e non dovevo fidarmi di loro”;
 - il personale di agenzia non poteva quindi accorgersi della “vulnerabilità psicologica” della ricorrente né di quanto stava realmente accadendo;
 - la stessa documentazione allegata dalla ricorrente ha una datazione di molto precedente al 20 giugno 2024 giorno in cui la ricorrente ha disposto il pagamento di € 13.000;
 - nel caso di specie, la Banca, ha accertato che l’operazione fosse riconducibile alla effettiva volontà del cliente, che di sua spontanea iniziativa ha conferito la disposizione di pagamento, indicato la causale (peraltro coerente con l’importo trasferito) e le coordinate iban del beneficiario e di conseguenza, la Banca ha eseguito la disposizione del ricorrente;
 - venuta a conoscenza del disconoscimento delle operazioni, non ha potuto bloccare l’operazione in quanto bonifico urgente, ma ha avviato l’azione di recall, che a tutt’oggi non ha portato ad alcuna restituzione;
 - da quanto sopra esposto si evince che la Banca, nello svolgimento della propria attività professionale, ha realizzato tutte le misure di sicurezza e prevenzione idonee al fine di tutelare il cliente che, però, qualora rese inefficaci dal suo comportamento, nulla può.
- Con le repliche la ricorrente ha affermato che:
- la sua condotta deve essere scrutinata sulla scorta delle sue qualità soggettive;
 - nella specie si tratta di persona fragile, investita da una telefonata proveniente da numero di un telefono della banca ove la stessa è correntista;
 - il sedicente operatore, oltre a presentarsi senza errori grammaticali, risultava credibile atteso che lo stesso era a conoscenza del rapporto bancario intrattenuto con l’intermediario e delle somme giacenti sul conto, circostanza questa che rendeva ancora più verosimile quanto dallo stesso suggerito;
 - è da considerarsi un prius logico nella causazione dell’evento l’inadeguatezza degli strumenti di protezione della banca che hanno consentito a terzi la possibilità di introdursi nel sistema ed apprendere dati sensibili della correntista, da utilizzare per rendere credibili le istruzioni che vengono impartite;
 - sotto questo profilo la banca non è esente da responsabilità, poiché nel rischio di impresa si comprende anche l’attivazione di sofisticati sistemi di sicurezza per evitare eventuali intrusioni da parte di terzi, al fine di evitare truffe ai danni dei consumatori.

DIRITTO

Le operazioni contestate sono state poste in essere sotto il vigore del d.lgs. 27 gennaio 2010, n. 11, come modificato dal d.lgs. 15 dicembre 2017, n. 218 di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2), entrato in vigore il 13.01.2018, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010 e abroga la direttiva 2007/64/CE e di adeguamento delle disposizioni interne al regolamento (UE) n.751/2015 sulle commissioni interbancarie delle operazioni di pagamento basate su carta.

L’art. 12 del d. lgs. n. 11/2010 regola il regime della responsabilità a fronte dell’utilizzo non autorizzato di strumenti e servizi di pagamento. La disposizione, con un evidente favor nei confronti dell’utilizzatore, opera uno spostamento della responsabilità in capo al prestatore dei servizi di pagamento in caso di

utilizzo fraudolento, estendendola a tutte le ipotesi di violazione degli obblighi di custodia e sicurezza non caratterizzate da frode, dolo o colpa grave.

Ne consegue che, nel caso in esame, al fine di escludere la responsabilità della parte ricorrente, è necessario escludere che il suo comportamento possa configurarsi quale colpa grave.

Sul punto deve essere richiamato l'art. 7, comma 3 del d. lgs. n. 11/2010, in base al quale l'utente *"adotta tutte le ragionevoli misure idonee a proteggere le credenziali di sicurezza personalizzate"*.

Ai sensi del 2° comma dell'art. 10 del d. lgs. n. 11/2010, l'onere della prova che l'utilizzatore abbia agito con dolo o colpa grave incombe sull'intermediario, il quale, ai sensi del primo comma della norma, nel caso di un'operazione di pagamento disconosciuta è tenuto a *"provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti"*.

Deve ancora richiamarsi l'art. 10 bis, comma 1, del d. lgs. n. 11/2010, il quale, recependo l'art. 98 della direttiva UE 2015/2399, sancisce l'obbligo per i prestatori di servizi di pagamento di applicare *"l'autenticazione forte del cliente" nei casi in cui questi acceda al proprio conto di pagamento on line, effettui un'operazione o "qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi"*. Richiamate le norme, posto che questo arbitro deve giudicare in base a quanto in concreto prodotto dalle parti, in base alla documentazione in atti oggetto dell'odierno ricorso è un'operazione eseguita personalmente dalla ricorrente, la quale – sebbene per via del raggio operato dai malfattori – autorizzava un bonifico per la somma di complessiva di €. 13.000,00.

Il Collegio, sulla base della documentazione agli atti, e in particolare delle dichiarazioni confessorie rilasciate dal ricorrente, risulta che la stessa ha personalmente eseguito la procedura, prestando il suo consenso all'esecuzione della stessa, che è pertanto avvenuta mediante corretta autenticazione. Trattasi, pertanto, di operazione che non rientra tra le c.d. transazioni non autorizzate (cfr., ABF Palermo nn. 275/23, 2374/23 e 2723/23 e 10042/2020; ABF Roma, n. 4685/2021, ABF Milano, n. 13553/2021), regolate dalle disposizioni normative sopra richiamate.

Alla luce di quanto dedotto, questo Collegio non accoglie il ricorso.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE