

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) SCIBETTA	Membro di designazione rappresentativa degli intermediari
(PA) PLATANIA	Membro di designazione rappresentativa dei clienti

Relatore ANTONINO FRANCESCO PLATANIA

Seduta del 11/12/2025

FATTO

Il ricorrente chiede la restituzione della somma di euro 840,00, corrispondente all'importo di operazioni disconosciute eseguite fraudolentemente da terzi non autorizzati lamentando che l'intermediario non ha ottemperato all'obbligo di diligenza qualificata meglio conosciuta come la diligenza del bonus argentarius o accorto banchiere, richiesta dal comma 2 dell'art 1176 c.c., in quanto non ha adottato alcuna misura minima per evitare l'accesso fraudolento di terzi ai depositi o a neutralizzarne gli effetti. Il ricorrente evidenzia che la sentenza n.2780/2024 della Corte di Cassazione civile, ha evidenziato che la possibilità di ottenere i codici personali dei correntisti tramite phishing rappresenta un rischio di impresa della banca e, di conseguenza, affinché l'istituto di credito possa sottrarsi dalla propria responsabilità, è necessario che esso dimostri di aver adottato soluzioni idonee a prevenire o ridurre l'uso fraudolento dei sistemi elettronici di pagamento. La diligenza richiesta alla banca si estende alle operazioni che rientrano nella sua sfera di competenza tecnica, considerando anche una valutazione di prevedibilità ed evitabilità ne discende che la banca può essere esonerata dalla responsabilità contrattuale nei confronti del cliente solo in presenza di una colpa grave da parte di quest'ultimo.

Costitutosi l'intermediario convenuto eccepisce che la presunta frode perpetrata ai danni del cliente sembrerebbe essere riconducibile allo schema del phishing classico, unita alla manipolazione del pagatore nella quale il malcapitato predispone operazioni di pagamento, partecipando in tal modo, seppur inconsapevolmente, alla truffa in suo stesso danno. Eccepisce che il ricorrente non ha fornito documentazione alcuna in relazione alla presunta frode subita, limitandosi a disconoscere l'operazione

e asserendo un presunto accesso abusivo dal proprio device in app. Evidenzia la correttezza delle procedure poste in essere in particolare: -L'operazione di pagamento in contestazione consiste in una operazione di bonifico istantaneo online disposta in data 30/07/2025; -Tale operazione risulta correttamente autenticata, registrata e contabilizzata, senza che vi sia stato alcun malfunzionamento o compromissione dei sistemi;- l'autenticazione a forte del cliente è avvenuta mediante autenticazione a due fattori, appartenenti rispettivamente alle categorie della conoscenza e del possesso;- In data 05/2024, risulta regolarmente avvenuta la fase di enrollment; tramite invio di sms OTP sul numero di cellulare indicato dal cliente;- Risulta regolarmente avvenuta la fase di log-in nella quale il ricorrente risulta essersi autenticato in data 30/07/2025, mediante il codice P***ID; Risulta regolarmente avvenuta a mezzo SCA la fase dispositiva dell'operazione oggetto del ricorso. Con riferimento all'art. 8 del D.M. 112/217, la giurisprudenza di merito enuncia il seguente principio di diritto: "Allo stato non è rinvenibile un obbligo di monitoraggio delle operazioni in capo all'intermediario, il quale non può evitare che i propri clienti dispongano liberamente delle somme di cui hanno la disponibilità sul presupposto – indimostrato ed indimostrabile – che ogni operazione anomala sarebbe di per sé truffaldina".In relazione alle operazioni in oggetto l'utenza telefonica collegata alla posizione del ricorrente non sembra aver ricevuto alcuna modifica e non vi è stato alcun cambio di utenza, dall'enrollment della carta e del rapporto;

Eccepisce che gravi sul ricorrente l'onere di fornire "elementi utili a provare che l'operazione sia stata realmente fraudolenta".

DIRITTO

1) Le operazioni contestate sono state eseguite 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 13/1/2018. Ai sensi dall'art. 10 del d.lgs. 11/2010, a fronte del disconoscimento di una operazione di pagamento da parte dell'utente, il prestatore di servizi di pagamento (PSP) ha l'onere di provare: l'autenticazione, la corretta registrazione e contabilizzazione dell'operazione contestata e l'assenza di malfunzionamenti delle procedure necessarie per la sua esecuzione o di altri inconvenienti;-il comportamento gravemente colposo (o fraudolento o doloso) dell'utilizzatore (anche per presunzioni).

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. Con riferimento all'autenticazione delle operazioni e alla valutazione di conformità ai requisiti della SCA si precisa che le fonti normative che regolano la *strong customer authentication* (cd. SCA) sono rinvenibili negli artt. 97 e 98 della PSD2, nell'articolo 10 bis del dlgs. 10/2011, nelle norme tecniche di regolamentazione emanate dall'EBA e recepite con Regolamento Delegato Ue 2018/389 della Commissione Europea, applicabile a far data dal 14 settembre 2019, nonché nei criteri interpretativi forniti dall'EBA.

Nello specifico, l'autenticazione forte (SCA) è richiesta quando il cliente: 1. accede al suo conto di pagamento online; 2. dispone un'operazione di pagamento elettronico; 3. effettua una qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi. La SCA si realizza con il ricorso ad almeno due dei seguenti tre fattori: conoscenza; inerenza; possesso. Gli elementi devono essere reciprocamente indipendenti e appartenere a categorie diverse.

Parte ricorrente lamenta l'esecuzione fraudolenta di un'operazione di bonifico istantaneo eseguito in data 30/07/2025 alle ore 14:27:

Con riferimento all'autenticazione delle operazioni e alla valutazione di conformità ai requisiti della SCA si precisa che le fonti normative che regolano la *strong customer authentication* (cd. SCA) sono rinvenibili negli artt. 97 e 98 della PSD2, nell'articolo 10 bis del dlgs. 10/2011, nelle norme tecniche di regolamentazione emanate dall'EBA e recepite con Regolamento Delegato Ue 2018/389 della

Commissione Europea, applicabile a far data dal 14 settembre 2019, nonché nei criteri interpretativi forniti dall'EBA

Nello specifico, l'autenticazione forte (SCA) è richiesta quando il cliente: 1. accede al suo conto di pagamento online; 2. dispone un'operazione di pagamento elettronico; 3. effettua una qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi. La SCA si realizza con il ricorso ad almeno due dei seguenti tre fattori: conoscenza; inerenza; possesso. Gli elementi devono essere reciprocamente indipendenti e appartenere a categorie diverse.

Con riferimento all'autenticazione forte l'intermediario premette che antecedentemente all'operazione contestata è necessario in via preventiva installare l'app dell'intermediario sul *device*, associare lo strumento di pagamento e configurare il codice P***ID.

La "procedura primaria" di autenticazione forte che caratterizzerebbe tanto le fasi prodromiche quanto quelle dispositive, richiede la conoscenza del codice p** e il possesso del dispositivo dal quale è stato generato il codice p*** nonché l'*enrollment* dell'app sul dispositivo. L'intermediario fornisce evidenze su tali procedure.

Con riferimento alla data di esecuzione dell'operazione fraudolenta – 30/07/2025 – riferisce che non vi sono state modifiche relative all'utenza telefonica del ricorrente. Tale utenza è evidenziata nel documento prodotto e nel modulo di contestazione dell'addebito, in denuncia.

Inoltre, fornisce ulteriore documentazione a riprova che il *device* ID risultante nella fase dalla *enrollment* corrisponde con quello risultante dalla documentazione inerente all'operazione dispositiva. Con riferimento alla fase di accesso in app, prodromica al compimento delle operazioni contestate, l'intermediario rappresenta che il ricorrente risulta essersi autenticato in data 30/07/2025 al proprio *home banking* mediante inserimento del codice P***ID sul proprio *device*.

Sulla base delle evidenze prodotte risulta quindi che la fase di accesso in app sia avvenuta tramite autenticazione forte e, in particolare, mediante l'inserimento del codice P***ID – per il fattore di conoscenza – sul proprio *device* e del fattore di possesso –. Al riguardo si ha presente che, per giurisprudenza consolidata dei Collegi ABF (cfr. Collegio di Coordinamento n. 21285/21) devono essere presidiati dalla autenticazione forte a due fattori non solo le singole operazioni dispositive ma anche tutte quelle operazioni (modifica/aggiunta di un *device*, attivazione di un token, modifica del numero di cellulare e/o della mail associata al conto ecc.) idonee a incidere sulla sicurezza dello strumento e dei pagamenti con questo effettuati

Con riferimento all'operazione di bonifico istantaneo l'intermediario rappresenta che per le operazioni dispositive effettuate tramite l'App, la fase di autenticazione è avviata attraverso l'invio di una notifica *push* sul *device* dell'utente, a fronte della quale quest'ultimo dovrà inserire il codice alfanumerico precedentemente scelto.

Secondo quanto affermato dall'intermediario, una volta attivata, l'App esegue le seguenti attività:- Verifica la firma sulla transazione apposta dal canale;-Mostra i dati transazione all'utente e chiede il PIN per l'autorizzazione;-Genera un OTP, contenente: ID transazione + chiave randomica + chiave simmetrica statica univoca per ciascuna coppia app/device;-Autorizza la transazione inviando al server di firma un messaggio (cifrato e firmato) contenente i seguenti parametri: OTP, ID Transazione, dati Transazione, PIN, Identificativo della singola istanza dell'app. L'intermediario allega Estratti informatici dell'operazione. Da tali evidenze risultano il *device* ID, il canale utilizzato e il metodo dispositivo dell'operazione (MOD DISP – PID, sta a indicare l'utilizzo del codice P***ID).

Sulla base delle evidenze prodotte risulta che il ricorrente ha autenticato correttamente la transazione e, in particolare: Il *device* ID da cui è stata autorizzata l'operazione è quello anzitempo associato al conto (cfr. *File native enrollment*) L'autorizzazione viene fornita tramite inserimento del codice P***ID - Pin.

Risulta pertanto il fattore di conoscenza – con riferimento al codice P***ID – ed il fattore di possesso – con riferimento al *device* utilizzato –.

Si ritiene sussistere la colpa grave del ricorrente in presenza della prova dell'autenticazione forte dell'operazione disconosciuta e dalla mancata allegazione del ricorrente sulle circostanze di fatto della frode .

Il Collegio per quanto sopra ritiene non meritevole di accoglimento la domanda proposta dal ricorrente.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE