

COLLEGIO DI PALERMO

composto dai signori:

(PA) MAUGERI	Presidente
(PA) MELI	Membro designato dalla Banca d'Italia
(PA) FORGIONE	Membro designato dalla Banca d'Italia
(PA) SCANNELLA	Membro di designazione rappresentativa degli intermediari
(PA) DI STEFANO	Membro di designazione rappresentativa dei clienti

Relatore ENZO SCANNELLA

Seduta del 31/03/2026

FATTO

Dopo aver invano esperito la fase di reclamo, con ricorso pervenuto in data 29.12.2025, il ricorrente chiede la restituzione della somma di euro 2.005,50, corrispondente all'importo di operazioni disconosciute eseguite fraudolentemente da terzi non autorizzati.

Parte ricorrente riferisce che/di:

- Essere titolare della carta prepagata presso la resiste n. ***068, associato IBAN ***421;
- In data 23.04.2025, dopo aver ricevuto alcuni messaggi fraudolenti che lo invitavano ad effettuare un presunto "aggiornamento Android" per il proprio dispositivo mobile, si avvedeva, intorno alle ore 23:00, di un ammanco sul saldo della propria carta;
- Accedendo all'applicazione, constatava la presenza di un'operazione a lui non riconducibile, disposta in pari data per l'importo di € 2.005,00 in favore di un soggetto sconosciuto, oltre ad € 0,50 per commissioni, per un totale di € 2.005,50;
- resosi conto di essere stato vittima di una frode informatica agiva con la massima diligenza e tempestività per effettuare quanto segue:
 - In data 23.04.2025, portava il proprio smartphone presso un centro di assistenza tecnica, il quale diagnosticava "TELEFONO HACKERATO" e procedeva alla "RIMOZIONE APPLICAZIONI DANNOSE" e alla "RIMOZIONE VIRUS";
 - In data 24.04.2025, sporgeva formale denuncia-querela disconoscendo formalmente l'operazione e dichiarando di non aver mai smarrito la carta né ceduto a terzi i relativi codici segreti;

- Sempre in data 24.04.2025, presentava formale reclamo alla convenuta contestando l'addebito e descrivendo la dinamica fraudolenta;
 - In data 30.04.2025, si recava presso l'intermediario per richiedere il richiamo dell'operazione fraudolenta;
 - La resistente negava il rimborso asserendo che l'operazione era stata autorizzata tramite un "sistema di autenticazione forte" imputando quindi l'accaduto a una presunta incauta custodia delle credenziali da parte del cliente;
 - Stante il diniego opposto dall'intermediario inviava formale diffida a mezzo PEC in data 08.05.2025 rimasta anch'essa priva di positivo riscontro;
 - Nel caso di specie, l'intermediario si è limitato a eccepire l'avvenuta autenticazione "forte" dell'operazione, senza tuttavia fornire alcuna prova circa la sussistenza di una condotta dolosa o gravemente colposa in capo al ricorrente. Tale allegazione è insufficiente a superare la presunzione di responsabilità a carico dell'intermediario;
 - La prova documentale offerta dalla convenuta dimostra in modo incontrovertibile che il telefono del ricorrente è stato "hackerato" e infettato da virus, proprio nel giorno della transazione. Ciò corrobora la dinamica fraudolenta e smentisce la tesi avversaria secondo cui il cliente avrebbe "incautamente reso disponibili" i propri codici. Le credenziali non sono state cedute, ma fraudolentemente sottratte tramite un attacco informatico. Al contrario, il comportamento post-factum del ricorrente (immediata verifica del dispositivo, denuncia alle Autorità, reclamo all'intermediario) dimostra la sua assoluta buona fede e la massima diligenza esigibile, escludendo in radice qualsiasi profilo di colpa, a maggior ragione grave;
 - La banca non ha adottato sistemi di presidi idonei a prevenire le frodi; infatti, il fatto che un'operazione anomala (di importo rilevante verso un beneficiario sconosciuto e mai utilizzato prima) sia stata autorizzata senza alcun alert o blocco preventivo, evidenzia una potenziale vulnerabilità nei sistemi di monitoraggio e sicurezza.
- L'intermediario, con le controdeduzioni, eccepisce che/di:
- la frode perpetrata ai danni del cliente sembrerebbe essere riconducibile allo schema del "phishing" classico, nel quale il malcapitato, comunicati i propri codici (ricevuti anche per SMS), consente al frodatore di predisporre operazioni dispositive, partecipando in tal modo, seppur inconsapevolmente, alla truffa in suo stesso danno;
 - è stata contestata n. 1 operazione non autorizzata eseguita in data 23/04/2025 utilizzando le credenziali di sicurezza riferibili al ricorrente. Tale operazione risulta correttamente autenticata, registrata e contabilizzata, senza che vi sia stato alcun malfunzionamento o compromissione dei sistemi;
 - l'operazione in esame – posta in essere sotto il vigore del d.lgs. 27 gennaio 2010, n. 11 (il "D.Lgs. n.11/2010"), così come successivamente 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") – sia stata eseguita dalla Società, in conformità art. 10-bis del D.lgs n.11/2010 ovvero, solo in seguito alla corretta e regolare "autenticazione forte del cliente" mediante "autenticazione a due fattori" appartenenti rispettivamente alle categorie della conoscenza (i.e. qualcosa che solo l'utente conosce, ossia il codice P**Id della ricorrente) e del possesso (qualcosa che solo l'utente possiede, ovvero il device sul quale è stata ricevuta la push in app);
 - risulta regolarmente avvenuta la fase di enrollment, la fase di login e la fase dispositiva delle operazioni disconosciute;
 - parte ricorrente ha disposto dallo stesso dispositivo dal quale è stata autorizzata l'operazione contestata un'operazione in data antecedente quella della frode e tale transazione non è stata disconosciuta da controparte;
 - In merito all'eventuale contestazione circa l'asserito mancato adempimento da parte dell'intermediario di un generale obbligo di monitoraggio ex ante dell'operazione disconosciuta, richiama della

giurisprudenza secondo cui l'obbligo di monitoraggio e di sospensione dei pagamenti in caso di "anomalia" degli stessi, non sarebbe espressamente sancito all'art. 8 d. lgs. n. 11/2010;

- In relazione all'operazione in oggetto l'utenza telefonica collegata alla posizione della parte ricorrente non sembra aver ricevuto alcuna modifica;
- La colpa grave del ricorrente in quanto risulta agevole dedurre che il ricorrente abbia ricevuto sulla propria utenza telefonica un contatto da un finto operatore dal quale si è fatto guidare seguendone pedissequamente le istruzioni.
- È presumibile che il cliente abbia provveduto a comunicare i codici segreti, partecipando in tal modo, seppure inconsapevolmente, alla truffa in suo stesso danno, utilizzando per l'operazione contestata il codice P*ID;
- Il blocco della carta in questione è avvenuto contestualmente all'estinzione della stessa, alle ore 09:59 del giorno 24/04/2025 pertanto successivamente all'operazione per cui è controversi;
- Sono stati attivati sistemi di alert mediante notifica push in app.
- per quanto riguarda le richieste risarcitorie avanzate dal ricorrente e da costui quantificate in € 15,00, chiede che l'istanza volta ad ottenere il risarcimento dei danni non dovrebbe trovare accoglimento, stante la carenza di sussistenza di un pregiudizio risarcibile.

In conclusione, l'intermediario chiede al Collegio di rigettare il ricorso in quanto infondato.

DIRITTO

Parte ricorrente chiede la restituzione della somma corrispondente all'importo di operazioni disconosciute eseguite fraudolentemente da terzi non autorizzati.

Preliminarmente, il Collegio evidenzia che mentre il ricorso è stato proposto da parte ricorrente nei confronti dell'intermediario "X", le controdeduzioni sono stati formulati da parte dell'intermediario "Y", soggetto emittente la carta di pagamento mediante cui è stata disposta l'operazione disconosciuta.

L'intermediario "Y", costituitosi nel presente procedimento e appartenente allo stesso Gruppo dell'Intermediario convenuto, parrebbe dunque aver accettato il contraddittorio rispetto alla questione oggetto del ricorso.

In questi casi il Collegio di Palermo ha ritenuto che il contraddittorio possa considerarsi correttamente integrato (cfr. ex. multis, Collegio di Palermo dec. n. 14496/22), pronunciandosi nei confronti dell'Intermediario convenuto.

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:

A. 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.

B. 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.

Parte ricorrente lamenta l'esecuzione fraudolenta di un'operazione di euro 2.005,00 – oltre oneri commissionali pari ad euro 0,50, avvenuta in data 23/04/2025. Pertanto, la domanda ricorrente parrebbe pari alla restituzione di euro 2.005,50 inclusi oneri commissionali.

In merito alla autenticazione delle operazioni e modalità: valutazione di conformità ai requisiti della SCA, le fonti normative che regolano la strong customer authentication (cd. SCA) sono rinvenibili negli

artt. 97 e 98 della PDS2, nell'articolo 10 bis del D.lgs. 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 (v. in particolare il parere dell'EBA del 21 giugno 2019).

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.

Preliminarmente si rileva che la resistente evidenzia che l'utenza telefonica collegata all'utenza del cliente non ha subito alcuna modifica prima dell'esecuzione dell'operazione disconosciuta.

In particolare, il numero indicato nella seguente evidenza corrisponde a quello dichiarato dal ricorrente in sede di denuncia.

In merito alla autenticazione forte con riferimento alla fase di accesso in app e disposizione dell'operazione di giroconto, la resistente riferisce che i fattori autentificativi impiegati siano i seguenti:

-Conoscenza: il Codice P**ID che è un codice di sei caratteri (numeri e/o lettere) scelto dall'utente in fase di abilitazione dei prodotti finanziari in APP P**Pay o B**P**.

Il Codice P**ID si attiva direttamente dalle App installate su smartphone o tablet dell'utente ed è associato in modo univoco al dispositivo dal quale viene generato;

-Possesso: la disponibilità del dispositivo dal quale precedentemente è stato generato il Codice P**ID. Con riferimento all'attivazione del codice P**ID, dichiara quanto segue:

L'attivazione del codice P**ID avviene tramite una procedura di autenticazione forte guidata, che prevede principalmente le seguenti fasi:

1. accesso all'APP, installata sul dispositivo dell'utente, con credenziali (username e password) di registrazione al sito p**.it (fattore conoscenza);

2. abilitazione in APP di almeno un prodotto finanziario. L'abilitazione avviene utilizzando elementi di sicurezza univoci specifici per ciascun prodotto:

- carte prepagate: inserimento data scadenza e CVV2/ CVC2, inserimento di un OTP ricevuto sul numero di cellulare securizzato associato al rapporto (fattore possesso);

- carte debito retail: inserimento data scadenza e CVC2, inserimento della password statica Codice Conto, inserimento di un OTP ricevuto sul numero di cellulare securizzato (fattore possesso);

3. scelta e creazione di un codice alfanumerico di 6 caratteri.

4. Completata l'attivazione del Codice P**ID, il cliente può utilizzare la procedura di autenticazione "primaria" in App (inserendo il codice alfanumerico precedentemente scelto) sia per le operazioni informative che per le operazioni dispositive effettuate tramite l'App stessa ovvero attraverso altri canali (sito internet P**Pay/P** o siti e-commerce).

5. In quest'ultimo caso, la fase di autenticazione è avviata attraverso l'invio in App di una notifica push sul device dell'utente, a fronte della quale quest'ultimo dovrà inserire il codice alfanumerico precedentemente scelto.

L'utilizzo del Codice P**ID è consentito in logica "multi-device" con un vincolo di numero massimo di dispositivi utilizzabili. Per abilitare un secondo dispositivo è necessario avviare un processo di sincronizzazione tramite QR code volto a dimostrare il possesso del primo device. Nel caso in cui l'utente non sia in grado di effettuare la sincronizzazione tramite QR code, dovrà disabilitare i prodotti sul primo device ed effettuare una nuova associazione in App del prodotto finanziario secondo le modalità di dettaglio descritte in precedenza.

Con riferimento alla fase di accesso in app nel caso di specie, la resistente riferisce che nel caso in esame sia stato inserito il codice P**ID e il cliente avrebbe operato all'interno dell'app autenticata.

Sulla base delle evidenze prodotte e sopra riportate, risulta che:

-In data 23/04/2025, alle ore 14:22 è stato registrato un accesso da dispositivo Android LM**525;

- L'accesso è stato autorizzato con inserimento del codice P**ID
 - Segue la disposizione di un'operazione di giroconto di euro 2.005,00;
 - L'operazione di giroconto è stata autorizzata mediante inserimento del codice P**ID.
- Pertanto, parrebbe che la SCA sia provata con riguardo ai seguenti fattori autentificativi:
- L'impiego del device su cui è stato creato il P*ID, che proverebbe il fattore di possesso;
 - L'inserimento del codice P**ID, che proverebbe il fattore di conoscenza.

In merito alle modalità della truffa e sussistenza degli indizi di colpa grave in capo all'utilizzatore, preliminarmente si precisa che la colpa grave del ricorrente assume rilievo solo se l'intermediario fornisce la prova di autenticazione delle operazioni che – secondo l'orientamento condiviso dai Collegi – rappresenta, in aderenza al dato normativo, un prius logico rispetto alla prova della colpa grave dell'utente (cfr. Collegio di Coordinamento, con decisione n. 22745/2019).

Da quanto riferito da parte ricorrente in sede di denuncia parrebbe che:

- In data 23/04/2025 intorno alle ore 23:00 entrava nell'app della resistente e si avvedeva di un ammanco di euro 2.005,00;
- Tale somma era riconducibile a un soggetto dal cliente sconosciuto;
- Dichiara altresì di non avere mai rivelato i codici segreti;
- Non parrebbe riferire nulla in ordine alle modalità della truffa;
- Non appare possibile desumere se trattasi di smishing, phishing o spoofing.

Parte ricorrente deduce tuttavia che il proprio device sarebbe stato oggetto di attacco hacker. In data 23.04.2025, portava infatti il proprio smartphone presso un centro di assistenza tecnica, il quale diagnosticava "TELEFONO HACKERATO" e procedeva alla "RIMOZIONE APPLICAZIONI DANNOSE" e alla "RIMOZIONE VIRUS", come da scheda di riparazione (v. Doc. 3). Tale intervento, costato € 15,00, comproverebbe in modo inequivocabile che la sottrazione delle credenziali sarebbe avvenuta tramite malware installato sul dispositivo a insaputa dell'utente e non per sua negligenza.

Sul punto, si evidenzia tuttavia come parte ricorrente non abbia dedotto le circostanze della frode e non è dunque possibile desumere se le presunte app. malevole siano riconducibili alla frode subita considerato anche che, come visto, i sistemi di autenticazione non hanno registrato alcuna anomalia.

Si osserva che, secondo l'orientamento condiviso dai Collegi territoriali, nel caso in cui:

- i. l'intermediario ha offerto la prova dell'autenticazione delle transazioni sconosciute;
- ii. il sistema di pagamento risulta conforme alla Strong Customer Authentication (SCA);
- iii. non risultano indizi di anomalia delle operazioni e/o ulteriori elementi;

le mancate allegazioni del cliente sulle circostanze di fatto della frode, che afferma di aver patito, rappresentano un elemento da cui il Collegio può trarre il proprio convincimento, insieme ad altre circostanze, circa la colpa grave del ricorrente medesimo.

In un caso simile, il Collegio di Roma, con decisione n. 3358 del 01 aprile 2025, ha osservato quanto segue: "La ricorrente ulteriormente nega di aver ricevuto email o sms di phishing e ipotizza un man in the browser o un attacco malware. Posto che le regole che impongono agli operatori stringenti requisiti di sicurezza sull'autenticazione e sull'autorizzazione dei pagamenti, come risulta essere quello adottato dall'intermediario resistente (anche) per le operazioni qui contestate, hanno la funzione di offrire la massima sicurezza possibile per le operazioni di pagamento, è evidentemente onere di chi allega un'anomalia nel funzionamento provarla. Tuttavia, in assenza di elementi idonei a contestualizzare l'evento truffaldino (come nel caso di specie), questo Collegio ritiene di respingere la richiesta restitutoria del ricorrente, desumendone la colpa grave".

In merito al blocco della carta, posto che il giroconto contestato è avvenuto in data 23/04 e il blocco della carta in data 25/04, quest'ultimo risulta successivo rispetto all'operazione contestata.

Parte ricorrente non ha contestato il superamento del plafond.

In merito ai sistemi di alert, secondo le risultanze degli atti:

- Sembrerebbero essere stati offerti sistemi di alert per le operazioni contestate mediante notifiche push in app;

-Vi è prova della relativa trasmissione della push.

Non si rinvencono indici di anomalia ai sensi dell'art. 8 del DM 112/2007. Non sono presenti in atti evidenze che attestino la normale operatività della ricorrente.

Parte resistente non ha domandato l'applicazione della franchigia.

Parte ricorrente ha domandato anche il riconoscimento degli interessi legali dalla data degli addebiti.

Il ricorrente avanza domanda di risarcimento del danno patrimoniale quantificato in euro 15,00.

In particolare, lo stesso ritiene che l'operazione contestata sia stata eseguita a fronte di un virus/hackeraggio del proprio dispositivo.

Riferisce che il giorno successivo alla frode avrebbe portato il proprio dispositivo in assistenza, ed in tale sede parrebbe essere stata confermata la sussistenza del virus malevolo.

A sostegno di quanto affermato produce evidenza in atti e quantifica il danno patrimoniale nelle spese sostenute per la rimozione del virus.

In conclusione, il Collegio ritiene di respingere la richiesta restitutoria del ricorrente, desumendone la colpa grave.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE