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) NASO	Membro di designazione rappresentativa dei clienti

Relatore MARCO MARINARO

Seduta del 08/09/2025

FATTO

Dal modulo di ricorso e dal verbale di ricezione della denuncia versato in atti si evince che:
- il ricorrente è titolare di un conto corrente presso l'intermediario al quale risulta collegata una carta di debito;
- in data 12.03.2024, riceveva un sms che gli notificava l'esecuzione di un pagamento di euro 2.700,00 indicando un numero di telefono da contattare in caso di disconoscimento dell'operazione;
- il ricorrente chiamava il citato numero e, nel corso dell'interlocuzione telefonica, un sedicente operatore della banca lo invitava a cliccare sul link che gli avrebbe di lì a poco inviato;
- a questo punto veniva indirizzato su una pagina riconducibile al sito della banca all'interno della quale inseriva le credenziali richieste comunicando altresì all'interlocutore i "due codici di sicurezza" nel frattempo pervenuti sul suo cellulare;
- riceveva quindi una serie di mail che gli notificavano sia le spese tentate che le due operazioni autorizzate presso un esercente per un totale di euro 1.500,00.

L'istante riferisce di aver fatto affidamento sulla genuinità delle richieste ricevute in quanto il messaggio proveniva dall'id dell'intermediario e si inseriva all'interno di una chat preesistente contenente messaggi genuini.

Tanto ricostruito, contesta la vulnerabilità dei sistemi sicurezza impiegati dalla banca chiedendo il rimborso della somma indebitamente sottratta.
Costituitosi l'intermediario eccepisce quanto segue:
• in data 11.03.2025, venivano disposte n. 2 operazioni di pagamento per un totale di euro 1.500,00 tramite carta di debito n. **** **21 collegata al conto di titolarità del ricorrente virtualizzata nel wallet G* Pay;
• in pari data, l'istante chiedeva il blocco dalla suddetta carta;
• le operazioni disconosciute sono state effettuate previo accesso all'internet banking del cliente;
• l'accesso è avvenuto mediante: digitazione di codice utente, password, e codice di conferma temporaneo (OTP) inviato per SMS sull'utenza telefonica del ricorrente;
• nella medesima sessione di accesso veniva attivato, attraverso l'apposita sezione presente all'interno dell'area privata, il wallet G*pay, tramite l'inserimento in procedura dell'OTP inoltrato, via sms alle ore 13:02:05, sul recapito di cellulare del ricorrente;
• di tale attivazione, il ricorrente riceveva apposita notifica sempre via sms alle ore 13:03;
• l'asserita truffa subita dal ricorrente si è potuta concretizzare solo a causa del comportamento incauto e negligente assunto dal medesimo;
• quest'ultimo, una volta ricevuto un sms apparentemente inoltrato dalla banca, dava seguito alla richiesta in esso contenuta e contattava imprudentemente un'utenza mobile in alcun modo riconducibile all'Istituto;
• cliccava successivamente su un link e inseriva i dati che consentivano al truffatore di operare sul suo home banking compiendo le operazioni oggetto di contestazione;
• il ricorrente, inoltre, avrebbe potuto evitare i pagamenti se avesse prestato attenzione agli avvisi contenuti nei messaggi recanti i codici OTP autorizzativi.
Conclude per il rigetto del ricorso.
In sede di repliche la ricorrente insiste per l'accoglimento delle richieste formulate richiamando quanto già affermato nel ricorso introduttivo.
In sede di controrepliche l'intermediario richiama il contenuto delle precedenti difese rinnovando la richiesta di accoglimento delle conclusioni ivi rassegnate.

DIRITTO

1.- Le operazioni di pagamento online disconosciute dalla parte ricorrente sono state eseguite in data 11 marzo 2025. Risultano pertanto effettuate dopo l'emanazione della direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015, (c.d. PSD 2 - Payment Services Directive 2), recepita con il d.lgs. n. 218 del 15.12.2017, entrato in vigore in data 13.01.2018, che modifica in più punti il d.lgs. n. 11 del 2010. Si rileva che tali operazioni sono altresì successive alla data di entrata in vigore del Regolamento Delegato (UE) n. 2018/389 della Commissione.
Sulla base di quanto previsto dalla direttiva (art. 115, par. 4), l'art. 5, comma 6, d.lgs. n. 218/2017 prevede tuttavia che "le misure di sicurezza di cui agli articoli 5-bis, commi 1, 2 e 3, 5-*ter*, 5-*quater* e 10-*bis* del decreto legislativo 27 gennaio 2010, n. 11, si applicano decorsi diciotto mesi dalla data di entrata in vigore delle norme tecniche di regolamentazione di cui all'articolo 98 della direttiva (UE) n. 2015/2366". In particolare, la Commissione – delegata ad adottare tali norme tecniche di regolamentazione, ai sensi dell'art. 98, par. 4, della direttiva – ha emanato il 27.11.2017 il regolamento delegato (UE) n. 2018/389 che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri. Il regolamento, ai sensi dell'art. 38, par. 2, si applica a decorrere dal 14.09.2019 e cioè diciotto mesi dopo la

pubblicazione sulla Gazzetta Ufficiale dell'Unione Europea, avvenuta in data 13.03.2018. Ne consegue che anche le norme del d.lgs. n. 11/2010 riferite alle misure di sicurezza, così come modificate dal d.lgs. n. 218/2017, hanno efficacia a partire dal 14.09.2019.
Esse risultano dunque applicabili alla vicenda oggetto del ricorso in esame.
2.- In estrema sintesi, la nuova normativa fa ricadere sull'intermediario la responsabilità delle operazioni disconosciute laddove quest'ultimo non abbia predisposto un c.d. "sistema di autenticazione forte" (in inglese *strong customer authentication* o SCA). Un simile sistema deve essere applicato, stando alla previsione dell'art. 10-*bis*, dai prestatori di servizi di pagamento anche quando l'utente dispone un'operazione di pagamento elettronico ovvero effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi. Quanto alla responsabilità del pagatore, ai sensi del comma 2-*bis* dell'art. 12 d.lgs. n. 11/2010, come inserito dal d.lgs. n. 218/2017, "salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente. Il beneficiario o il prestatore di servizi di pagamento del beneficiario rimborsano il danno finanziario causato al prestatore di servizi di pagamento del pagatore se non accettano l'autenticazione forte del cliente".
3.- Orbene, il concetto di "autenticazione forte" trova la propria definizione all'art. 1, comma 1, lett. q-*bis*), d.lgs. n. 11/2010 (lettera introdotta dal d.lgs. n. 218/2017): "un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione".
Il concetto è oggi ribadito e precisato, specie per quanto concerne la conformità di singole fattispecie concrete alle suddette categorie dell'autenticazione forte, *dall'Opinion of the European Banking Authority on the elements of strong customer authentication under* PSD2 del 21 giugno 2019.
L'EBA ha chiarito, per esempio, che, mentre l'OTP ricevuta tramite sms integra un elemento di possesso idoneo ai fini della strong customer authentication, i dati riportati sulla carta (numero, scadenza e CVV), non costituiscono né un valido elemento di possesso (par. 28), né un valido elemento di conoscenza (par. 33). Al par. 43 di tale documento si legge, in particolare, che "*a number of existing approaches within e-commerce, for card payments in particular, would not be compliant with SCA. This includes approaches in which card details printed in full on the card are used as stand-alone elements or used in combination with a communication protocol such as EMV® 3-D Secure or with only one compliant SCA element (such as SMS OTP)*".
4.- Le operazioni disconosciute consistono in n.2 pagamenti eseguiti tramite digital wallet a valere sulla carta di debito del ricorrente l'11.03.2025 per un importo totale di euro 1.500,00.
Secondo quanto riferito dall'intermediario, le operazioni contestate sono state eseguite mediante wallet G*Pay previa registrazione della carta di debito del ricorrente nella predetta applicazione.
Alla fattispecie è applicabile il principio di diritto espresso dal Collegio di Coordinamento nella Decisione n. 21285/2021, secondo cui:
"*L'utilizzo di un wallet affidato a un terzo gestore per l'esecuzione di operazioni di pagamento non esime l'intermediario, in qualità di prestatore di servizi di pagamento, dall'onere di fornire prova dell'autenticazione forte delle operazioni compiute. La prova non può limitarsi alla fase di c.d. tokenizzazione della carta nel wallet, ma deve riguardare anche la fase esecutiva delle singole operazioni, non potendosi ritenere implicito che le*

transazioni siano state correttamente autenticate dal fatto che le stesse risultino autorizzate o comunque dalla sola evidenza che siano state effettuate in modalità contactless".

Ne deriva che, nel caso di specie, l'intermediario deve fornire la prova della SCA relativamente a ciascuna delle fasi in cui si è articolata la truffa, e segnatamente: (i) l'accesso all'area personale del cliente; (ii) la registrazione della carta sul digital wallet; (iii) l'esecuzione delle operazioni di pagamento.

(i) Accesso all'home banking

Le operazioni disconosciute sono state effettuate previo accesso all'internet banking del cliente mediante le seguenti credenziali:

- username (codice utente) e password statica di esclusiva conoscenza del cliente (elemento di conoscenza);
- digitazione di OTP inviato per SMS sull'utenza telefonica del ricorrente (elemento di possesso).

Nel caso di specie, l'autenticazione è avvenuta secondo le seguenti fasi:

1) avvio sessione di login (accesso all'area privata da App) in data 11.03.2025 alle ore 12:59:30 tramite l'inserimento a sistema di Codice utente e password;
2) invio notifiche di accesso insolito tramite notifiche via SMS sul recapito di cellulare del ricorrente, e-mail e notifiche push su App alle ore 12:59:29;
3) invio codice OTP, via SMS, per validazione della modalità di accesso sopra descritta, sempre sul recapito di cellulare del ricorrente alle ore 12:59:31;
4) inserimento a sistema del codice OTP sopra citato, alle ore 13:00:11, per finalizzazione accesso all'internet banking.

Il numero di telefono cui risulta inviato l'SMS recante il codice OTP coincide con quello indicato dal cliente in sede di denuncia.

(ii) Digitalizzazione della carta

Durante questa sessione di accesso veniva attivato, in relazione alla carta di debito in esclusivo possesso del ricorrente, il servizio wallet G*pay.

L'attivazione si è finalizzata, post accesso tramite codice utente, password e codice OTP autorizzativo (session_id -2042727214), attraverso l'apposita sezione presente all'interno dell'area privata, e tramite l'inserimento in procedura dello specifico codice OTP inoltrato, via SMS in data 11 marzo 2025 alle ore 13:02:05, sul recapito di cellulare del ricorrente.

Di tale attivazione, il ricorrente ha ricevuto apposita notifica, via SMS sul recapito sopra richiamato, alle ore 13:03:35.

L'associazione della carta al Wallet risulta dunque essere avvenuta attraverso la App bancaria.

Con la Q&A ID 2019_4910 l'EBA ha precisato che l'associazione di una carta di pagamento ad un wallet digitale rientra tra quelle azioni che possono comportare un rischio di frode nei pagamenti o altri abusi e, pertanto, richiede l'applicazione della SCA; ciò significa che i PSP devono impiegare una procedura di autenticazione forte per l'accesso al conto di pagamento e una seconda SCA quando l'utente aggiunge la carta di pagamento al digital wallet.

Con riguardo alla fase di associazione della carta al digital wallet, in genere, gli standard dei wallet provider consentono ad oggi due modalità di tokenizzazione della carta:

a) una prima avviene direttamente dal wallet e, in questo caso, i dati della carta sono catturati dalla fotocamera o inseriti mediante input manuale;
b) la seconda si realizza dall'app di mobile banking, con la conseguenza che i dati della carta sono già disponibili e l'utente può limitarsi semplicemente a dare il comando "aggiungi carta al wallet".

In tale ultima ipotesi, il Collegio riconosce un sistema di autenticazione conforme alla disciplina vigente. Tale modalità di associazione utilizza un fattore di conoscenza (credenziali statiche) ovvero di inerenza per sbloccare l'app e un fattore di possesso (SMS OTP o l'app stessa) per il completamento della procedura di associazione della carta al wallet (Collegio di Roma, decisione n. 6543/2024).

(iii) Le operazioni dispositive

Le operazioni sono state eseguite da Wallet G*pay, avvicinando la carta digitalizzata al pos in modalità contacless.

L'intermediario sostiene che i due pagamenti contestati sono stati autenticati mediante il device del truffatore e la password (allega la documentazione tecnica e la relativa legenda).

L'utilizzo della carta tokenizzata costituisce un fattore di possesso secondo la Question ID: 2019_4827 dell'EBA.

Quanto al secondo fattore, nella legenda si specifica che dalla dicitura "Tipo oper.: AUT" si evince l'uso dell'ulteriore elemento di conoscenza.

I Collegi si sono espressi in merito alla valenza da attribuire alle informazioni presenti nei log prodotti dagli intermediari per provare l'autenticazione forte del cliente nelle operazioni di pagamento disconosciute (artt. 10, comma 1 e 10-bis del D.lgs. 11/2010), nei casi in cui dalla tracciatura informatica non risulti in modo esplicito uno dei fattori di autenticazione inseriti (conoscenza, possesso o inerenza).

Tenuto conto che la PSD2 è tecnologicamente neutrale e non prevede un sistema informatico standard per l'inserimento e la tracciatura dei fattori di autenticazione forte, i Collegi ritengono che, per valutare l'assolvimento dell'onere della prova della SCA, possono essere valutati (oltre ai log) anche ulteriori elementi esplicativi, quali la legenda e/o quanto rappresentato dal PSP nelle proprie difese in relazione al caso concreto, purché consentano di verificare i singoli passaggi registrati dal sistema informatico come prova di autenticazione. I Collegi ritengono inoltre che eventuali dichiarazioni confessorie del cliente possano assumere valore di prova legale ai sensi dell'art. 2730 c.c.

5.- Il ricorrente chiede la restituzione dell'importo di euro 1.500,00 che asserisce essergli stato fraudolentemente sottratto all'esito di truffa perpetrata ai suoi danni tramite la tecnica dello smishing/vishing (a suo dire con id spoofing).

Riferisce di aver ricevuto -in data 11.03.2025- un sms che gli notificata l'esecuzione di un pagamento di euro 2.700,00 indicando un numero di telefono da contattare in caso di disconoscimento dell'operazione.

Il ricorrente chiamava il numero indicato e, nel corso dell'interlocuzione telefonica, un sedicente operatore della banca lo invitava a cliccare sul link che gli avrebbe, di lì a poco, inviato.

A questo punto veniva indirizzato su una pagina riconducibile al sito clone della banca all'interno della quale inseriva le credenziali richieste comunicando altresì all'interlocutore i "due codici di sicurezza" nel frattempo pervenuti sul suo cellulare.

È versato in atti il messaggio da cui è partita la frode; da tale evidenza sembra evincersi che:

- il messaggio si inserisce all'interno di una chat preesistente contenente messaggi apparentemente genuini;
- contiene un numero di telefono non riconducibile all'intermediario che il ricorrente ammette di aver chiamato.

Non è prodotta evidenza del registro chiamate né del messaggio contenente il link che il ricorrente riferisce di aver cliccato.

Solo nella denuncia si rinviene una trascrizione del link truffaldino che contiene un richiamo all'intermediario.

6.- Tanto premesso, con riguardo alle frodi perpetrate mediante la fattispecie dello spoofing, l'orientamento condiviso dai Collegio ABF è nel senso di ritenere che sia quando il messaggio civetta si inserisca in una "*conversazione"* o "*chat*" contenente precedenti messaggi genuini provenienti dall'intermediario, sia quando sussista un singolo messaggio civetta che risulti apparentemente proveniente dall'intermediario in relazione alla simulazione del nome del mittente, occorra valutare caso per caso eventuali profili di colpa grave del cliente, non potendosi ipotizzare automatismi di sorta circa il riparto di responsabilità tra le parti (es. presenza di errori grammaticali nel testo del messaggio civetta).
In relazione alla rilevanza del messaggio parlante, i Collegi ABF hanno ritenuto che può essere rilevata in via esclusiva la colpa grave del cliente (con conseguente rigetto del ricorso) laddove, oltre ad indici di anomalia (inequivoca non riconducibilità all'intermediario del link contenuto nel messaggio civetta; evidenti errori grammaticali o di sintassi del medesimo messaggio) pervenga al cliente una comunicazione ulteriore rispetto alla procedura di autenticazione forte, tale da sollecitare la sua attenzione sull'operazione che sta per autorizzare (ad es. OTS) e il cui contenuto informativo non sia messo in dubbio da indicazioni di segno contrario (ad es. messaggi di storno).
Nei casi in cui si riscontrino indici di inattendibilità o anomalie del messaggio, il Collegio di Roma è solito orientarsi per un concorso di colpa tra le parti.
La colpa del cliente, peraltro, è stata altresì dedotta dalla ricezione, immediatamente di seguito alla ricezione del messaggio decettivo, di un messaggio genuino di avviso dell'attivazione di un mobile token, senza che ciò sia valso a insospettire il cliente (Collegio di Roma, decisione n.451/25).
7.- Pertanto, il Collegio accoglie parzialmente il ricorso e ritiene che la quota di responsabilità da addebitare all'intermediario in relazione alla fattispecie concreta vada determinata ex art. 1226 c.c. nella misura di euro 750,00 che dovrà essere versata alla parte ricorrente.

PER QUESTI MOTIVI

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda alla parte ricorrente la somma di euro 750,00, 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

Firmato digitalmente da
PIETRO SIRENA