

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MARINARO	Membro designato dalla Banca d'Italia
(RM) MAIMERI	Membro designato dalla Banca d'Italia
(RM) CARATELLI	Membro di designazione rappresentativa degli intermediari
(RM) NASO	Membro di designazione rappresentativa dei clienti

Relatore MARCO MARINARO

Seduta del 24/02/2026

FATTO

La parte ricorrente espone quanto segue:

- in data 24/04/2025, ha ricevuto 3 SMS che lo allertavano di disposizioni di pagamento per ingenti somme di denaro, da lui non autorizzate, con l'invito a contattare immediatamente il numero di telefono riportato nel messaggio ai fini del disconoscimento;
- si è convinto della genuinità dei messaggi in quanto sono pervenuti nella medesima chat in cui la banca invia sms di sicurezza e poiché un mese prima aveva già subito un tentativo di frode in una simile modalità ed era stato contattato dalla banca nel medesimo modo per bloccare la carta di credito che è poi stata sostituita ed inviata pochi giorni dopo;
- quindi ha contattato il numero di telefono indicato nell'SMS al quale ha risposto una persona identificandosi come operatore antifrode della banca resistente;
- costui ha carpito la sua fiducia in quanto era a conoscenza del primo tentativo di frode, di cui lui non aveva fatto menzione e della sostituzione della sua carta di credito;
- dunque, credendo di essere realmente in contatto con la banca ha seguito le istruzioni fornite per bloccare tutte le sue carte e disattivare il servizio di home banking;
- il sedicente operatore antifrode gli indicava di procedere anche ad un ulteriore livello di sicurezza, posto che si trattava del secondo tentativo di frode e, seguendo le sue istruzioni, spegneva il cellulare in modo da porre in essere le verifiche di clonazione del suo numero telefonico;

- l'operatore gli richiedeva dunque un ulteriore contatto telefonico su cui contattarlo per informarlo del responso delle verifiche ed egli indicava il numero di cellulare della moglie;
- il sedicente operatore lo ha ivi contattato una prima volta intorno alle 15,30 chiedendogli di attendere un'altra ora per non interrompere le operazioni di verifica;
- alle ore 17 circa è stato ricontattato e gli è stato comunicato che l'operazione era andata a buon fine;
- una volta acceso il cellulare, ha ricevuto un ulteriore sms relativo ad una disposizione di pagamento, allora ha chiamato il numero verde della banca e ha realizzato di essere rimasto vittima di frode e ha chiesto il blocco dello strumento di pagamento.

Chiede la restituzione della somma sottratta fraudolentemente.

Nelle controdeduzioni, l'intermediario rileva che:

- nel ricorso, il ricorrente non ha specificato l'esatto ammontare della somma che richiede in restituzione; tuttavia, nel modulo di contestazione che il cliente ha inviato alla Banca ha chiesto il rimborso di 2 operazioni;
- pertanto, si deve intendere che il presente ricorso ha ad oggetto esclusivamente tali 2 operazioni di spesa eseguite online con la carta di credito n. *875, in data 24.04.2025, rispettivamente per € 2.020,00 delle ore 14:51 e di € 1.212,00 delle ore 14:53 per complessivi € 3.232,00;
- invero, nella denuncia il ricorrente disconosce plurime operazioni che tuttavia non sono state oggetto di contestazione nel reclamo e pertanto, ove intenda chiedere il rimborso delle stesse, la domanda dovrà ritenersi inammissibile;
- peraltro, in base a quanto narrato in denuncia, il ricorrente ammette di aver indicato le sue credenziali ai frodatori e di aver approvato le notifiche push, consentendo al perfezionamento della frode ai suoi danni;
- il cliente ha provveduto a bloccare la carta di credito n. **875 in data 24.04.2025 alle ore 17:19;
- le operazioni disconosciute sono risultate eseguite mediante l'utilizzo delle credenziali di sicurezza personalizzate, su sito "3d secured", cioè che opera in modalità sicura e validate attraverso l'utilizzazione del codice OTP generato dal dispositivo in possesso del cliente;
- i casi di phishing, in senso lato, sono ormai conosciuti dagli utenti e pertanto il comportamento del ricorrente appare connotato da colpa grave;
- nel caso che qui interessa, è risultata palese l'incauta custodia da parte del ricorrente delle credenziali legate al proprio strumento di pagamento;
- peraltro, il ricorrente appartiene alle forze dell'ordine e dunque in ragione della professione svolta la colpa grave risulta tanto più evidente.

Chiede il rigetto del ricorso.

DIRITTO

1.- Le operazioni di pagamento online disconosciute dalla parte ricorrente sono state eseguite in data 24 aprile 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)*".

Alla luce di un simile orientamento, con riguardo alle operazioni successive al 14.09.2019, questo Collegio ritiene che l'inserimento dei dati della carta, al fine di dar corso alle operazioni di pagamento, non integri un idoneo fattore di autenticazione (così, per esempio, Collegio di Roma, decisione n. 8493/2020, decisione n. 15221/2021 e decisione n. 21761/2021).

4.- Nel ricorso, l'istante non indica analiticamente le operazioni contestate né il loro ammontare complessivo. Tuttavia, allega al ricorso un documento con evidenza di molteplici disposizioni di pagamento eseguite il giorno della frode 24.04.2025 per complessivi € 7.272,86 (cfr. allegato al ricorso denominato "operazioni").

Si tratta in particolare di 10 operazioni eseguite in data 24.04.2025: un'operazione per € 101,00; tre operazioni per € 308,53; un'operazione per € 772,28; un'operazione per € 219,18; un'operazione per € 238,03; un'operazione per € 217,38; un'operazione per € 665,47; un'operazione per € 901,93; un'operazione per € 1.212,00; un'operazione per € 2.020,00.

Nella denuncia del 24.04.2025 il ricorrente sostiene di aver subito addebiti per circa € 10.000,00; nella integrazione di denuncia del 28.04.2025 lamenta addebiti per € 4.040,86 e nella successiva integrazione di denuncia del 28.04.2025 lamenta l'addebito di due ulteriori operazioni per € 1.212,00 e per € 2.020,00.

In effetti, la somma di € 4.040,86 e di € 3.232,00 disconosciuti nelle denunce del 28.04.2024 ammonta a complessivi € 7.272,86.

Tuttavia, l'intermediario eccepisce che nel modulo di disconoscimento parte ricorrente contesta unicamente due transazioni per € 1.212,00 e per € 2.020,00 del 24.04.2025.

Pertanto, la banca sostiene che solo tali operazioni possono rientrare nella cognizione dell'Arbitro posto che per le ulteriori transazioni non è stato previamente proposto il reclamo.

In effetti, le disposizioni ABF (Sez. VI, par. I) prevedono che "Il ricorso deve avere ad oggetto la stessa questione esposta nel reclamo".

A fronte di tali contestazioni sollevate dall'intermediario in sede di controdeduzioni, il ricorrente non ha presentato repliche.

Pertanto, l'individuazione delle transazioni disconosciute deve intendersi come pacifica.

5.- Alla luce di quanto sopra precisato, occorre precisare che la parte ricorrente disconosce due operazioni di pagamento eseguite on line, con la carta di credito n. *875, in data 24.04.2025: un pagamento di € 2.020,00 delle ore 14:51; un pagamento di € 1.212,00 delle ore 14:53; per complessivi € 3.232,00.

L'intermediario afferma che le operazioni di pagamento risultano correttamente autenticate, registrate e contabilizzate e che non è emerso alcun malfunzionamento o compromissione dei sistemi.

L'accesso da altro dispositivo (presumibilmente appartenente al frodatore) è avvenuto mediante inserimento di id utente e codice PIN (fattore di conoscenza) e successiva attivazione del mobile token sul nuovo dispositivo mediante inserimento del codice PIN (fattore di conoscenza) e codice OTP ricevuto via SMS (fattore di possesso).

Pertanto, la fase di accesso e di attivazione del mobile token su un nuovo dispositivo appare conforme a SCA.

L'intermediario afferma in particolare che le operazioni sono state effettuate online su sito che opera in modalità sicura e validate mediante Pin e OTP generata da mobile token.

Dai LOG prodotti emerge che le operazioni fraudolente sono state entrambe validate con codice PIN (fattore di conoscenza) e codice OTP (fattore di possesso).

Al fine di generare l'OTP silente è stato necessario approvare una notifica push o conferire apposita autorizzazione dalla "lista delle autorizzazioni" presente sull'APP dell'intermediario, mediante touch/face ID o codice PIN.

Nel caso di operazione validata con PIN e OTP generata da token App, i Collegi ritengono conforme alla SCA il processo di autenticazione sopra descritto, il quale prevede l'utilizzo di un fattore di conoscenza (PIN) o inerenza (touch o face id) e di un fattore di possesso (OTP generato dal mobile token) (Collegio di Roma, decisione n. 5250 del 28.03.2022).

6.- Il ricorrente ha presentato una denuncia successivamente integrata da altre due denunce da cui emerge che:

- in data 24.04.2024, alle ore 13:09 ha ricevuto un SMS apparentemente proveniente dalla banca che lo ha informato dell'esecuzione di diversi pagamenti con la sua carta di credito rispettivamente di € 500,00, di € 870,00 e di € 990,00 presso degli e-commerce, da lui non autorizzati;
- nel testo dell'SMS gli veniva comunicato che per disconoscere suddetti pagamenti avrebbe dovuto chiamare il numero indicato;
- parte ricorrente non ha versato in atti i suddetti SMS; pertanto, non è possibile verificare se si sono collocati nella chat in cui è solito ricevere le comunicazioni bancarie né se presentano errori grammaticali (cfr. sul punto integrazione istruttoria infra);
- ha contattato il numero indicato al quale ha risposto un sedicente operatore antifrode, il quale era a conoscenza di un precedente tentativo di frode subito dal ricorrente;
- l'interlocutore telefonico ha illustrato al ricorrente la necessità di seguire le istruzioni che gli avrebbe impartito e così il ricorrente ha validato le notifiche push ricevute, comunicando i relativi codici all'operatore;

- al termine delle operazioni, l'interlocutore ha comunicato al ricorrente che avendo già subito due tentativi di frode era necessario "isolare" il cellulare e che pertanto bisognava spegnerlo per circa due ore; il ricorrente ha quindi comunicato il numero di cellulare della moglie sul quale veniva contattato dal frodatore che faceva presente che il blocco era andato a buon fine;
- dopo circa due ore, ha acceso il cellulare e ha ricevuto degli SMS alert relativi al compimento di operazioni dispositive, ha quindi realizzato di essere rimasto vittima di frode; ha contattato il numero verde della banca e ha bloccato gli strumenti di pagamento.

Nel caso di specie, la parte ricorrente ha allegato alla denuncia gli screenshot degli SMS.

Pertanto, questo Collegio, nella riunione del 12.11.2025, ha deliberato quanto segue: "Il Collegio, ritenuto necessario acquisire ulteriori elementi ai fini della decisione, invita la parte ricorrente a produrre, entro 15 giorni dalla ricezione del presente provvedimento, copia delle schermate relativi agli SMS relativi alla truffa. Proroga di 90 giorni il termine per l'assunzione della decisione".

Il provvedimento è stato comunicato alla parte ricorrente il 14.11.2025 ed è stato riscontrato in data 15.11.2025. Il ricorrente ha prodotto una serie di screenshot, dall'esame dei quali emerge che l'SMS esca si è posizionato nella chat in cui il ricorrente è solito ricevere le comunicazioni bancarie, in quanto è seguito da SMS genuini; gli SMS fraudolenti non presentano errori grammaticali.

7.- All'esito dell'esame istruttorio, ad avviso del Collegio nel caso di specie la parte ricorrente deve ritenersi essere rimasta vittima di una fattispecie delittuosa riconducibile al c.d. "sms spoofing".

Secondo l'orientamento condiviso fra i Collegi ABF, nelle fattispecie di spoofing non è generalmente ravvisabile la colpa grave del ricorrente, "a meno che non si rinverano [...] indici di inattendibilità o anomalia del messaggio; in tale caso, potrà essere ravvisato 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".

Pertanto, non sussistendo indici di inattendibilità o anomalie del messaggio tali da consentire di ritenere che cliente abbia tenuto una condotta gravemente colposa, la domanda restitutoria deve essere integralmente accolta con riguardo alle due operazioni oggetto di esame.

PER QUESTI MOTIVI

Il Collegio, in accoglimento del ricorso, dispone che l'intermediario corrisponda alla parte ricorrente la somma di euro 3.232,00. Respinge nel resto.

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