

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) FULCHERI	Membro di designazione rappresentativa dei clienti

Relatore MARCO MARINARO

Seduta del 22/12/2025

FATTO

Da quanto dichiarato in sede di denuncia – querela e dai fatti affermati in ricorso, si desume che:

- il ricorrente riceveva una telefonata da un sedicente operatore del servizio antifrode dell'intermediario;
- questi induceva il ricorrente a entrare nella propria area personale del sito internet della banca e a disporre alcune operazioni di pagamento;
- conclusa la telefonata, il ricorrente contattava un operatore della filiale della banca resistente, il quale lo informava che probabilmente era stato vittima di una truffa;
- alcune tra le operazioni dispositive effettuate dal ricorrente su indicazione del truffatore venivano bloccate dall'addetto di filiale;
- due bonifici di importo pari a € 2.000,00 cadauno, per un totale di € 4.000,00, non potevano essere annullati;
- veniva presentato reclamo all'intermediario, che negava ogni responsabilità;
- la banca, nell'esercizio di un'attività pericolosa ex art. 2050 c.c., è tenuta a osservare ogni misura per evitare danni a carico dei clienti;
- nel caso di specie, non sussiste dolo o colpa grave del ricorrente, indotto a credere di essere contattato da un operatore della banca;
- inoltre, la banca non ha inviato alcun alert, circostanza che ha reso impossibile il contenimento dei danni subiti dal ricorrente.

Chiede il rimborso dell'importo di € 4.000,00.

L'intermediario resiste al ricorso ed eccepisce di aver messo in atto ogni misura possibile per evitare il danno, ma per i due bonifici oggetto di ricorso il recall non è andato a buon fine per mancata autorizzazione dell'istituto del conto di radicamento del bonifico.

Le operazioni sono state materialmente poste in essere dal ricorrente, dunque, non trova applicazione la disciplina in materia di operazioni non autorizzate.

L'autorizzazione delle operazioni è avvenuta in modalità SCA compliant, mediante doppio fattore, utilizzando il dispositivo certificato in uso al ricorrente.

Ha diffuso una campagna informativa sul proprio sito internet relativa alle frodi più diffuse, tra cui rientra quella della quale il ricorrente è rimasto vittima. E' configurabile la colpa grave del cliente, che ha dato corso alle istruzioni ricevute telefonicamente senza accertarsi della loro genuinità. Inoltre, i bonifici sono stati disposti in favore del ricorrente medesimo, per cui non è configurabile alcun danno.

Chiede che il ricorso venga respinto.

Con le repliche il ricorrente eccepisce che l'intermediario non è stato diligente nell'osservare i propri doveri di protezione nei confronti del cliente. Infatti, non è stato attivato il servizio di SMS alert e non ha provato che le operazioni contestate siano state disposte entro i limiti del plafond giornaliero.

Nelle controrepliche l'intermediario precisa che il servizio di SMS alert non avrebbe impedito la truffa; le operazioni sono state effettuate a distanza di pochi minuti l'una dall'altra (circa 3 minuti) e sono state disposte in favore del ricorrente medesimo, quindi non è configurabile alcun danno. Il plafond delle operazioni dispositive è pari a € 30.000,00/giorno, per cui le operazioni rientrano entro i limiti contrattualmente previsti.

DIRITTO

1.- Le operazioni di pagamento online disconosciute dalla parte ricorrente sono state eseguite in data 13 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.- La controversia ha ad oggetto due operazioni di bonifico istantaneo di importo € 2.000,00 cadauna. L'intermediario afferma che le operazioni sono state eseguite materialmente dal ricorrente, su indicazioni del truffatore.

Le operazioni sono state disposte tramite internet banking, attraverso un doppio fattore di autenticazione.

In particolare, per accedere alla propria area personale, il cliente è tenuto a digitare: due password statiche, Codice PIN e Codice Titolare (fattori di conoscenza); una password dinamica OTP generata da APP installata su device certificato o ricevuta via SMS su numero di cellulare certificato (fattore di inerenza). Produce i relativi LOG.

Tale sistema di autenticazione è ritenuto conforme alla SCA dal Collegio di Roma (cfr., ex multis, Coll. di Roma, 3017/2023).

5.- Il ricorrente afferma di aver disposto materialmente l'operazione oggetto di ricorso per essere stato indotto da un sedicente operatore dell'intermediario, che lo contattava telefonicamente.

Il numero di telefono indicato in denuncia corrisponderebbe a quello della resistente.

Le circostanze dedotte in ricorso sono coerenti con quanto dichiarato in sede di denuncia-querela, porta il giorno successivo a quello della truffa.

L'orientamento unanime dei Collegi territoriali ritiene che, quando l'operazione è eseguita per intero dal pagatore, deve considerarsi autorizzata e non è quindi soggetta al regime di responsabilità previsto dalla PSD2.

I Collegi convengono che, in questi casi, non è configurabile una responsabilità oggettiva del PSP. Il Collegio potrà comunque rilevare una responsabilità concorrente del PSP, sulla base delle evidenze disponibili e secondo le norme di diritto comune, quando emerge in concreto dalla documentazione in atti un apporto causale dell'intermediario alla frode.

Il ricorrente non ha prodotto con il ricorso evidenza del registro chiamate; questo Collegio, nella riunione dell'8 settembre 2025, ha deliberato di chiedere alla parte ricorrente la produzione di copia delle schermate relative al registro chiamate del giorno della truffa.

La parte ricorrente non ha fornito riscontro.

6.- In conclusione, laddove il ricorrente ammetta di aver dato seguito a una comunicazione di *phishing* (via email, sms o chiamata vocale), fornendo le proprie credenziali, i Collegi, in linea con la decisione n. 3498/2012 del Collegio di Coordinamento, ritengono che il cliente sia vittima di colpevole credulità, risultando "tali forme di accalappiamento" "ormai note al pur non espertissimo navigatore di internet". Nel caso di specie, la parte ricorrente ha fatto affidamento su una telefonata proveniente da un numero del quale non è stata data evidenza circa la dedotta riconducibilità all'intermediario.

7.- Alla luce di quanto esposto, il Collegio ritiene che la domanda non possa trovare accoglimento.

PER QUESTI MOTIVI

Il Collegio respinge il ricorso.

IL PRESIDENTE