

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) BONACCORSI DI PATTI	Membro di designazione rappresentativa degli intermediari
(RM) FULCHERI	Membro di designazione rappresentativa dei clienti

Relatore DOMENICO BONACCORSI DI PATTI

Seduta del 06/02/2026

FATTO

Nel ricorso, parte ricorrente espone di essere titolare di una carta di pagamento emessa dal resistente che è solito ricaricare con la provvista proveniente dal conto corrente radicato presso l'intermediario X. Il ricorrente, in data 14.05.2025, riceveva una notifica dall'applicazione bancaria dell'istituto di credito resistente per l'autorizzazione di una transazione di € 200,00 che non ha autorizzato; immediatamente dopo, il cliente riceveva una chiamata da un numero in chiaro apparentemente riconducibile all'intermediario resistente; l'interlocutore si è presentato come operatore del servizio clienti e lo ha invitato a non acconsentire alle notifiche via app e ha – apparentemente – trasferito la chiamata all'assistenza clienti dell'istituto X di radicamento del conto corrente. Poco dopo ha ricevuto una chiamata da altro numero (riconducibile alla filiale presso la quale è attivo il conto corrente presso l'intermediario X) nel corso della quale l'operatore confermava l'esistenza di un tentativo di frode a suo danno; per tali motivi il ricorrente avrebbe dovuto eseguire dei bonifici guidati utili a “mettere al sicuro” i fondi. Constatato il funzionamento dell'iter, ha trasferito la somma di € 4.980,00 dal proprio conto corrente alla carta di credito emessa dal resistente, ricevendo la rassicurazione che anche detto importo gli sarebbe stato in seguito restituito in un'unica soluzione, al termine delle operazioni di “messa in sicurezza” dei fondi. Successivamente riceveva una telefonata da parte di un sedicente Maresciallo dei Carabinieri di Frosinone incaricato di svolgere le indagini circa il tentativo di frode compiuto a suo danno; tale soggetto, diffidava il ricorrente dal parlare con altri dell'accaduto, pena l'apertura di un procedimento penale a suo carico; veniva poi contattato da un'utenza telefonica in chiaro e, su indicazioni dell'operatore, dopo aver compiuto un'operazione per € 87,13 su una

piattaforma di delivery, ha trasferito tramite l'app bancaria della resistente sulla carta di credito emessa dalla resistente ulteriori € 5.000,00; veniva poi eseguito un bonifico di € 4.980,00 senza la sua collaborazione. Il ricorrente chiede il rimborso di € 10.047,13.

Nelle controdeduzioni, l'intermediario resistente espone che: i) con riferimento ai n. 2 addebiti su carta di debito oggetto di ricorso, risulta che questi sono stati autorizzati dal dispositivo mobile associato al conto del ricorrente mediante SCA rispettivamente alle ore 14:30 e alle ore 16:30 del 14 maggio 2025; ii) con riferimento al bonifico contestato, si precisa che questo è stato autorizzato dal device personale associato al conto del ricorrente alle ore 00:11 del 15 maggio 2025; iii) tutte le predette operazioni venivano eseguite all'interno delle sessioni in-app per l'accesso al conto avviate il 14.05.2025 dalle ore 14:28 ora locale, alle ore 00:05 del 15.05.2025 sempre tramite SCA ossia mediante inserimento dell'ID biometrico (fattore di inerenza) nell'app del ricorrente (fattore di possesso); iv) le operazioni dispositive sono state autorizzate mediante inserimento del codice PIN (fattore di conoscenza) al ricevimento della notifica push in app (fattore di possesso); v) dalla denuncia non risulta che il ricorrente abbia effettuato qualche verifica preventiva o contestuale del numero telefonico dal quale ha ricevuto le chiamate, facendo pieno affidamento su quanto gli veniva riferito dai frodatori. L'intermediario chiede il rigetto del ricorso.

DIRITTO

Il ricorrente chiede il rimborso delle somme oggetto di n. 3 pagamenti disconosciuti, per un importo complessivo di € 10.047,13. Le operazioni contestate sono state effettuate sotto la vigenza del d.lgs. 11/2010, così come modificato dal d.lgs. 218/2017, che ha recepito la nuova Direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015 (c.d. PSD 2). In data 14.05.2025, il ricorrente ha ricevuto una notifica da parte dell'app bancaria del resistente, a cui è collegata una carta prepagata, nella quale si chiedeva di accettare un pagamento di circa € 200,00 che egli non autorizzava; poco dopo il cliente ha ricevuto una chiamata da un numero fisso apparentemente riconducibile all'intermediario resistente, nel corso della quale il presunto operatore ha informato il ricorrente di un tentativo di frode informatica a valere sulla carta emessa dal resistente (produce relativo screenshot). Subiva quindi una perdita di € 10.047,13 a seguito delle varie operazioni fraudolente. Dalle risultanze in atti non risulta quando è intervenuto il blocco della carta di pagamento emessa dal resistente. L'intermediario sostiene che le operazioni sono state regolarmente autenticate mediante doppio fattore di autenticazione. A tal riprova ha allegato i log informativi relativi all'accesso in app e alle operazioni disconosciute.

Si fa presente che la frode ha avuto inizio con una chiamata proveniente da un numero riconducibile all'intermediario resistente alla quale hanno fatto seguito ulteriori chiamate apparentemente riconducibili ad un intermediario terzo (la banca X). Lo screenshot registro chiamate prodotto dal ricorrente conferma che il numero di telefono chiamante era riconducibile al servizio clienti della banca resistente. Nella vicenda in esame, è lo stesso ricorrente a dichiarare di aver ricevuto una chiamata apparentemente proveniente dalla banca resistente che comunicava "un tentativo di accesso fraudolento". Il sedicente operatore della banca induceva il ricorrente a fornirgli i "codici di accesso al servizio home banking". Tuttavia, appare significativa la circostanza per cui la frode sembra essersi configurata alla stregua di un'ipotesi, più specifica, di c.d. vishing caller ID. In particolare, il ricorrente produce lo screenshot della schermata dello smartphone contenente i riferimenti della chiamata truffaldina, da cui si evince che il numero di telefono corrisponde a quello del servizio clienti dell'intermediario. In simili ipotesi, l'orientamento prevalente tra i Collegi territoriali dell'ABF ravvisa un concorso colposo delle parti, imputando all'intermediario la colpa di "non avere adottato tutti i presidi di sicurezza necessari a impedire che il truffatore potesse chiamare la cliente con un numero riferibile all'intermediario medesimo" (così Collegio di Milano, decisione n. 17467/2021). Si richiede a tal fine solo l'allegazione da parte del ricorrente della lista delle chiamate ricevute, onde poter verificare la corrispondenza del numero utilizzato dal truffatore con il numero verde dell'intermediario (così Collegio di Milano, decisione n. 22105/2021). La frode, così congegnata, non sembra in effetti differire in

maniera significativa dalle ipotesi di “spoofing”, ossia dalle ipotesi di smishing in cui il messaggio “esca” reca, quale mittente, la denominazione dell’intermediario, in modo tale che il testo si inserisca, nei moderni smartphone, all’interno della conversazione contenente messaggi genuini (effettivamente provenienti dall’intermediario). E, secondo la più recente posizione condivisa dai Collegi territoriali dell’ABF, nelle fattispecie di spoofing è al più ravvisabile “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” (in questi termini v., per esempio, Collegio di Roma, decisione n. 1625/2022). Tenuto conto di tutti i suddetti elementi di fatto e delle previsioni richiamate del d.lgs. n. 11 del 2010, il Collegio accerta una responsabilità dell’intermediario resistente, in concorso con il comportamento gravemente negligente del cliente, per i danni derivanti dal compimento delle operazioni di pagamento non autorizzate e dispone che l’intermediario corrisponda alla parte ricorrente l’importo di euro 4.000,00, a titolo di risarcimento del danno determinato in via equitativa.

PER QUESTI MOTIVI

Il Collegio, in parziale accoglimento del ricorso, dispone che l’intermediario corrisponda alla parte ricorrente la somma di euro 4.000,00, 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