

COLLEGIO DI ROMA

composto dai signori:

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

Relatore MASSIMO CARATELLI

Seduta del 28/10/2025

FATTO

La controversia verte sulla contestazione di alcuni addebiti operati a valere su due distinti strumenti di pagamento intestati al proponente e rilasciati dalla convenuta.

In particolare, in base alla dinamica riferita da parte attrice, l'istante – in data 17 marzo 2024, alle ore 18.00 – riceveva una mail in apparenza riferibile alla resistente, che lo invitava a verificare il corretto funzionamento delle sue carte cliccando sul link in essa contenuto. Seguendo le istruzioni, il cliente veniva reindirizzato su un sito che gli chiedeva di inserire “*vari pin*”. Subito dopo, il proponente riceveva dei messaggi relativi a due addebiti non autorizzati, rispettivamente di euro 451,90 ed euro 450,00, eseguiti uno con la carta di credito e l'altro con carta di debito. Avvedutosi di essere stato truffato, il cliente contattava il numero verde della banca, sporgeva denuncia e disconosceva formalmente tali operazioni, con esito negativo. Tanto premesso, il ricorrente invoca il rimborso delle somme fraudolentemente sottratte.

Con le controdeduzioni parte convenuta precisa che parte attrice è contitolare di un conto corrente, abilitato al servizio di home banking. Al contempo, l'istituto di credito fa presente che per accedere ai propri servizi online è richiesto l'inserimento simultaneo di password statiche e dinamiche, cioè il codice titolare (password statica), il codice PIN (password statica) e il codice O-Key (vale a dire il codice OTP, ossia la password dinamica). Una volta collegati al servizio online, per autorizzare le operazioni dispositive è necessario un nuovo codice dinamico OTP, generato via APP ovvero via SMS. Nel caso di specie – alle ore 18.17 del 17 marzo 2025 – vi è stato l'enrollment di un nuovo device, autorizzato mediante inserimento del codice dinamico OTS, inviato via SMS al numero certificato del ricorrente. L'operazione di enrollment è stata comunicata a parte attrice anche tramite notifica push sul suo device.

Successivamente, alle ore 18.19, è stato registrato un accesso da App dal device del truffatore, autorizzato mediante fattore biometrico. Alle 18.20 e alle 18.27 sono stati autorizzati i pagamenti di euro 450,00 ed euro 451,99 con il codice OTP, previa autenticazione mediante fattore biometrico. Per ciascuna operazione è stato inviato un SMS alert al numero certificato del proponente. Quanto alla colpa grave, dalle dichiarazioni del cliente emerge che quest'ultimo ha inserito le proprie credenziali e il codice OTS necessario per l'enrollment del nuovo device in un sito raggiunto cliccando nel link contenuto in una e-mail ricevuta da un indirizzo non riconducibile all'intermediario. Il ricorrente, altresì, non ha prestato attenzione all'avvertimento contenuto nell'SMS in cui era riportato il codice necessario per l'enrollment del nuovo dispositivo, inviato al suo cellulare certificato. Tutto ciò premesso, l'istituto di credito chiede, quindi, all'Arbitro di dichiarare inaccoglibile la richiesta restitutoria oggetto del presente ricorso, in quanto immotivata ed infondata. In subordine, la convenuta invoca una ripartizione della colpa tra le parti ai sensi dell'art. 1227, commi 1 e 2 c.c., con riconoscimento della franchigia di euro 50,00.

DIRITTO

Ai fini della decisione, vanno anzitutto considerate quali siano le eventuali responsabilità ascrivibili alle parti, alla luce dei criteri indicati dal d.lgs. 27 gennaio 2010, n. 11, che regola la materia dei servizi di pagamento nel mercato interno, così come modificato dal d.lgs. 15 dicembre 2017, n. 218, che ha recepito la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio del 25 novembre 2015 (c.d. "PSD 2").

Ciò posto, considerati i fatti così come ricostruiti in atti, occorre anzitutto rilevare che le operazioni in contestazione sono state eseguite tramite i servizi dispositivi associati ad un rapporto di conto corrente, di cui è cointestatario il proponente.

L'intermediario ha offerto riscontro del procedimento seguito per l'enrollment di un nuovo dispositivo, così come per autorizzare le operazioni disconosciute, producendo i relativi log, con buon fine della digitazione dei codici. Ne consegue questo Arbitro che il sistema di autenticazione adottato in fase di enrollment e dispositiva appare in grado di garantire un elevato livello di sicurezza (cfr. Collegio di Roma, decisione n. 8530/2021).

Peraltro, non si rilevano nella documentazione prodotta dalle parti riscontri che lascino supporre qualche malfunzionamento del sistema di parte resistente durante il processo dispositivo.

Dalla documentazione agli atti, si evince altresì che parte attrice ha dato seguito a una comunicazione ricevuta via e-mail, contenente la richiesta di accedere ad un link.

Pertanto, il Collegio rileva come, nel caso di specie, l'intrusione non autorizzata nel sistema – lungi dall'essere causata da un insufficiente grado di protezione informatica del servizio offerto dall'intermediario – appare ascrivibile a colpa grave del cliente, incappato in un caso di "phishing", con conseguente utilizzo abusivo delle sue credenziali di accesso (cfr. Collegio di Roma, n. 16837/2021). Avendo riguardo alle circostanze del caso concreto, ritiene inoltre questo Arbitro – in linea con la decisione n. 3498/2012 del Collegio di Coordinamento – che il proponente sia vittima di colpevole credulità, risultando *"tali forme di accalappiamento" "ormai note al pur non espertissimo navigatore di internet"*.

Il ricorrente ha, peraltro, dimostrato scarsa attenzione rispetto agli avvisi che pervenivano sul suo cellulare. Ne sono prova evidente, ad esempio, le notifiche trasmesse dalla banca al momento

dell'attivazione del nuovo mobile token e che non hanno sollecitato l'utente a prestare maggior cautela al proprio operato (cfr. Collegio di Roma, decisione n. 16564/2021).
In relazione a quanto precede, il ricorso non può, pertanto, essere accolto.

PER QUESTI MOTIVI

Il Collegio respinge il ricorso.

IL PRESIDENTE