

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) BILOTTI	Membro di designazione rappresentativa degli intermediari
(RM) FULCHERI	Membro di designazione rappresentativa dei clienti

Relatore FABRIZIO MAIMERI

Seduta del 24/04/2026

FATTO

Con ricorso prot. n. del 30.10.2025, parte attrice dichiara che il 18.8.2025, alle ore 7:15, ha trovato nella propria casella di posta elettronica due *e-mail* provenienti dall'intermediario resistente: la prima *e-mail* delle ore 2:42 comunicava l'avvenuto cambio di indirizzo di posta elettronica; non avendo autorizzato detta variazione, ha effettuato accesso *all'app* bancaria e ha avviato il ripristino della *e-mail*; alle ore 7:25 ha ricevuto il codice OTP necessario per autorizzare il cambio indirizzo *e-mail*, completato

alle ore 7:28 mediante l'inserimento del secondo codice OTP; a seguito dell'inserimento dei codici richiesti, alle ore 7:31 ha ricevuto la conferma dell'avvenuto cambio dell'*e-mail*. Ha poi appurato l'esistenza di una seconda *e-mail* ricevuta alle ore 2:44, con la quale l'intermediario ha comunicato al ricorrente il cambio di recapito mobile; non avendo autorizzato detta variazione, ha provveduto immediatamente al ripristino del proprio numero di telefono, mediante l'inserimento di n. 3 codici OTP. Ha poi provato a contattare il servizio clienti con esito negativo: gli veniva infatti comunicato che avrebbe potuto farlo in data 16.8.2025.

Nella medesima giornata, verso le ore 15:15 ha notato la presenza di n. 4 notifiche inviate dalla banca resistente alla sua casella di posta elettronica, con le quali le veniva comunicata l'avvenuta esecuzione di un bonifico istantaneo di € 4.430,00, effettuato a favore di un beneficiario sconosciuto alle ore 14:53 del 15.8.2025; una *mail* successiva ha informato il ricorrente della disposizione di un secondo bonifico di € 4.270,00 a favore di un beneficiario sconosciuto, alle ore 14:57 del 15.8.2025; una terza comunicazione lo informava di un bonifico di € 3.020,00 disposto alle ore 15:01 del 15.8.2025 e di un quarto bonifico di € 1.590,00; alle ore 15:12, ha ricevuto una *e-mail* di dubbia provenienza, con la quale le si chiedeva di aggiornare alcuni dati personali per la sicurezza del conto; dubitando della genuinità della comunicazione ricevuta, non ha eseguito quanto richiesto; alle ore 15:13 ha ricevuto una *e-mail* ed un *sms* con i quali le è stato comunicato l'avvenuto blocco del conto corrente per motivi di sicurezza. Ha effettuato l'accesso all'*app* della banca ed ha constatato che era stato pagato solo il primo bonifico fraudolento di € 4.430,00, eseguito alle ore 14:53, mentre gli ulteriori bonifici sono stati bloccati dalla banca. Alle ore 15:15 ed alle ore 16:16 del 16.8.2025 ha tentato di contattare senza successo il servizio clienti. Il 17.8/2025, alle ore 15:12, ha effettuato l'accesso all'*app* della banca al fine di modificare il proprio PIN, ma non gli è stato possibile. In quest'occasione ha potuto constatare che l'*app* della banca multicanale risulta attiva su due *smartphone* a lui sconosciuti, che ha prontamente rimosso. Chiede il rimborso di € 4.430,00.

In sede di controdeduzioni, l'intermediario espone che il ricorrente, titolare di un conto corrente, disconosce un'operazione di bonifico istantaneo di € 4.430,00 eseguita in data 15.8.2025; la banca adotta un sistema di autenticazione forte di accesso all'Area Riservata e di autorizzazione delle disposizioni di pagamento nel pieno rispetto delle previsioni normative. Il 13.8.2025 è stata registrata l'installazione dell'*app* bancaria su un *device* diverso da quello in uso al cliente; per completare suddetta operazione, occorre inserire un codice di 7 cifre (c.d. codice cliente) assegnato dalla banca al cliente al momento della conclusione del contratto, la data di nascita ed il codice PIN (elemento di conoscenza); per attivare l'*app* è previsto l'inserimento di un codice OTP inviato al numero di telefono del cliente (elemento di possesso); dunque, è verosimile che il cliente abbia comunicato il codice PIN e il codice OTP ricevuto tramite *sms* così consentendo l'installazione dell'*app* bancaria su un nuovo dispositivo, di cui è stata data notizia al cliente via *e-mail*; l'operazione oggetto del presente ricorso è stata disposta dal nuovo *device* collegato al conto corrente del ricorrente.

Il ricorrente nulla riferisce in merito ai fatti occorsi nelle giornate del 13 e del 15.8.2025, limitandosi a disconoscere l'operazione oggetto di doglianza e la variazione del recapito cellulare intervenuta in data 15.8.2025; egli ha consentito all'installazione dell'*app* su un diverso dispositivo, violando il dovere di tenere un comportamento idoneo a garantire la sicurezza del dispositivo ed il suo utilizzo; il ricorrente ha ricevuto in data 13.8.2025 una notifica *alert* relativa all'installazione dell'*app* su nuovo dispositivo ed avrebbe potuto in quell'occasione bloccare l'installazione, posto che il bonifico fraudolento è stato eseguito due giorni dopo. Il bonifico istantaneo oggetto del presente procedimento è stato correttamente eseguito mediante autenticazione forte. Chiede il rigetto del ricorso.

In sede di repliche, il ricorrente dichiara che il 13.8.2025, ha ricevuto una *mail* che ha ritenuto fraudolenta in quanto presentava immagini e messaggi ingannevoli; tale *mail* gli comunicava l'installazione dell'*app* su nuovo dispositivo, senza però informarlo del tipo o modello di dispositivo installato; ha dunque abilitato la sua impronta digitale quale elemento di accesso alla *app*; è evidente, dunque, che i frodatori sono venuti a conoscenza dei codici di accesso all'*app* e di autenticazione a causa di un mal funzionamento del sistema operativo dell'intermediario. Non ha potuto contattare il servizio clienti in data 15.8.2025 in quanto si trattava di un giorno festivo. Insiste per il rimborso di € 4.430,00.

In sede di controrepliche, l'intermediario reitera le difese già svolte.

In relazione alle rispettive argomentazioni, il ricorrente chiede all'Arbitro «il rimborso integrale della somma sottratta di € 4.430,00». Dal canto suo, l'intermediario chiede al Collegio «di respingere il ricorso, in quanto infondato».

DIRITTO

La controversia ha ad oggetto l'esecuzione di un bonifico istantaneo di € 4.430,00 eseguito in data 15.8.2025 alle ore 14:53. Si tratta dell'unico bonifico andato a buon fine (il primo) perché i tre successivi sono stati bloccati dalla Banca.

Circa la corretta autenticazione delle operazioni effettuate, la banca documenta anzitutto le modalità con cui è avvenuto l'*enrollment* del nuovo *device*. Essa è avvenuta in data 13.8.2025 alle ore 11:58, sullo *smartphone* da cui è stato poi eseguito il bonifico fraudolento. L'intermediario fa presente che l'*enrollment* avviene inserendo: il codice cliente (codice composto da 7 cifre che viene assegnato dalla Banca al cliente al momento della conclusione del contratto) e la data di nascita; il codice PIN (fattore di conoscenza); il codice OTP (fattore di possesso).

Dopo aver scaricato ed installato l'*app*, sono stati inseriti (e l'inserimento è documentato) per l'appunto il codice cliente, la data di nascita e il codice PIN; infine, è stato inviato il codice OTP via *sms* sul numero di cellulare del ricorrente alle ore 11:57; questo codice è stato inserito alle ore 11:58 con esito positivo (*status*: "SUCCESS", "VALIDATED"). Pertanto, la fase di *enrollment* è avvenuta conformemente a SCA, con doppio fattore di autenticazione.

L'intermediario ha prodotto anche le evidenze relative alla fase di accesso all'*app* bancaria attiva sul nuovo dispositivo associato, propedeutica alla disposizione di pagamento, avvenuto alle ore 14:50 del 15.8.2025. L'accesso è stato validato con l'inserimento del PIN (cfr. "MPIN"). Pertanto, la fase di accesso in *app* risulta avvenuta con doppio fattore di autenticazione ossia l'*app* bancaria (fattore di possesso) e l'inserimento del codice PIN (fattore di conoscenza).

Quanto alla fase dispositiva, l'intermediario ha prodotto un *log* da cui risulta che l'operazione è avvenuta in *app* bancaria (fattore di possesso) con inserimento di PIN (fattore di conoscenza), alle ore 14:53 del 15/08/2025.

Pertanto, dalla documentazione in atti, è stata fornita evidenza del corretto funzionamento della SCA in relazione a tutte le operazioni interessate dalla truffa lamentata dal ricorrente.

In base a quanto emerge dalla denuncia e dalle ulteriori evidenze in atti, la truffa ai danni del ricorrente è iniziata il 13.8.2025 alle ore 11.58, quando egli ha ricevuto una *e-mail* (genuina) con la quale gli è stata comunicata l'installazione dell'*app* bancaria su un nuovo dispositivo: tuttavia, egli non chiarisce come la frode abbia avuto inizio, limitandosi a dichiarare di aver ritenuto fraudolenta l'*e-mail* in

questione e di non averle dato seguito; si tratta invece di una *e-mail* genuina, che l'avvertiva dell'installazione del nuovo *device*.

In presenza della SCA, la scarsa contestualizzazione dei fatti assume rilievo nella valutazione della colpa grave del ricorrente: questi è tenuto ad allegare i fatti dai quali presumere che l'operazione di pagamento è stata disposta da un terzo non autorizzato. In caso contrario, l'Arbitro valuta negativamente la scarsa contestualizzazione dei fatti da parte del ricorrente e riconosce, in capo a costui, «un onere di allegazione delle circostanze che possano, al minimo, offrire una attendibile ipotesi alternativa rispetto a quella, altrimenti residuale (ed anzi unica), dell'utilizzo imputabile (direttamente o per colpa grave) al titolare» (Collegio di Roma, decisione n. 10723/2019). Recentemente, questa posizione è stata ribadita dal medesimo Collegio con decisione n. 1319/2025: «secondo l'orientamento condiviso dai Collegi territoriali, le mancate allegazioni del cliente sulle circostanze di fatto della frode rappresentano un elemento da cui l'Arbitro può trarre il proprio convincimento, insieme ad altre circostanze, circa la colpa grave del ricorrente, qualora l'intermediario abbia offerto la prova dell'autenticazione delle transazioni sconosciute (cfr. Collegio di Roma, decisione n. 11050/2024). (...) Tanto premesso, in assenza di elementi idonei a contestualizzare l'evento truffaldino, questo Collegio ritiene di respingere la richiesta restitutoria del proponente, desumendone la colpa grave, in linea con quanto già espresso con la decisione n. 23474/2021, per cui "[l']assoluta carenza di allegazione da parte del cliente rende eccessivamente generica la rappresentazione del fatto costitutivo della pretesa restitutoria, che legittima la veridicità dell'ipotesi dell'utilizzo dello strumento di pagamento imputabile per colpa grave al titolare».

La condotta del ricorrente, come dal medesimo riferita, dà adito a qualche perplessità. Egli dichiara di aver preso contezza della frode solo in data 18.8.2025 quando al suo risveglio verso le ore 7:31 avrebbe trovato due *e-mail* provenienti dall'intermediario resistente: la prima delle ore 2:42 lo informava del cambio di indirizzo *e-mail* e la seconda delle ore 2:44 del cambio di numero di telefono. Tuttavia, l'*e-mail* relativa alla modifica dell'indirizzo *e-mail* e del numero di telefono sono state ricevute in data 15.8.2025. Il ricorrente ha ricevuto l'*e-mail* relativa alla disposizione del bonifico istantaneo di € 4.430,00 alle ore 14:53 del 15.8.2025; tra le ore 14:57 e le ore 15:01, ha ricevuto ulteriori *e-mail* mediante le quali l'intermediario comunicava la mancata esecuzione di ulteriori tre bonifici istantanei, per un totale di € 8.880,00; alle ore 15:13, ha ricevuto un'ultima *e-mail* ed un *sms*, mediante i quali veniva informato che il suo conto era stato bloccato automaticamente per motivi di sicurezza. Il sistema di *sms alert* è risultato funzionante e il ricorrente è stato minutamente informato delle vicende del suo conto; così come è stato dimostrato che il conto corrente è stato bloccato automaticamente per motivi di sicurezza in data 15.8.2025, alle ore 15:13 (cioè dopo venti minuti rispetto all'operazione fraudolenta), avendo la banca bloccato l'esecuzione dei bonifici fraudolenti successivi al primo.

Come già detto, il ricorrente non descrive né in denuncia né nel ricorso la modalità in cui si è realizzata la frode; in particolare, dichiara di essersi accorto dell'operazione fraudolenta in data 18.8.2025, visualizzando l'*e-mail* di conferma di esecuzione del bonifico istantaneo ricevuta sul suo telefono. Il Collegio di Roma riconosce, in capo al ricorrente, «non tanto un onere probatorio che la legge, in principio, non gli addossa, ribaltandolo piuttosto sull'intermediario; quanto piuttosto un onere di allegazione delle circostanze che possano, al minimo, offrire una attendibile ipotesi alternativa rispetto a quella, altrimenti residuale (ed anzi unica), dell'utilizzo imputabile (direttamente o per colpa grave) al titolare»: decisione n.10723 del 18.4.2019. Il Collegio ritiene, dunque, che, in caso di disconoscimento dell'operazione, è onere del ricorrente fornire «elementi utili a provare che l'operazione sia stata realmente fraudolenta»: decisione n. 299 del 10.1.2020).

Collegio di Roma, decisione n. 8058/2022: «il sistema descritto dall'intermediario è conforme a SCA, e così l'operazione controversa risulta effettuata attraverso i passaggi previsti da questo sistema, senza anomalie. Un sistema che procede solo se vengono inserite correttamente le credenziali statiche e dinamiche di cui sopra. Il ricorrente nega di averle fornite a terzi, ma né in sede di querela, né nel ricorso offre elementi idonei a contestualizzare l'evento truffaldino, che renderebbe possibile una ricostruzione alternativa rispetto all'ipotesi di una sua comunicazione delle credenziali ai truffatori. Posto che le regole che impongono agli operatori stringenti requisiti di sicurezza sull'autenticazione e sull'autorizzazione dei pagamenti, come risulta essere quello adottato dall'intermediario resistente (anche) per l'operazione qui contestata, hanno la funzione di offrire la massima sicurezza possibile per le operazioni di pagamento, è evidentemente onere di chi allega un'anomalia nel funzionamento provarla. Tuttavia, in assenza di elementi idonei a contestualizzare l'evento truffaldino, questo Collegio ritiene di respingere la richiesta restitutoria del ricorrente, desumendone la colpa grave».

PER QUESTI MOTIVI

Il Collegio respinge il ricorso.

IL PRESIDENTE