Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

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

Relatore FABRIZIO MAIMERI

Seduta del 09/12/2025

FATTO

Con ricorso del 28.3.2025, parte attrice riferisce che, il 13.11.2024 intorno alle 14:00, ha ricevuto un *sms* che la allertava di alcuni bonifici non autorizzati e preannunciava la chiamata di un operatore della Banca. Effettivamente, poco dopo ha ricevuto una chiamata da un numero apparentemente riconducibile alla Banca: il sedicente operatore le ha chiesto di accedere al proprio conto. Il ricorrente ha eseguito le istruzioni e si è reso conto che nell'area privata venivano effettuate movimentazioni da remoto; successivamente, il sedicente operatore ha chiesto di autorizzare le operazioni nel frattempo svolte. Parte attrice disconosce cinque bonifici: due a favore dell'IBAN ***598 per € 2.490,00 e € 4.990,00 e tre a favore dell'IBAN ***334 per € 2.490,00, € 2.490,00 ed € 4.990,00; ravvisa responsabilità della Banca, i cui sistemi non hanno rilevato l'anomalia delle operazioni; in particolare, sostiene di non aver utilizzato in passato il bonifico istantaneo quale mezzo di pagamento. Chiede il rimborso integrale della somma sottratta.
In sede di controdeduzioni, l'intermediario ha riconosciuto € 6.650,00, pari ad 1/3 dell'importo frodato, come da accredito eseguito il 25.11.2024. Le operazioni disconosciute risultano essere state eseguite senza anomalia alcuna, personalmente dal ricorrente e risultano correttamente assistite dalla SCA. Il cliente ha attivato il servizio *token* il 14.9.2021 su di uno *smartphone* al quale vengono inviate tutte le *push*. Per poter accedere all'area riservata tramite *web* occorre che (i) il cliente digiti il proprio codice cliente e la propria data di nascita; (ii) le verifiche su codice cliente e data di nascita diano esito positivo e il processo di autenticazione prosegua mostrando un tastierino sul quale digitare le tre cifre del PIN richieste. Alle 14:20:43 il sistema prepara la *push* per autorizzare l'accesso all'area riservata e alle 14:21 il cliente autorizza l'accesso all'area medesima dall'*app* attraverso l'impronta digitale (*TouchID*). I l processo di autenticazione si è completato correttamente, tutti i controlli hanno dato esito positivo e

alle 14:21 la banca ha registrato nei suoi archivi l'avvenuto accesso all'area riservata da *web*. Anche i bonifici risultano essere stati effettuati tramite autenticazione forte, attraverso *push* ricevuta sul *device* del cliente.
Ravvisa colpa grave dell'utente per aver consentito il controllo da remoto del proprio pc, violando il dovere di tenere custodite le credenziali e per aver autorizzato personalmente i bonifici. Il cliente riferisce egli stesso di aver ricevuto il primo *sms* c.d. "civetta" da numero di telefono non riconducibile ad alcuno dei contatti ufficiali della Banca. Orbene, tali elementi, valutati complessivamente, consentono di ritenere provata la sussistenza di una colpa grave in capo al cliente e, pertanto, di ritenere congruo il riconoscimento dell'importo pari ad 1/3 dell'importo complessivo a titolo di ristoro, già accreditato il 25.11.2024. Chiede, quindi, il rigetto del ricorso.
In sede di repliche, il ricorrente ravvisa responsabilità della banca che non ha protetto il numero con il quale contatta i propri utenti. Perciò, nel momento in cui è stato chiamato dal servizio Clienti della banca, ha creduto in buona fede di parlare realmente con essa. Inoltre, le operazioni autorizzate, cioè bonifici istantanei, normalmente non possono essere eseguiti immediatamente se i destinatari non sono presenti nella rubrica o se non sono già stati oggetto di bonifici precedenti. Quindi per eseguire tali operazioni ipotizza che i truffatori abbiano forzato il sistema a prescindere dalle autorizzazioni fornite.
Infine, fa presente il comportamento contraddittorio della banca che, da un lato, ravvisa colpa grave dell'istante e, dall'altro, restituisce un importo pari a 1/3 della somma frodata.
In sede di controrepliche, l'intermediario si riporta alle controdeduzioni.
In relazione alle rispettive argomentazioni, il ricorrente chiede all'Arbitro di essere «risarcito della cifra totale sottratta e non solo dei 6700 euro che mi hanno dato non si sa bene a quale titolo». Dal canto suo, l'intermediario chiede al Collegio il rigetto del ricorso.

DIRITTO

La controversia ha ad oggetto il disconoscimento di cinque bonifici istantanei eseguiti il 13.11.2024, due a favore di un beneficiario e tre ad altro nominativo. Dalla ricostruzione in atti emerge che il ricorrente ha fatto accesso alla *home banking* e in seguito ha concesso il controllo da remoto al truffatore, che verosimilmente ha inserito i dati dei bonifici.
Per dimostrare la SCA in relazione all'accesso all'area riservata, l'intermediario produce i relativi *log* e l'accesso medesimo viene confermato con biometria sulla notifica *push* ricevuta sul *device* del ricorrente.
Anche i bonifici risultano effettuati tramite autenticazione forte: il cliente ha ricevuto la *push* sul suo *smartphone*, del quale solo lui è in possesso (conoscenza) e ha autorizzato le operazioni attraverso i suoi dati biometrici (inerenza). Vengono anche a questo riguardo riportati i *log* e il sistema di autenticazione predisposto dall'intermediario per l'esecuzione dell'operazione è stato ritenuto *compliant* alla SCA da Collegio di Roma, decisione n. 19734/2021: «l'intermediario ha fornito evidenza, tramite i relativi *log* informatici dell'avvenuta autenticazione dell'operazione in contestazione tramite inserimento del codice CVV riportato sul retro della carta nonché mediante l'utilizzo di un doppio fattore, e cioè tramite *mobile token* che consiste in un'*app* installata sul cellulare del cliente, sulla quale compare un messaggio di richiesta di autorizzazione, cui il cliente deve dare conferma – nonché inserimento dello *s***code*/codice biometrico, che consiste in un codice scelto dal cliente e solo da questi conosciuto, oppure dall'impronta digitale o *Face Id*. (…) Difatti l'operazione in questione è stata comunque correttamente autenticata secondo i requisiti richiesti per la *strong customer authentication* , nel caso di specie mediante un fattore di conoscenza noto solo al cliente (*s*code*/codice biometrico) e un fattore di possesso (*app* generatrice del *mobile token*)».
Il 13.11.2024 il ricorrente ha ricevuto una chiamata da un numero apparentemente riconducibile alla banca (come afferma in denuncia), ma dal registro chiamate versato in atti non risulta il numero telefonico, ma solo l'intestazione. Nella riunione del 25.9.2025, il Collegio ha disposto integrazione istruttoria, chiedendo al ricorrente di produrre «le schermate relative al registro chiamate del giorno della truffa, che riportino il numero indicato in denuncia, nonché copia dell'*sms* fraudolento». Con nota

del 29.9.2025 il ricorrente ha riscontrato la richiesta producendo però *screenshot* che non recano il numero chiamante, ma solo l'intestazione della Banca. Ed è noto che solo qualora venga effettivamente riscontrato un caso di *vishing callerID*, fattispecie considerata una frode più insidiosa, i Collegi individuano un concorso colposo delle parti: ma qui questa tipologia di frode non può essere riscontrata, in assenza di ogni prova adeguata della riconducibilità all'intermediario dei numeri telefonici adoperati dai truffatori.

C'è ancora un altro elemento che conduce alla imputabilità della vicenda esame alla responsabilità del ricorrente ed è costituito dalla circostanza per cui la frode risulta attuata tramite controllo remoto, circostanza in presenza della quale i Collegi sono soliti affermare di norma la colpa grave del ricorrente (cfr. Collegio di Milano, decisione n. 196/2023): «in simili fattispecie, questo Arbitro riconosce la colpa grave dell'utente che, su indicazione del frodatore, installi un'applicazione "la cui funzionalità risiede […] nel permettere l'accesso ed il controllo di pc e *smartphone* da remoto", consentendo in tal modo al frodatore di agire indisturbato e disporre i pagamenti (cfr. Collegio di Roma, decisione n. 7806/2023)»: così Collegio di Roma, decisione n. 4317/2024.

Il ricorrente, infine, contesta l'esecuzione di cinque bonifici istantanei e ravvisa responsabilità dell'intermediario per non aver rilevato l'anomalia delle operazioni. Secondo l'istante, infatti, la banca avrebbe dovuto predisporre un sistema di monitoraggio in grado di bloccare le operazioni. L'art. 2 del Regolamento delegato n. 839/2018 prevede un monitoraggio *ex post* sulle operazioni di pagamento mentre non prevede, di contro, un obbligo di monitoraggio delle operazioni in tempo reale (se non nei casi in cui l'intermediario voglia avvalersi della esenzione SCA), come chiarito dalla Q&A dell'EBA n. 4090/2018. In ogni caso, occorre valutare che i bonifici istantanei sono irrevocabili e quindi, una volta ordinati, non più eliminabili.

Tuttavia, nel caso concreto, l'intermediario deve aver ritenuto di aver avuto una qualche responsabilità nell'esecuzione della truffa e per questa ragione ha ritenuto opportuno corrispondere una somma, pari a 1/3 dell'importo disconosciuto, a titolo di concorso di colpa. Il Collegio ritiene che il ricorrente non abbia più nulla a pretendere dalla Banca, oltre alla somma che ha già ricevuto.

PER QUESTI MOTIVI

Il Collegio respinge il ricorso.

IL PRESIDENTE