Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(MI) BALDINELLI	Membro designato dalla Banca d'Italia
(MI) PERON	Membro di designazione rappresentativa degli intermediari
(MI) CESARE	Membro di designazione rappresentativa dei clienti

Relatore FABIO CESARE

Seduta del 17/12/2024

Esame del ricorso n. 1980322 del 10/10/2024

proposto da [redacted]

nei confronti di [redacted]

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(MI) BALDINELLI	Membro designato dalla Banca d'Italia
(MI) PERON	Membro di designazione rappresentativa degli intermediari
(MI) CESARE	Membro di designazione rappresentativa dei clienti

FABIO CESARE

17/12/2024

FATTO

La ricorrente riferisce quanto segue. Afferma di essere titolare di un conto corrente cointestato con la persona che aderisce al ricorso. Uno dei cointestatari riceveva un sms che lo avvisava di un pagamento su un sito non autorizzato; provava infruttuosamente a chiamare il numero indicato nell'sms stesso per bloccare l'operazione; riceveva quindi una chiamata da un numero apparentemente riferibile alla banca convenuta da parte di un operatore che si presentava come appartenente al servizio antifrode dell'intermediario e chiedeva di bloccare immediatamente le operazioni fraudolente.
Appurata la genuinità della chiamata dopo il confronto tra il numero di telefono chiamante e quello dell'intermediario, la ricorrente seguiva le indicazioni dell'operatore, il quale riferiva che era in corso un bonifico di importo pari a € 1.500,00 in favore di tale C** F** e che per bloccare la frode in corso, era necessario resettare la password dell'applicazione R** Banking mediante conferma del banner di notifica proveniente dalla stessa.
Eseguite le istruzioni impartite dal finto operatore, la cliente riceveva due sms dall'utenza telefonica ***006, che indicavano rispettivamente che l'operazione e il bonifico erano stati correttamente bloccati.
I cointestatari si avvedevano di essere stati vittima di una truffa quando contattavano il servizio clienti e apprendevano che erano stati eseguiti, a loro insaputa, due bonifici del

valore di € 1.500,00 ciascuno; presentavano pertanto reclamo all'intermediario che lo rigettava.
La ricorrente e l'aderente chiedono pertanto la restituzione dell'importo di € 3.000,00.
L'intermediario replica chiedendo la declaratoria di inammissibilità per difetto di legittimazione attiva per mancanza di identità soggettiva tra il ricorrente e il soggetto leso dalla frode, in quanto il ricorso è a nome della sig.ra F** F**, cointestataria del conto corrente, e il soggetto a cui sono riferiti i fatti è il sig. P** P**, il quale non ha sottoscritto la dichiarazione di adesione; nel merito riferisce che l'operazione risulta contabilizzata in assenza di anomalie e autorizzata mediante corretta autenticazione del sistema; sarebbe pacifico che lo stesso cliente abbia autorizzato personalmente le operazioni seguendo le istruzioni del frodatore. Dalla ricostruzione dei fatti, emerge poi un comportamento gravemente colposo del cliente, essendo l'evento fraudolento riconducibile esclusivamente alla condotta dello stesso, e pertanto chiede il rigetto della domanda.

DIRITTO

Il caso all'esame del collegio riguarda due operazioni disconosciute di € 1.500,00 ciascuna.
Va anzitutto precisato che il procuratore delle parti ha sottolineato che il ricorso con cui è stato instaurato il presente procedimento è stato proposto nell'interesse della sig.ra F** F** e del sig. P** P**, entrambi parti ricorrenti hanno conferito procura e pertanto deve essere superata l'eccezione di legittimazione attiva sollevata dall'intermediario.
Le operazioni contestate rientrano nell'ambito di applicazione della disciplina del D. Lgs. 27/1/2010, n. 11 di recepimento della Direttiva sui servizi di pagamento come modificato dal D.Lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU (PSD 2).
La normativa richiamata ha provveduto a ripartire una serie di obblighi tra il prestatore di servizi di pagamento e l'utilizzatore di detti servizi. L'utilizzatore, in particolare, ha il dovere di utilizzare lo strumento di pagamento in conformità con i termini contrattuali, di denunciarne lo smarrimento, il furto o l'utilizzo non autorizzato appena ne viene a conoscenza e deve adottare le misure idonee a garantire la sicurezza dei dispositivi personalizzati che ne consentono l'utilizzo (ad esempio conservare adeguatamente i codici PIN). Per quanto riguarda l'intermediario, la normativa ricordata prevede, tra gli altri, l'obbligo di assicurare che i dispositivi personalizzati che consentono l'utilizzo di uno strumento di pagamento non siano accessibili a soggetti terzi.
Si richiede, pertanto, da ambedue le parti, la necessaria diligenza per evitare che lo strumento di pagamento possa essere utilizzato senza la necessaria autorizzazione o in maniera fraudolenta.
La normativa mostra un chiaro *favor* probatorio nei confronti dell'utilizzatore, in quanto l'intermediario, per liberarsi da ogni responsabilità in caso di utilizzo fraudolento dello strumento, dovrà dimostrare che l'operazione è stata autorizzata dall'utilizzatore medesimo oppure che questi abbia agito in modo fraudolento ovvero con dolo o colpa grave.
Alla luce di tali disposizioni, pertanto, due sono i passaggi ineludibili in materia. In primo luogo è l'intermediario a dover provare l'autenticazione, la corretta registrazione e contabilizzazione delle operazioni contestate, prova che comunque di per sé non è sufficiente a dimostrare il dolo o la colpa grave dell'utilizzatore. In secondo luogo, è sempre l'intermediario a dover provare tutti i fatti idonei ad integrare la colpa grave dell'utilizzatore, unica ipotesi in cui, oltre al dolo, lo stesso può patire le conseguenze dell'utilizzo fraudolento dello strumento di pagamento.

Con riferimento alla *strong customer authentication* (c.d. SCA) le fonti normative sono rinvenibili negli artt. 97 e 98 della PDS2, nell'articolo 10 bis del D. Lgs. 10/2011, nelle norme tecniche di regolamentazione emanate dall'EBA e recepite con Regolamento Delegato Ue 2018/389 della Commissione Europea, applicabile a far data dal 14 settembre 2019, nonché nei criteri interpretativi forniti dall'EBA (v. in particolare il parere dell'EBA del 21 giugno 2019). Nello specifico, l'autenticazione forte (SCA) è richiesta quando il cliente 1) accede al suo conto di pagamento online; 2) dispone un'operazione di pagamento elettronico; 3) effettua una qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi.
La SCA si realizza con il ricorso ad almeno due dei seguenti tre fattori: conoscenza; inerenza; possesso. Gli elementi devono essere reciprocamente indipendenti e appartenere a categorie diverse.
Venendo al caso di specie, i LOG riportati consentono unicamente di trarre evidenza di una *push* inviata al dispositivo della cliente, relativa all'autorizzazione dell'operazione di reset password login, riconducibile all'elemento di possesso.
Non vi è nemmeno evidenza dell'inserimento – né descrizione di quale sia – dell'ulteriore fattore di autenticazione (di conoscenza/inerenza), né se esso sia stato richiesto prima dell'invio della notifica *push* ovvero se esso sia stato richiesto per consentire all'utente di validare detta notifica.
Dalla mancata verifica dei fattori di possesso, inerenza e autenticazione discende l'accoglimento del ricorso.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 3.000,00
Il Collegio dispone inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di € 200,00, quale contributo alle spese della procedura, e alla parte ricorrente la somma di € 20,00, quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
ANDREA TINA