

COLLEGIO DI BOLOGNA

composto dai signori:

(BO) TENELLA SILLANI	Presidente
(BO) BULLO	Membro designato dalla Banca d'Italia
(BO) LEMME	Membro designato dalla Banca d'Italia
(BO) MIRABELLI	Membro di designazione rappresentativa degli intermediari
(BO) TRAVERSI	Membro di designazione rappresentativa dei clienti

Relatore LORENZA BULLO

Seduta del 23/09/2025

FATTO

Parte ricorrente espone quanto segue.

- di essere titolare della carta n***8120;
- in data 01/01/2025 riceveva sulla propria utenza telefonica una chiamata da parte del numero riconducibile al sistema antifrode dell'intermediario (***3144 – qualificato come servizio antifrode dell'intermediario) che lo avvisava dell'esecuzione di un bonifico dell'importo di €1.750,00 effettuato con la carta di sua proprietà ed insisteva affinché [parte ricorrente] si recasse a sporgere denuncia alle autorità competenti;
- ritenendo affidabile e veritiera la chiamata accedeva all'APP e constatava la disposizione di un bonifico di € 1.700,00;
- non avendo autorizzato l'operazione provvedeva a bloccare immediatamente la carta e sporgeva denuncia alle competenti autorità;
- provvedeva a recarsi presso una filiale dell'intermediario ove depositava formale reclamo che veniva riscontrato negativamente dall'intermediario;
- l'intermediario è responsabile delle operazioni fraudolente disconosciute poiché non ha garantito le autenticazioni multifattoriali recanti codici o basate sull'uso di due o più elementi.

Parte ricorrente, infruttuosamente esperito il reclamo, chiede che l'Arbitro condanni la parte resistente al rimborso della somma di euro 1750,00 illegittimamente sottrattagli, oltre ad interessi legali dalla data del fatto al saldo; chiede altresì la condanna di parte convenuta alla refusione delle spese legali pari ad euro 366,00 oltre oneri accessori e delle spese di procedura di euro 20,00.

L'intermediario resistente contro deduce quanto segue:

- al momento della materiale esecuzione della operazione oggetto di contestazione i sistemi informativi non hanno rilevato alcuna anomalia o irregolarità essendo stata disposta dietro diretta ed immediata autenticazione da parte del legittimo titolare;
- la carta di pagamento n***8120 è oggetto di enrollment al sistema autorizzativo di tipo dinamico funzionante mediante invio con sms della password dinamica sul numero di cellulare della parte ricorrente;
- in fase di log-in il ricorrente risulta essersi autenticato in App mediante autenticazione con codice P***;
- l'operazione contestata è stata eseguita con sistema dinamico di autenticazione necessitando l'utilizzo del codice P*** al ricevimento della notifica in App che riporta la descrizione in dettaglio dell'operazione per la quale è richiesta autorizzazione;
- mette a disposizione dei propri clienti il servizio di sms Alert, che è attivo di default nell'app;
- ha predisposto accorgimenti atti a tutelare il cliente sottoponendo il suo strumento di pagamento a controlli da parte del servizio antifrode e contattando tempestivamente il cliente per effettuare una verifica sulla genuinità della operazione disposta consentendo il blocco dello strumento;
- nel modulo di reclamo il cliente riferisce di aver subito il furto/smarrimento del supporto sul quale erano riportate le credenziali di sicurezza per l'utilizzo delle piattaforme online dell'intermediario. Tale evento può aver contribuito al verificarsi della frode;
- parte ricorrente non evidenzia di aver modificato tali ultime credenziali dopo l'episodio di furto/smarrimento con il conseguente incorretta gestione delle proprie credenziali;
- parte ricorrente non dichiara di aver mai ricevuto o risposto a comunicazioni truffaldine volte a carpire le credenziali di accesso ai propri strumenti di pagamento;
- dalla mancata allegazione delle circostanze della frode il Collegio può trarre il convincimento circa la gravità della negligenza;
- la richiesta di refusione delle spese legali risulta infondata in quanto il presente giudizio non richiede necessariamente l'assistenza di un legale.

Parte resistente conclude quindi chiedendo all'Arbitro di rigettare il ricorso in quanto infondato in fatto e in diritto.

Seguono *repliche e contro repliche* in forza delle quali:

- **parte ricorrente** insiste per l'accoglimento del ricorso, evidenziando quanto segue: **a)** dall'esame delle evidenze riportate dallo stesso intermediario [in sede di controdeduzioni] emerge che in data 01/01/2025 tra le ore 8:58 e le ore 18:36 ci siano stati ben 11 tentativi di effettuare la medesima operazione con diversi indirizzi IP; **b)** l'operazione contestata sarebbe stata effettuata alle ore 9:00:28; la medesima operazione compare inoltre con altri orari differenti e in particolare alle ore 9:00:26 e 9:40:30; **c)** dalle evidenze informatiche prodotte dall'intermediario emerge che l'operazione stessa è stata qualificata con "frode" e che vi siano stati 3 alert mai invero pervenuti al ricorrente; **d)** è lo stesso intermediario ad aver riconosciuto la mancata autorizzazione dell'operazione in capo all'istante attivandosi per informarlo tramite il

suo sistema antifrode; **e)** l'intermediario non ha provato elementi fattuali atti a desumere la colpa grave dell'utente e altresì la produzione documentale volta a provare l'autenticazione e formale regolarità dell'operazione non soddisfa l'onere probatorio sullo stesso ricadente;

- **parte resistente** controreplica richiamandosi a quanto già eccepito nelle controdeduzioni e insiste per il rigetto del ricorso.

DIRITTO

Non essendovi questioni preliminari da affrontare, il Collegio procede con l'esame nel merito della richiesta di rimborso dell'unica operazione disconosciuta costituita, alla luce della documentazione in atti, da un bonifico istantaneo dell'importo di euro 1750,00 effettuato su canale *app* in data 1.1.2025 alle ore 9.00.28 (come si ricava dai log prodotti dall'intermediario) con addebito sulla carta ****8120 emessa dalla parte resistente e intestata al ricorrente.

Parte ricorrente, in sede di ricorso e di denuncia, afferma (senza peraltro allegare evidenza di ciò) di aver provveduto al blocco dello strumento di pagamento nr. ****8120, dopo essersi avveduto dell'esecuzione del bonifico oggetto dell'odierna contestazione, tramite l'utenza telefonica dedicata dell'intermediario.

L'operazione contestata è stata posta in essere sotto il vigore del d.lgs. 27 gennaio 2010, n. 11, come modificato dal d.lgs. 15 dicembre 2017, n. 218 di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2), che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE, nonché di adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta.

Dalla richiamata normativa e, in particolare, dall'art. 10 del d. lgs. 11/2010, discende che, qualora l'utilizzatore neghi - come nella vicenda oggetto del ricorso- di aver autorizzato l'operazione di pagamento in oggetto, gravi sull'intermediario l'onere di provare l'avvenuta autenticazione della medesima operazione, la sua corretta registrazione e contabilizzazione, nonché il mancato verificarsi di malfunzionamenti delle procedure necessarie per la sua esecuzione o di altri inconvenienti. Tale prova –precisa il comma 2 del citato articolo- non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utente medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi sul medesimo gravanti, essendo onere del prestatore di servizi di pagamento fornire la prova della frode, del dolo o della colpa grave dell'utente. Nel caso di mancato assolvimento dell'onere probatorio di cui sopra, l'intermediario è obbligato a riaccreditare l'importo dell'operazione sul conto del cliente, ai sensi dell'art. 11 del medesimo d.lgs. n. 11/2010. L'onere di dimostrare la colpa grave o il comportamento fraudolento del titolare dello strumento di pagamento grava pertanto sull'intermediario, ma, come più volte affermato dai Collegi territoriali e dal Collegio di Coordinamento, la relativa prova può essere fornita mediante «indizi chiari, precisi e concordanti idonei a comprovare che parte ricorrente non abbia custodito la carta di pagamento con la dovuta diligenza» (cfr. la decisione ABF, Collegio di coordinamento, n. 897/2014), ovvero, fermo restando che «la produzione documentale volta a provare l'”autenticazione” e

la formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere probatorio», essere fornita dall'intermediario indicando «una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente» (così la decisione ABF, Collegio di Coordinamento, n. 22745/2019).

Il prestatore di servizi di pagamento deve prevedere forme di autenticazione c.d. "forte" per l'autorizzazione di operazioni di pagamento a tutela della sicurezza delle operazioni stesse e del titolare del mezzo di pagamento; diversamente si applica infatti quanto previsto dall'art. 12 comma 2 bis del Dlgs. 11/2010.

La definizione di autenticazione forte si rinviene nell'art. 1, lett. q bis) d.lgs. n. 11/2010 come modificato dal d. lgs. 218/2017, ove si prevede che per autenticazione forte del cliente si intende: «un'autenticazione basata *sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente)* che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri (...)».

Occorre quindi verificare dapprima se, *nel caso in specie*, l'intermediario abbia fornito elementi a sostegno dell'autenticazione e corretta registrazione e contabilizzazione dell'operazione contestata e del tipo di autenticazione predisposta; qualora infatti non fosse stata adottata dal PSP la c.d. autenticazione forte (SCA), il cliente ai sensi dell'art. 12 comma 2bis del DLGS 11/2010 risponderebbe soltanto in caso di frode, frode assente nel caso in esame. A tale riguardo, va ribadito che secondo il costante orientamento dei Collegi, il deposito dei fogli o tabulati, riproduttivi delle tracciate informatiche, corredato da apposita legenda esplicativa, deve essere ritenuto idoneo ad assolvere all'onere probatorio posto a carico dell'intermediario, nella misura in cui consenta al Collegio di verificare la corretta applicazione della S.C.A., con riferimento alle *diverse operazioni (dispositive e non)* per le quali essa è necessaria, a norma dell'art. 10 bis, d. lgs. 27 gennaio 2010, n. 11.

L'art. 10-bis, comma 1, del d.lgs. n.11/2010 dispone infatti, in conformità all'articolo 98 della PSD2 e alle relative norme tecniche di regolamentazione adottate dalla Commissione europea, che *"i prestatori di servizi di pagamento applicano l'autenticazione forte del cliente quando l'utente: a) accede al suo conto di pagamento on-line; b) dispone un'operazione di pagamento elettronico; c) effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi"*.

Il Collegio, in ordine alla prova della SCA, ricorda che secondo l'orientamento condiviso dai Collegi ABF, posto che la PSD2 è tecnologicamente neutrale e non prevede un sistema informatico standard per l'inserimento e la tracciatura dei fattori di autenticazione forte, per valutare l'assolvimento dell'onere della prova della SCA, possono essere valutati (oltre ai log) anche ulteriori elementi esplicativi, quali appunto la legenda esplicativa e/o quanto rappresentato dal PSP nelle proprie difese in relazione al caso concreto, purché consentano di verificare i singoli passaggi registrati dal sistema informatico come prova di autenticazione. Eventuali dichiarazioni confessorie del cliente assumono valore di prova legale ai sensi dell'art. 2730 c.c.

Ciò premesso con riguardo al quadro normativo di riferimento come sopra delineato, ne deriva che la prova dell'autenticazione forte da fornirsi da parte dell'intermediario rappresenta, in aderenza al dato normativo, un *prius* logico rispetto alla prova della colpa grave dell'utente, in mancanza della quale il ricorso deve essere accolto.

Venendo al merito del presente ricorso, il Collegio rileva che la controversia concerne un bonifico dell'importo di € 1.750,00 di cui il ricorrente dichiara di essersi avveduto solo a seguito di una chiamata apparentemente proveniente dalla funzione antifrode dell'intermediario. Per contro l'intermediario chiede il rigetto del ricorso, rilevando come, al momento della materiale esecuzione della operazione oggetto di contestazione, i sistemi informativi non abbiano rilevato alcuna anomalia o irregolarità, essendo stata disposta l'operazione dietro diretta ed immediata autenticazione da parte del legittimo titolare; a supporto di ciò l'intermediario deposita specifica evidenza attestante l'avvenuto *enrollment* della carta di pagamento in oggetto n. **** 8120 di titolarità del ricorrente al sistema autorizzativo di tipo dinamico funzionante mediante l'invio con sms di password dinamica sul numero di cellulare indicato da parte del ricorrente in denuncia..

L'intermediario sottolinea altresì che nel *modulo di reclamo* il ricorrente risulta aver flaggato l'apposita casella prestampata in cui si afferma di aver subito il *furto/smarrimento* del supporto sul quale erano riportate le credenziali di sicurezza per l'utilizzo delle piattaforme online dell'intermediario, circostanza questa che potrebbe aver contribuito al verificarsi della frode; stando invece a quanto dichiarato nella denuncia sporta in data 1.1.2025 (poche ore dopo l'addebito) il ricorrente stesso afferma, con valenza confessoria, che la *carta in oggetto* n. ***8120 è *sempre stata in suo possesso* e ciò nonostante egli non ha mai autorizzato il pagamento de quo. Da ciò si deve supporre che il flag sul furto nel successivo modulo di reclamo sia la risultante di un errore di compilazione del modulo stesso.

Ciò premesso, venendo ai passaggi rilevanti ai fini della autenticazione della operazione contestata, il Collegio sulla base della documentazione in atti rileva quanto segue: l'operazione disconosciuta è stata effettuata in data 1.1.2025 previo accesso alle ore 8.58.24 *all'home banking* con *Log-in in App* (*requisito di possesso*) mediante inserimento del codice di autenticazione P***ID (*fattore di conoscenza*); in data la vera e propria operazione dispositiva (bonifico) è avvenuta poco dopo, alle ore 9.00.28 del medesimo giorno mediante notifica *push in App* (*requisito di possesso*) validata mediante inserimento del codice di autenticazione P***ID (*fattore di conoscenza*) nell'ambito di un sistema dinamico rispondente ai requisiti indicati nelle tabelle stilate dall'EBA nell'Opinion del giugno 2019 relative ai fattori di autenticazione in oggetto.

Dalla documentazione prodotta dall'intermediario risulta che il *device utilizzato* (integrante il *fattore di possesso*) è sempre il medesimo in quanto identificato dallo stesso codice "B60B31***CC45" nella colonna "DeviceID" corrispondente al device certificato del ricorrente; tuttavia poiché sempre dai log prodotti emergevano, ciononostante due differenti "User-agent" identificati rispettivamente con le diciture "Dalvik72.1.0***.007" e "OneApp Android****Android/14" ricondotti al suddetto medesimo device, il Collegio nella riunione del 4 giugno 2025 ha richiesto una specifica integrazione istruttoria alla parte resistente al fine di chiarire come mai ad un medesimo device ID fossero abbinati due diversi User Agent.

Al riguardo parte resistente ha riscontrato la richiesta sottolineando che, con riguardo ad un medesimo device, la circostanza per cui vengono evidenziati nei log due differenti "User-agent" (identificati nel caso di specie rispettivamente con le diciture "Dalvik72.1.0***.007" e "OneApp Android****Android/14") dipende dalla presenza di due App differenti *sul medesimo device*; specifica infatti che lo "User-agent" dipende dal "client https" utilizzato a livello del *software dell'App* e non dal *device stesso*.

In base alla documentazione prodotta risulta dunque provato che l'operazione disconosciuta è stata correttamente autenticata con sistema multifattoriale e ciò sia per quanto riguarda la fase di accesso al

l'home banking sia per quanto riguarda la vera e propria fase dispositiva di pagamento il tutto mediante app installata sul *device* certificato del cliente.

La prova dell'autenticazione forte per il pagamento *on line* disconosciuto, ai sensi della normativa sopra richiamata, non è tuttavia ancora sufficiente per esimere da responsabilità l'intermediario dovendo quest'ultimo - in aderenza al dato normativo (art. 10 del D.Lgs. 11/20105) – fornire *anche la prova della frode, del dolo o della colpa grave dell'utente*.

Il Collegio di Coordinamento, con la citata decisione n. 22745/2019, ha tuttavia ritenuto che l'intermediario possa andare esente da tale responsabilità ove indichi una serie di elementi di fatto che caratterizzano le modalità esecutive delle operazioni dalle quali possa trarsi la *prova, in via presuntiva, della colpa grave dell'utente*.

Quanto alle circostanze della truffa parte ricorrente, in denuncia, afferma di aver ricevuto in data 01/01/2025 una telefonata dall'utenza telefonica ***3144 attraverso la quale un operatore, non meglio qualificato, lo informava che era stato eseguito un pagamento mediante bonifico dell'importo di €1.750,00 tramite la propria carta di debito e insisteva affinché procedesse a sporgere denuncia per il disconoscimento della operazione suddetta;

riferisce altresì di aver verificato l'effettiva presenza di un bonifico non autorizzato tramite App e di aver quindi provveduto al blocco dello strumento di pagamento tramite canali dell'intermediario (utenza telefonica ***8120). L'ufficiale della P.G. ricevente la denuncia dà altresì atto di aver visionato la registrazione della chiamata ricevuta da parte ricorrente alle ore 11:24 del 01/01/2025 e la conferma del bonifico giunta tramite l'App dell'intermediario. Parte ricorrente, in sede di repliche produce in atti anche evidenza del ricevimento della suddetta chiama dall'utenza ***3144, apparentemente riconducibile alla parte resistente.

L'intermediario, per contro, eccepisce la grave lacunosità della narrazione fornita dalla ricorrente ravvisandone un indice di colpa grave. Il Collegio concorda nella eccezione sollevata dall'intermediario di scarsa contestualizzazione dei fatti da parte del ricorrente il quale sembra essere rimasto vittima di un'ipotesi di phishing classico.

Con riguardo agli utilizzi fraudolenti on line, come quello in esame, l'orientamento dei Collegi ABF è nel senso di distinguere l'ipotesi in cui la mancata autorizzazione dell'operazione di pagamento sia legalmente presunta (come nei casi di furto o smarrimento dello strumento di pagamento) da quella in cui, in assenza della predetta presunzione (come accade anche nel caso in esame, stante quanto sopra esposto), il ricorrente *debba allegare i fatti che rendano plausibile che l'operazione di pagamento è stata disposta da un terzo non autorizzato*.

Conseguentemente, nelle contestazioni di utilizzi fraudolenti on line di strumenti di pagamento in cui:

- i. l'intermediario ha offerto la prova dell'autenticazione delle transazioni disconosciute;
- ii. il sistema di pagamento risulta conforme alla Strong Customer Authentication (SCA);
- iii. non risultano indici di anomalia delle operazioni e/o ulteriori elementi;

le mancate allegazioni del cliente sulle circostanze di fatto della frode, che afferma di aver patito, rappresentano un elemento da cui il Collegio può trarre il proprio convincimento, insieme ad altre circostanze, circa la colpa grave del ricorrente medesimo.

In tal senso anche il presente Collegio nella propria precedente decisione n.9593/24 ove si è affermato quanto segue: *“L’intermediario ha eccepito la lacunosità della narrazione fornita dalla ricorrente, ipotizzando che la stessa sia rimasta vittima di un consueto episodio di phishing, nel corso del quale la cliente comunicava a terzi le credenziali necessarie per installare il token su altro device e compiere l’operazione disconosciuta. Sul punto, si osserva che i Collegi sono soliti valutare negativamente la scarsa contestualizzazione dei fatti da parte del ricorrente, laddove l’intermediario abbia fornito prova della corretta autenticazione delle operazioni (cfr. ex multis, Collegio di Bologna, decisione n. 3888/23)”*.

Sulla base di tale orientamento, stante la lacunosa e talvolta anche contraddittoria contestualizzazione dei fatti della truffa offerta dal ricorrente, il Collegio ritiene di considerare pertanto provata la colpa grave del ricorrente. Non constano indicatori di anomalia che possano incidere su tale valutazione. Trattandosi infine di un’unica operazione disconosciuta non rileva l’eventuale invio o meno di alert.

Il presente ricorso, pertanto, non può essere accolto; stante il rigetto della domanda principale risulta rigettata anche la domanda di refusione delle spese legali.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE