

COLLEGIO DI MILANO

composto dai signori:

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

Relatore (MI) BARTOLOMUCCI

Seduta del 06/05/2026

FATTO

La ricorrente, insoddisfatta dell'interlocuzione intercorsa nella fase del reclamo, adiva questo Arbitro deducendo di aver pubblicato, in data 30 settembre 2025, un annuncio su una piattaforma di compravendita online, in seguito al quale veniva contattata da un soggetto che si mostrava interessato all'acquisto e che le chiedeva di proseguire la conversazione su WhatsApp, inviandole un link che la indirizzava ad un sito che sembrava legittimo, in realtà rivelatosi fraudolento.

Faceva presente di aver inserito i dati richiesti e un Codice OTP che aveva ricevuto sul telefono, avvedendosi di aver involontariamente autorizzato un'operazione di € 350,00.

Affermava di aver immediatamente bloccato la carta, disconosciuto l'operazione e presentato denuncia alle autorità.

Chiedeva, pertanto, il rimborso dell'importo fraudolentemente sottratto.

Si costituiva l'odierno resistente il quale rilevava che l'operazione disconosciuta fosse stata correttamente contabilizzata, registrata e autenticata in quanto posta in essere con il corretto inserimento delle credenziali.

Evidenziava che la truffa avesse avuto luogo al di fuori dell'ambito di competenza della banca, in quanto avvenuta su un sito fraudolento ad essa non riconducibile; riteneva, pertanto, sussistente la colpa grave della cliente in quanto avrebbe cliccato su un link contenente parole incomprensibili e non riconducibili ad alcun sito noto e inserito i propri dati personali e un Codice OTP ricevuto sul telefono.

Sottolineava pure che il messaggio OTP, inoltre, l'avesse informata circa il fatto che l'inserimento del codice avrebbe comportato l'autorizzazione dell'operazione; quindi, la cliente sarebbe stata adeguatamente informata delle conseguenze delle sue azioni e la truffa sarebbe a lei esclusivamente imputabile.

Chiedeva, pertanto, il rigetto del ricorso.

Alle controdeduzioni dell'intermediario replicava la ricorrente, ribadendo di aver autorizzato l'operazione a causa di un raggirio sofisticato e di aver agito tempestivamente per cercare di bloccare l'operazione, ma senza successo.

Le repliche della ricorrente venivano riscontrate dall'intermediario, il quale osservava che la truffa in questione non fosse affatto insidiosa o sofisticata, posto che il messaggio truffaldino presentava delle evidenti anomalie che avrebbero dovuto insospettire la cliente; soggiungeva che la cliente avesse effettuato un pagamento pensando di ricevere denaro, cosa non possibile attraverso la sua carta bancomat che non dispone di un IBAN.

DIRITTO

La domanda proposta dal ricorrente è relativa all'accertamento del proprio diritto alla restituzione del controvalore di un'operazione di pagamento, successivamente disconosciuta.

La materia, come noto, è regolata dal d. lgs. n. 11/2010 come modificato dal d. lgs. n. 218/2017 con cui è stata recepita la direttiva 2015/2366/Ue (c.d. PSD2- Payment Services Directive 2).

Tale disciplina, al fine di rafforzare i presidi di sicurezza e di incentivare il corretto utilizzo di strumenti di pagamento diversi dal contante, introduce una serie di obblighi in capo tanto ai fruitori quanto ai prestatori di servizi di pagamento: ai primi è imposto di usare detti strumenti in modo diligente, in conformità alle prescrizioni contrattuali, adottando misure idonee ad assicurare la segretezza dei codici personalizzati necessari per usufruire dei servizi e onerando gli stessi di informare tempestivamente i prestatori in caso di operazioni fraudolente; ai secondi, invece, è imposto di predisporre sistemi di sicurezza che impediscano l'accesso da parte di terzi ai dispositivi personali degli utilizzatori (c.d. strong customer authentication SCA), nonché ad impedire l'uso degli strumenti di pagamento successivamente alla comunicazione ricevuta da questi ultimi nei casi di operazioni disconosciute.

Con riferimento alla c.d. SCA gli artt. 97 e 98 della direttiva PSD2, nonché l'articolo 10-bis del d. lgs. n. 11/2010, oltre che le norme tecniche di regolamentazione emanate dall'EBA e recepite con Regolamento Delegato Ue 2018/389 della Commissione Europea e i criteri interpretativi adottati dalla stessa Autorità (cfr. in particolare il parere dell'EBA del 21 giugno 2019), hanno stabilito che essa 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. In relazione a tutte le predette fasi, la SCA si realizza con il ricorso ad almeno due dei seguenti tre fattori, che devono essere reciprocamente indipendenti e appartenere a categorie diverse: conoscenza; inerenza; possesso.

Al fine di bilanciare le diverse posizioni, ed in ragione del rischio d'impresa riconosciuto in capo al prestatore dei servizi di pagamento, la normativa de qua prevede una diversa distribuzione degli oneri probatori in conseguenza del disconoscimento di un'operazione, con l'obiettivo di attribuire la responsabilità degli utilizzi fraudolenti all'impresa, nel caso in cui essi non siano stati cagionati da frode, dolo o colpa grave del cliente. Tale criterio di imputazione della responsabilità, tuttavia, presuppone sul piano fattuale che gli utilizzi non autorizzati siano stati effettuati in conseguenza del furto o dello smarrimento degli strumenti di pagamento, ovvero dell'illecito utilizzo dei codici dispositivi degli strumenti di pagamento da parte di terzi frodatori.

Risulta documentalmente che l'operazione in parola consista in un pagamento online di € 350,00 eseguito il 30 settembre 2025.

Le tracciate informatiche versate in atti evidenziano che l'operazione è stata autenticata tramite l'inserimento del Codice OTP (fattore di possesso) pervenuto tramite SMS sul numero certificato della cliente e la digitazione di un ulteriore codice noto esclusivamente alla stessa (fattore di conoscenza).

Attesa la conformità a SCA dell'operazione contestata, non resta che verificare se – dalla condotta tenuta dal ricorrente – siano evidenziabili profili di colpa grave, rispetto alla quale la prova di autenticazione rappresenta, in aderenza al dato normativo, un *prius* logico (cfr. Coll. coord., dec. n. 22745/2019).

A tale proposito, la ricorrente riferisce di aver inserito un annuncio su un noto sito di vendite online e di essere stata contattata da uno sconosciuto che si è finto interessato ai suoi articoli. Di tale circostanza, tuttavia, non fornisce alcuna prova documentale.

Secondo il consolidato indirizzo di questo Collegio, la mancata allegazione, da parte del cliente, del registro delle chiamate non consente di verificare se il numero da cui la telefonata truffaldina sarebbe partita possa essere riconducibile all'intermediario e, pertanto, se sia configurabile un legittimo affidamento dell'utente circa la sua genuinità.

A ciò si aggiunga, di contro, che ella afferma di aver ricevuto dal truffatore un link e, dopo avervi cliccato sopra, sarebbe stata condotta sul sito fraudolento. Dall'esame dell'sms, risulta che né il mittente né il link sono riconducibili all'intermediario; al contrario risulta che il primo sia riferibile alla piattaforma di vendita online.

L'intermediario soggiunge pure che il link avrebbe dovuto suscitare dubbi nella cliente, in quanto conteneva parole incomprensibili e sospette.

Dal canto suo, la ricorrente la cliente precisa di aver inserito i dati della propria carta e il Codice OTP in quanto indotta a credere che ciò servisse solo a verificare la propria identità e che non stesse affatto autorizzando un pagamento; l'odierno convenuto, invece, evidenzia (e documenta) di aver inviato due messaggi in cui le veniva espressamente comunicata la natura dell'operazione, oltre a precisare che lo strumento di pagamento non fosse abilitato a ricevere accrediti, non essendo munito di iban.

L'insieme delle riferite circostanze induce il Collegio a ritenere che la condotta della ricorrente sia stata contraddistinta da colpa grave. Non vi sono, pertanto, elementi che consentano di accogliere il ricorso.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso

IL PRESIDENTE