

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(MI) RIZZO	Membro designato dalla Banca d'Italia
(MI) FORMAGGIA	Membro di designazione rappresentativa degli intermediari
(MI) SCARANO	Membro di designazione rappresentativa dei clienti

Relatore (MI) BARTOLOMUCCI

Seduta del 14/04/2026

FATTO

La ricorrente, insoddisfatta dell'interlocuzione intercorsa con l'intermediario nella fase di reclamo, adiva questo Arbitro deducendo di aver ricevuto, in data 2 settembre 2025, una telefonata da un numero corrispondente all'utenza telefonica fissa dei Carabinieri di Brescia, nel corso della quale il sedicente maresciallo dei carabinieri la avvisava di essere stata rilevata l'esistenza di una transazione illecita con la sua carta di debito e le chiedeva di spostare la comunicazione sulla piattaforma Whatsapp.

Faceva presente che il truffatore procedesse ad effettuare una videochiamata tramite Whatsapp, con numero di telefonia mobile, durante la quale riferiva con esattezza i suoi dati personali e quelli della sua carta di debito (probabilmente carpiri su qualche sito internet hackerato utilizzato dalla ricorrente per effettuare un acquisto on line) e chiedeva di avere il codice OTP per consentire il blocco del pagamento e il riaccredito dell'importo della transazione.

Rappresentava di essersi insospettita e di aver interrotto la conversazione avendo intuito potesse trattarsi di un tentativo di truffa, provvedendo al blocco della carta; evidenziava, tuttavia, che in data 4 settembre 2025 verificava l'addebito della somma di € 2.424,00 relativo a transazione non autorizzata effettuata il 02.09.25 ore 16:57.

Affermava di aver anche sporto denuncia alle competenti autorità e di aver presentato reclamo, illegittimamente rigettato nonostante che i riferimenti personali e della carta di debito fossero già in possesso del truffatore e che lei non avesse mai chiesto la conferma dell'operazione di pagamento tramite invio con sms dell'OTP né tantomeno avesse comunicato alcunché.

Evidenziava che, per effettuare pagamenti on line, avesse scelto esclusivamente la modalità di autenticazione biometrica e segnatamente a mezzo impronta digitale; segnalava, tuttavia, che il sistema adottato dall'istituto di credito, in mancanza di autorizzazione biometrica da parte del cliente entro un certo tempo, ovvero in caso di malfunzionamento temporaneo della biometria, provvede comunque - automaticamente - ad inviare sul cellulare dell'utente via sms il codice temporaneo.

Da ultimo, rilevava che l'OTP inviato tramite sms, come ben noto alle banche, può essere intercettato sul cellulare della vittima senza che questa nemmeno se ne accorga.

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

Si costituiva ritualmente l'intermediario convenuto, il quale osservava che l'operazione fosse stata correttamente contabilizzata, registrata e autenticata in quanto posta in essere con il corretto inserimento delle credenziali, sottolineando che la tecnologia SCA 3DS è stata reputata la più avanzata ed affidabile nell'ambito dei pagamenti online in quanto si tratta di un sistema di autorizzazione "a due fattori".

Con riferimento alle modalità di autenticazione delle operazioni di pagamento e-commerce, precisava che in data 17/01/2025, fosse stata disabilitata la biometria tramite canale App e fosse stato pertanto ripristinato di default il servizio 3DS; segnalava che, alla data di effettuazione dell'operazione del 02/09/2025, la biometria non risultasse attiva sul profilo utente della ricorrente e pertanto non potesse essere utilizzata come metodo di autenticazione per l'operazione contestata.

Evidenziava che la ricorrente fosse perfettamente a conoscenza della modalità di autenticazione dell'operazioni di pagamento e-commerce tramite invio del codice OTP ed inserimento del codice 3DS, considerato che nei mesi successivi alla modifica del 17/01/2025, la stessa aveva autorizzato altri pagamenti con tale modalità.

Riteneva, pertanto, che l'operazione fosse stata resa possibile esclusivamente per effetto della comunicazione del codice OTP da parte della ricorrente a soggetti terzi. Tale circostanza integra una cessione, seppur inconsapevole, delle credenziali di sicurezza, in violazione degli obblighi di custodia gravanti sull'utilizzatore dello strumento di pagamento.

Chiedeva, pertanto, il rigetto del ricorso ovvero di disporre – in caso di accoglimento – il concorso di colpa con la ricorrente.

Alle controdeduzioni dell'intermediario replicava la ricorrente, la quale confermava che la disabilitazione della biometria fosse stata effettivamente effettuata in ragione del fatto che il suo cellulare era stato sottoposto nel periodo dal 03.01.2025 al 17.01.2025 a riparazione presso un rivenditore, all'esito della quale le APP erano state reinstallate; specificava che, per riattivare correttamente il sistema di autenticazione, avesse dapprima rimosso e disabilitato la biometria inserendo il PIN per poi riattivarla immediatamente con autenticazione a mezzo impronta digitale.

Sosteneva che le due operazioni richiamate dalla banca nelle proprie controdeduzioni fossero state eseguite a mezzo inserimento del codice OTP e 3DS proprio perché si trattava di ipotesi nelle quali il sistema utilizzato dall'istituto di credito, per malfunzionamenti propri o per non tempestiva autenticazione biometrica del cliente, anziché annullare l'operazione, invia il codice OTP.

Contestava in ogni caso l'idoneità della documentazione prodotta dalla banca ed invitava la stessa a produrre la documentazione relativa all'autenticazione di tutte le operazioni evidenziate negli estratti conto allegati.

Ribadiva di non aver comunicato al truffatore il codice OTP (anche perché pervenuto con SMS in un momento in cui la telefonata con il sedicente maresciallo era già stata interrotta), così come di non aver mai comunicato a terzi, altri dati e/o credenziali riferite alla propria carta di debito.

Le repliche della ricorrente venivano riscontrate dall'intermediario, il quale eccepiva l'inammissibilità della nuova domanda relativa all'esibizione documentale ivi richiesta, poiché relative ad operazioni mai contestate, né disconosciute.

Ribadiva che la cliente, in data 17/01/2025 21:59:17, avesse disabilitato la biometria generale relativa all'autorizzazione di tutte le operazioni e che ciò avesse comportato anche la disattivazione automatica della biometria per autorizzare le operazioni eseguite con carte di pagamento.

Riteneva di aver pienamente dimostrato che l'operazione contestata fosse stata autenticata correttamente mediante inserimento del codice OTP e del codice statico 3DS, che non fosse stata rilevata alcuna anomalia tecnica nel processo di autorizzazione e che tutte le credenziali utilizzate fossero nella disponibilità esclusiva dell'utente.

Evidenziava, ad ogni modo, che la ricorrente non avesse fornito alcuna spiegazione plausibile su come il truffatore avrebbe potuto ottenere il codice OTP necessario all'autorizzazione dell'operazione senza una qualche forma di collaborazione, diretta o indiretta, da parte della cliente, posto che era stato inviato esclusivamente al suo numero di telefono personale e non risultavano compromissioni del dispositivo né anomalie tecniche che potessero giustificare un'acquisizione illecita del codice da parte di terzi.

DIRITTO

La domanda proposta dalla 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.

Emerge documentalmente che l'operazione contestata consista in un pagamento on line effettuato in data 02.09.2025, per un importo di € 2.424,00.

L'intermediario osserva, in via generale, che i pagamenti e-commerce sono autenticati e disposti utilizzando i dati riportati sulla carta di debito, ossia il PAN, la data di scadenza, il codice CVC2 ed inserendo il codice OTP inviato tramite SMS al numero di cellulare certificato dell'utente ed il codice 3DS, di natura statica, composto da 5 a 10 numeri, impostato direttamente dall'utente accedendo alla sezione dedicata "3DS Codice di sicurezza e-commerce" sulla propria area personale.

Con riferimento alla transazione in esame, le tracciate informatiche evidenziano che essa sia stata autenticata mediante la digitazione dell'OTP ricevuto via sms sull'utenza univocamente riferibile alla ricorrente (elemento di possesso) e l'inserimento del codice statico "3DS" ai fini della conferma dell'operazione (elemento di conoscenza).

Alla luce di tali risultanze documentali, appare non assumere rilievo la diversa rappresentazione sulle modalità di autenticazione che viene fornita dalle parti: parte ricorrente lamenta la mancata autenticazione in modalità biometrica, mentre l'intermediario afferma che la biometria è stata disattivata dalla cliente il 17.01.2025. Poiché l'autenticazione dell'operazione è avvenuta in modalità 3DS, ai fini della prova della SCA è necessario che vi sia comunque evidenza di un doppio fattore di autenticazione, indipendentemente dalla relativa natura, come si è appena rilevato.

Attesa la conformità a SCA di tali operazioni, non resta che verificare se – dalla condotta tenuta dalla 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).

Alla luce della rappresentazione dei fatti e delle evidenze prodotte, è chiaro che la frode ha avuto luogo mediante un canale in alcun modo riferibile all'intermediario, ossia una chiamata e successiva chat in apparenza riconducibile ai Carabinieri, peraltro con chiari indizi di anomalia, tra cui l'utilizzo di una piattaforma di messaggistica che utilizza un numero di telefonia mobile, sulla quale risultano *per tabulas* messaggi con numerosi errori grammaticali oltre che caratterizzati da un tono allarmistico ed intimidatorio.

La stessa ricorrente ha pure prodotto evidenza delle chiamate al servizio clienti della banca; la prima risulta effettuata alle ore 16:57, ossia lo stesso minuto in cui è stata eseguita l'operazione oggi disconosciuta, rendendo quindi verosimile che la banca abbia appreso della frode in corso proprio nell'esatto momento in cui il pagamento truffaldino veniva eseguito, senza peraltro possibilità di recupero in quanto transazione e-commerce.

Deve, quindi, ritenersi sussistente la colpa grave della cliente che – con la propria condotta – ha permessa la consumazione della truffa ai suoi danni.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso

IL PRESIDENTE