

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) CAPIZZI	Membro di designazione rappresentativa degli intermediari
(MI) SCARANO	Membro di designazione rappresentativa dei clienti

Relatore (MI) BARTOLOMUCCI

Seduta del 01/09/2026

FATTO

La ricorrente, insoddisfatta dell'interlocuzione intercorsa nella fase del reclamo, adiva questo Arbitro deducendo di aver ricevuto, in data 13/10/2025, una chiamata che sembrava provenire dall'assistenza clienti dell'intermediario.

Faceva presente che l'interlocutore l'avesse indotta a fornire le proprie credenziali e ad autorizzare l'accesso remoto ai suoi conti, facendole credere di autorizzare la revoca di movimenti da lei non effettuati. Da quel momento, i truffatori riuscivano a svincolare delle somme e disporre due giroconti da € 15.000,00 e € 14.500,00 dal suo conto deposito al conto cointestato con suo marito, nonché a svincolare delle somme e disporre due ulteriori giroconti da € 24.000,00 e € 25.000,00 dal suo conto deposito al conto cointestato con sua figlia. Soggiungeva che i malfattori avessero poi disposto un bonifico istantaneo di € 4.990,00 dal conto cointestato con suo marito ed un ulteriore bonifico istantaneo di € 4.990,00 dal conto cointestato con sua figlia.

Affermava che la sera stessa, alle 20.58, accortasi della truffa, avesse denunciato verbalmente l'accaduto al servizio clienti dell'intermediario, che provvedeva al blocco dei suoi conti e che avesse pure sporto denuncia presso le Autorità.

Considerava negligente da parte di un intermediario non trovare adeguati strumenti di tutela verso i propri clienti conoscendo la problematica e l'elevato numero di truffe effettuate dall'entrata in vigore

dei bonifici istantanei; precisava di aver ottenuto soltanto due bonifici di € 10,00 cadauno, da parte dell'istituto del beneficiario dei bonifici fraudolenti di € 4.990,00.

Lamentava che il bonifico di € 4.990,00 disposto in data 13/10/2025 fosse stato autorizzato nonostante in quel momento non vi fosse disponibilità sufficiente sul conto, al punto da aver reso necessari i giroconti sopracitati.

Chiedeva, pertanto, il rimborso delle somme fraudolentemente sottratte.

Si costituiva l'odierno resistente il quale rilevava che la stessa ricorrente avesse ammesso di aver comunicato a terzi tutti i propri codici personali, sia statici (PIN, password, credenziali di accesso) sia dinamici (OTP ricevuti via SMS), rendendosi così vittima di *social hacking*.

Evidenziava che le operazioni fossero state correttamente contabilizzate, registrate e autenticate in quanto poste in essere con il corretto inserimento delle credenziali; riteneva, pertanto, sussistente la colpa grave della cliente in quanto in denuncia avesse ammesso di aver seguito tutte le indicazioni ricevute telefonicamente dall'interlocutore, nonostante le stesse apparissero manifestamente inverosimili.

Metteva in luce l'incongruenza nella rappresentazione dei fatti, sottolineando che nel ricorso la cliente avesse riferito unicamente di essere stata contattata telefonicamente da un soggetto qualificatosi come operatore del servizio clienti dell'intermediario, mentre nella denuncia avesse dichiarato che il primo contatto fosse provenuto da un sedicente operatore di altro intermediario, al quale aveva comunicato tutti i codici del proprio *home banking*, autorizzando un bonifico e informandolo dell'esistenza di ulteriori rapporti di conto corrente.

Sottolineava che nel caso di specie non vi fosse stato alcun uso improprio o abusivo del sistema di comunicazioni ufficiale della banca né, tantomeno, un malfunzionamento dei sistemi di sicurezza. Evidenziava, peraltro, che la ricorrente non avesse neppure prodotto evidenza del registro chiamate e, in sede di reclamo, avesse prodotto evidenza di un SMS presumibilmente ricevuto da parte dei frodatori mentre si verificava la truffa. Tale messaggio, oltre ad avere un nome mittente improbabile e non riconducibile all'intermediario, non risultava inserito nella chat genuina della banca.

Precisava che la disponibilità delle somme afferenti alle operazioni di giroconto/bonifico interno fosse disciplinata dai Documenti di Sintesi sia dei Conti Deposito sia dei Conti Correnti, ciascuno dei quali prevede che per le "operazioni di giroconto [...] la disponibilità delle Somme sul rapporto beneficiario è immediata". Alla luce di tale disciplina contrattuale, nonché della sequenza temporale delle operazioni, sosteneva che dovesse escludersi che le disposizioni di bonifico fossero state eseguite in assenza di sufficiente disponibilità sul conto, come erroneamente sostenuto dalla cliente nel ricorso.

Affermava che, una volta informato del disconoscimento dei bonifici da parte della cliente, si fosse attivato al fine di cercare di recuperare l'importo sottratto, senza successo.

Chiedeva, pertanto, il rigetto del ricorso.

Alle controdeduzioni dell'intermediario replicava la ricorrente, la quale chiariva di non aver mai riferito nel ricorso della telefonata con il sedicente operatore di altro intermediario, mentre ribadiva di non aver capito, mentre era al telefono, che si trattasse di una truffa e che avesse fornito i codici personali all'interlocutore, al quale aveva creduto senza sospettare nulla, permettendo ai malfattori di abilitare i bonifici istantanei sul suo conto, di innalzare i limiti di spesa sul suo conto e su quello di sua figlia, di

svincolare i suoi depositi e di disporre quattro giroconti di € 15.000,00, € 14.500,00, € 24.000,00 e € 25.000,00 rispettivamente dal suo conto deposito al suo conto corrente e a quello cointestato con la figlia, nonché di disporre due bonifici di € 4.990.00 ciascuno.

Soggiungeva che sul momento non avesse controllato i messaggi ricevuti sul telefono se non il primo, con cui le veniva comunicato il nuovo codice di accesso e che si fosse avveduta della truffa solo quando sua figlia aveva riscontrato i due bonifici di importo rilevante sul conto corrente cointestato ed aveva avvisato suo marito, dal momento che lei era in linea con il truffatore.

Le repliche della ricorrente venivano riscontrate dall'intermediario, il quale reiterava le proprie allegazioni in merito alla comunicazione dei codici da parte della cliente, nonché del mancato assolvimento dell'onere probatorio in ordine allo *spoofing*.

DIRITTO

La domanda proposta dalla ricorrente è relativa all'accertamento del proprio diritto alla restituzione del controvalore di alcune operazioni di pagamento, successivamente disconosciute.

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 le operazioni in parola consistano in due bonifici eseguiti in data 13/10/2025, per un importo complessivo di € 9.960,00.

Le tracciature informatiche versate in atti evidenziano che alle ore 19.21 veniva effettuato un login da web tramite codice di accesso e OTP, ricevuto dalla cliente via SMS, al quale hanno fatto seguito due operazioni di svincolo e due giroconti.

Successivamente, alle ore 19.28, veniva abilitato il servizio di bonifico istantaneo sul conto della cliente cointestato con la figlia tramite OTP e venivano effettuate tre modifiche dei limiti dei bonifici sul conto, sempre tramite OTP; analogamente, le stesse disposizioni venivano eseguite sul conto della cliente cointestato con il marito. Mette conto rilevare che la stessa ricorrente ha dichiarato di essere stata indotta dal sedicente operatore dell'intermediario a fornire le proprie credenziali e ad autorizzare l'accesso remoto ai suoi conti, pensando di revocare dei movimenti da lei non effettuati.

Con riguardo alla fase successiva, i log versati in atti evidenziano che i bonifici contestati siano stati autenticati mediante digitazione del codice OTP, nell'ambito della sessione di login inizializzata in precedenza. A tale riguardo la stessa Autorità europea ha ritenuto conforme al quadro normativo l'esecuzione di un'operazione di pagamento con l'inserimento di un solo fattore di autenticazione quando si procede al riutilizzo di un secondo fattore di diversa natura già inserito nella stessa sessione per l'accesso al conto (nel caso di specie, il codice di accesso - presumibilmente una password - indicato dall'intermediario come secondo fattore di SCA: cfr. Q&A EBA 2018_4141).

Attesa la conformità a SCA delle operazioni contestate, 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).

A tale proposito, la cliente riferisce di aver ricevuto una chiamata da un numero riconducibile all'odierno resistente. Di tali circostanze, 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.

La cliente non riferisce di aver ricevuto messaggi truffaldini, né in ricorso né in denuncia. Tuttavia, l'intermediario afferma che ella avrebbe prodotto l'evidenza di un SMS presumibilmente ricevuto da parte dei frodatori mentre si verificava la truffa: dall'esame di tale evidenza documentale emerge che la denominazione della chat in cui è inserito il messaggio, e nella quale non sono presenti altri messaggi genuini antecedenti o successivi a quello civetta, non è riferibile all'intermediario.

Deve ritenersi, pertanto, che la cliente sia caduta colpevolmente vittima di *spoofing*.

Priva di pregio appare anche la doglianza relativa alla circostanza per la quale uno dei due bonifici, eseguito sul conto cointestato con la figlia, sia stato autorizzato anche in assenza di fondi sufficienti ovvero di un affidamento; invero, sulla scorta della disciplina contrattuale e della sequenza temporale delle operazioni, deve escludersi che le disposizioni di bonifico siano state eseguite in assenza di sufficiente disponibilità sul conto, avendo peraltro fatto seguito al preventivo recupero della provvista

mediante i giroconti di cui la stessa cliente ha dato conto e che risultano anche dai log informatici versati in atti.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE