

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) PERON	Membro di designazione rappresentativa degli intermediari
(MI) GILIBERTI	Membro di designazione rappresentativa dei clienti

Relatore (MI) BARTOLOMUCCI

Seduta del 31/03/2026

FATTO

La ricorrente, insoddisfatta dell'interlocuzione intercorsa nella fase del reclamo, adiva questo Arbitro deducendo di aver ricevuto, in data 02/07/2025, una chiamata da un numero che sembrava provenire dall'intermediario, con cui le veniva comunicato che era stata identificata un'operazione sospetta volta all'acquisto di criptovalute pari ad € 60,00, alla quale faceva seguito un SMS contenente un codice OTP che si inseriva nella chat usuale di conversazione con l'intermediario.

Faceva presente di essersi avveduta di essere rimasta vittima di una truffa in quanto, finita la chiamata, dall'esame della propria home banking risultavano tre operazioni eseguite non autorizzate, per il complessivo importo di € 4.163,98.

Rappresentava di aver sporto denuncia alle autorità e di aver disconosciuto le operazioni.

Chiedeva, pertanto, il rimborso dell'importo complessivo di € 4.500,00 oltre interessi legale e spese di assistenza difensiva.

Si costituiva l'odierno resistente il quale precisava di aver già disposto in favore della cliente, il rimborso della somma di € 1.000,00, della quale ella non faceva menzione nel ricorso.

Sosteneva che per scaricare l'app della home banking su un dispositivo a tal fine fosse necessario inserire dei dati che solo la cliente conosceva.

In base a tale ricostruzione, osservava che l'installazione della nuova APP sul dispositivo del frodatore fosse potuta avvenire solo a fronte della cooperazione, più o meno consapevole, della cliente, la quale gli aveva necessariamente fornito elementi di sua esclusiva conoscenza; soggiungeva, peraltro, che il bonifico istantaneo eseguito non potesse essere bloccato in quanto si tratta di un'operazione che va immediatamente a buon fine, come è comunicato al cliente in sede di autorizzazione dell'operazione.

Riteneva, pertanto, che la cliente fosse caduta vittima di phishing, su cui aveva avviato da tempo una campagna di sensibilizzazione contro tali tipologie di truffa.

Quanto alle operazioni contestate, rilevava che fossero state correttamente autorizzate, registrate e contabilizzate, in quanto poste in essere secondo un sistema di autenticazione forte (SCA) e senza alcun malfunzionamento dei sistemi.

Con riferimento alle chiamate a sé riconducibili, evidenziava che la cliente non avesse utilizzato l'APP di "verifica chiamata" per verificare la genuinità delle stesse, facendo emergere la sua condotta gravemente sprovveduta e colposa.

Considerava, pertanto, sussistente la colpa grave della ricorrente per aver fornito al truffatore i dati necessari per l'enrollment dell'app su un nuovo dispositivo contravvenendo agli obblighi di custodia dei dispositivi finalizzati all'uso di strumenti di pagamento e non avendo riscontrato malfunzionamenti o intrusioni nei propri sistemi informatici.

Chiedeva, pertanto, il rigetto del ricorso.

Alle controdeduzioni dell'intermediario replicava la ricorrente, la quale affermava che l'intermediario non avesse fornito una prova idonea a scaricarla da colpe o tale da provare la sua colpa grave.

Evidenziava che sia la chiamata sia gli sms ricevuti non presentassero elementi tali da renderli inattendibili, in quanto si era trattato di una truffa insidiosa per quanto concerne le modalità; soggiungeva che non vi fosse prova dell'inserimento da parte della stessa delle credenziali.

Affermava, dunque, che la banca avrebbe dovuto sospendere l'esecuzione dei bonifici discussi dati gli elevati importi ed avrebbe dovuto subordinare il compimento delle operazioni all'accertamento effettivo dell'identità del correntista.

Le repliche della ricorrente venivano riscontrate dall'intermediario, il quale si riportava ai propri scritti difensivi.

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 PDS2, 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 pagamenti on line e in un bonifico istantaneo, eseguiti in data 02/07/2025, per un importo complessivo di euro 4.163,98.

Quanto al processo di autenticazione, l'odierno convenuto chiarisce che le operazioni contestate sono state precedute, alle ore 15:15:03 del giorno 02/07/2025, dall'installazione dell'APP della banca su un nuovo device, descrivendo i singoli passaggi dell'iter: in particolare afferma che alle ore 15:10:32 il truffatore ha digitato il Codice Cliente e la propria data di nascita e conferma cliccando sul bottone "Continua", per poi digitare (alle ore 15:10:33) le tre cifre del PIN richieste e confermare cliccando sul bottone "Continua".

Ottenuto riscontro positivo dal sistema, alle ore 15:11:05, è stato scelto il codice segreto (Smart Code) ed è stata effettuata la scelta se utilizzare o meno i propri dati biometrici per accedere all'app e autorizzare le operazioni. Alle ore 15:11:26 la banca ha inviato un sms OTP al numero di telefono che corrisponde a quello dichiarato dal cliente in sede di denuncia.

Da ultimo, è stato inserito il Codice OTP ricevuto via SMS che ha ottenuto la validazione della banca alle ore 15:15:01. All'esito di tali passaggi, alle ore 15:15:02 la banca ha completato l'attivazione dell'APP sul nuovo dispositivo ed ha inviato la relativa e-mail di notifica.

Sulla scorta di tali risultanze documentali, deve ritenersi che l'accesso all'area riservata sia avvenuto in modalità conforme a SCA, mediante l'utilizzo dei due fattori di autenticazioni: il PIN (fattore di conoscenza) e l'SMS OTP (fattore di possesso).

Emerge altresì dall'analisi delle tracciate informatiche che le operazioni di carattere dispositivo siano state precedute dai rispetti accessi all'App scaricata sul nuovo device precedentemente enrollato; tali accessi risultano eseguiti in modalità conforme a SCA, tramite l'utilizzo dell'applicazione (fattore di possesso) e la digitazione del fattore biometrico, per il primo pagamento on line, ovvero dello Smart Code, per il bonifico istantaneo (fattore di conoscenza). Mette conto precisare che, con riguardo al secondo pagamento e-commerce, questo sia stato eseguito con l'inserimento del codice statico e del codice dinamico trasmesso via SMS; esso, pertanto, non richiede l'esame di fasi prodromiche quali accesso all'APP o all'home banking.

Con riferimento alla fase dispositiva, dai log versati in atti che tutte le operazioni siano state eseguite in conformità alla SCA poiché effettuato mediante l'utilizzo dell'app (fattore di possesso) e la digitazione del codice segreto (fattore di conoscenza).

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, nel corso della telefonata con il sedicente operatore dell'intermediario, un SMS contenente un codice OTP; tale fattispecie deve, quindi, essere ricondotta alla truffa qualificata come spoofing.

Ancorché, per quanto si evidenzia dalle risultanze documentali, la telefonata sembra essere pervenuta da una numerazione riferibile all'intermediario e gli sms siano inseriti nella chat ufficiale dell'odierno resistente, palesando dunque un certo carattere di insidiosità, deve pure rilevarsi che il contenuto dei messaggi "parlanti" fosse tale da poter mettere in allarme la cliente.

Emerge *per tabulas*, infatti, che i primi due messaggi recano il codice utile per la configurazione dell'App, mentre il terzo informa la cliente di aver sospeso la sua operatività sui prodotti dell'intermediario per ragioni di sicurezza; ad essi, segue pure un SMS alert relativo al bonifico istantaneo fraudolento.

Va pure precisato che i messaggi contenenti il codice necessario per la configurazione dell'App (evidentemente su un device diverso), contengono pure l'espresso avvertimento che – laddove non fosse stato la ricorrente ad inoltrare la richiesta – avrebbe dovuto contattare immediatamente l'intermediario. Tale evidenza documentale appare idonea non solo a far presumere che la cliente abbia previamente comunicato al truffatore il proprio codice PIN, ma che questa non abbia contattato l'intermediario per bloccare la configurazione dell'applicazione sul device del truffatore.

Tale comportamento, unitamente al fatto che il ricorrente non si sia avvalsa del servizio di verifica della genuinità delle telefonate messo a disposizione dall'intermediario, appare avere efficacia assorbente dal punto di vista causale in ordine alle conseguenze pregiudizievoli conseguenti alle operazioni fraudolente.

Pertanto, attesa la conformità a SCA delle rispettive operazioni ed in considerazione della colpa grave della ricorrente, alcun ulteriore rimborso può essere disposto in favore di quest'ultima.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso

IL PRESIDENTE