

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(MI) BALDINELLI	Membro designato dalla Banca d'Italia
(MI) CAPIZZI	Membro di designazione rappresentativa degli intermediari
(MI) CESARE	Membro di designazione rappresentativa dei clienti

Relatore (MI) BARTOLOMUCCI

Seduta del 10/02/2026

FATTO

Il ricorrente, insoddisfatto dell'interlocuzione intercorsa nella fase del reclamo, adiva questo Arbitro deducendo di aver ricevuto, in data 6.8.2025, un sms che sembrava provenire dall'intermediario – in quanto presente all'interno della chat con la banca – con cui gli veniva comunicata l'intervenuta richiesta di autorizzazione di una spesa pari ad € 4.997,00; il messaggio riportava anche l'indicazione di contattare il numero verde qualora l'operazione non fosse stata da lui eseguita.

Faceva presente di aver contattato il numero verde dal quale l'operatore gli chiedeva se avesse disposto il bonifico e gli confermava che nulla sarebbe stato addebitato sul suo conto, guidandolo nella procedura di storno del bonifico, che eseguiva convinto dell'autenticità della telefonata.

Soggiungeva di aver ricevuto sms dall'utenza telefonica della banca, ma di essere stato informato dal sedicente operatore che il bonifico in questione fosse stato in realtà bloccato; nei giorni successivi riceveva ulteriori telefonate da un'utenza telefonica mobile, ricevendo rassicurazione sull'andamento della procedura di blocco delle operazioni sospette sul conto corrente.

Affermava di essersi recato in filiale per verificare la veridicità delle telefonate e di aver appreso in quella occasione che dal suo conto fossero stati eseguiti cinque bonifici per un totale di € 23.101,20, sottolineando che fosse stato così superato il massimale giornaliero.

Riteneva che si fosse verificata la falsificazione dei sistemi di comunicazione dell'istituto di credito, che non aveva adottato idonee misure di sicurezza; rappresentava quindi di aver sporto denuncia alle autorità e di aver disconosciuto tutte le operazioni.

Chiedeva, pertanto, il rimborso dell'importo complessivo di € 23.101,20.

Costituitosi ritualmente, l'intermediario convenuto rilevava che il cliente non avesse fatto riferimento a nessun dettaglio tra quelli che dice siano conosciuti da parte del truffatore, se non l'IBAN e le sue generalità, oltre al numero di telefono sul quale era stato contattato; sottolineava che si trattasse di informazioni che i truffatori possono recuperare in svariati modi, senza il bisogno di violare la sicurezza della banca.

Evidenziava che non fossero stati rilevati accessi sospetti da parte di terzi e che le operazioni di bonifico fossero state, seppur inconsapevolmente, disposte dal cliente autonomamente tramite la propria banca multicanale a seguito di corretta digitazione delle credenziali.

Sottolineava che le operazioni fossero risultate formalmente regolari con corretta autenticazione, validazione, registrazione e contabilizzazione, e che non si fosse riscontrata alcuna anomalia, né malfunzionamenti o intrusioni nei propri sistemi informatici.

Precisava di aver pure tentato infruttuosamente il recall dei bonifici; considerava, dunque, il cliente vittima di spoofing.

Chiedeva, pertanto, il rigetto del ricorso.

Alle controdeduzioni dell'intermediario replicava il ricorrente, il quale riteneva pacifico l'illecito trattamento dei dati personali e la violazione del diritto alla riservatezza.

Osservava che la predisposizione dell'autenticazione forte per l'operatività del conto online non rappresenta il massimo delle cautele tecnologicamente possibili, affermando che l'intermediario avrebbe già potuto applicare il servizio di Verification of Payee (VoP) e se così fosse stato fatto la truffa avrebbe potuto non verificarsi.

Considerava agevole per l'intermediario inviare ai clienti una sorta di "alert" quando le operazioni, per beneficiario, causale e/o per contesto temporale di esecuzione, presentano caratteristiche anomale rispetto alle operazioni normalmente eseguite.

Evidenziava che negli ultimi 12 mesi avesse eseguito un solo bonifico di € 80,00 e che l'intermediario nulla aveva affermato in merito al superamento dei massimali.

Le repliche della ricorrente venivano riscontate dall'intermediario, il quale insisteva nelle proprie conclusioni.

DIRITTO

La domanda proposta dal ricorrente è relativa all'accertamento del diritto alla restituzione del controvalore di alcune operazioni, 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 contestate consistono in cinque bonifici eseguiti tra il 6 ed il 7 agosto 2025, per un importo complessivo di € 23.101,20.

Dalle dichiarazioni rese dal ricorrente non è chiaro se questi abbia effettuato autonomamente i bonifici, seppure cadendo vittima dell'inganno del frodatore, ovvero se abbia contribuito con quest'ultimo a portare a termine la truffa ai propri danni; in relazione al quadro complessivamente delineato dalle allegazioni delle parti, il Collegio ritiene preferibile concludere che l'apporto causale dell'utente sia stato parziale.

Con riferimento a fattispecie analoghe l'orientamento uniforme dei Collegi ha chiarito che la transazione non deve intendersi, per ciò solo, autorizzata, poiché la normativa speciale (PSD2 e disposizioni di recepimento), prescindendo dalla nozione civilistica di "consenso", dispone che quest'ultimo dev'essere prestato nella forma convenuta tra il pagatore stesso e il prestatore dei servizi di pagamento.

Laddove, invece, l'operazione di pagamento on-line sia stata preparata dal truffatore che ha a disposizione i codici dispositivi del cliente, questa non può ritenersi eseguita per intero dal pagatore, e quindi non può considerarsi sussistente il requisito necessario per escludere il regime di responsabilità previsto dalla PSD2. Nel caso di specie, dunque, può escludersi che le operazioni possano considerarsi eseguite personalmente dalla ricorrente.

Ciò chiarito in premessa, secondo l'intermediario l'accesso all'Internet Banking sarebbe avvenuto con l'inserimento di password statiche (codice adesione e PIN) e dinamiche (OTP) (sussistendo così i fattori di conoscenza e possesso); sulla base delle tracciate informatiche in atti risulta che i fattori di autenticazione in fase di login siano stati l'inserimento del codice PIN (elemento di conoscenza) e del codice prodotto dal token Va* (elemento di possesso).

Ciò nonostante, non risultano elementi dai quali sia possibile collegare detto token fisico al cliente; tuttavia, le dichiarazioni del ricorrente – il quale ha ammesso di aver condiviso le credenziali con il truffatore – unitamente alla circostanza per cui l'autenticazione risulta interamente svolta dallo stesso indirizzo IP, lasciano presumere che sia stata rispettata la SCA in questa fase.

Quanto alla fase dispositiva dei bonifici oggi contestati, parte resistente ha affermato che le operazioni sono state autenticate tramite controllo Ma* (inserimento PIN + Token Va* + Immagine con codice autorizzativo), un processo di sicurezza, legato agli sviluppi della PSD2.

I log prodotti in atti evidenziano che le operazioni siano state autenticate mediante inserimento del codice PIN (elemento di conoscenza) e del token Va* (elemento di possesso), per il quale non risulta chiara la sua riferibilità al cliente, per quanto (come già rilevato) l'autorizzazione risulti interamente effettuata dallo stesso indirizzo IP.

A ciò si aggiunge un ulteriore duplice controllo che, secondo l'intermediario, rientra nel sistema "Ma*". In ragione delle riferite evidenze documentali, deve ritenersi dunque che pure questa fase sia stata realizzata in conformità alla SCA; pertanto, non resta che verificare se – dalla condotta tenuta dal ricorrente – non 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).

Il cliente riferisce di aver ricevuto un messaggio di autorizzazione di un bonifico di € 4.997,00. Il messaggio conteneva l'indicazione di contattare il numero indicato per ottenere informazioni, cosa che il cliente faceva. In aggiunta, riceveva anche delle chiamate provenienti da un numero di cellulare. Dall'esame delle evidenze fornite, risulta che la denominazione della chat è riferibile all'intermediario e che essa contiene un precedente messaggio concernente un prelevamento eseguito dal cliente e non oggetto di contestazione; emerge pure che tutti i messaggi presentano la stessa forma e struttura. Dall'insieme di tutti questi elementi deve concludersi che la fattispecie in esame sia riconducibile allo ID caller spoofing, il quale – secondo l'orientamento condiviso dei Collegi – conserva ancora un carattere di insidiosità, nonostante la maggiore diffusione di campagne informative sul tema. Tuttavia non mancano, nel caso di specie, elementi riconducibili alla colpa grave del ricorrente; questi, infatti, non ha prodotto evidenza in merito alla chiamata effettuata e nemmeno alle chiamate, che pure riferisce di aver ricevuto. Pertanto, non è possibile stabilire se la chiamata in questione fosse riconducibile all'intermediario resistente, non consentendo al Collegio di stabilire se la fattispecie sia qualificabile come ID caller spoofing. Peraltro, nella denuncia dichiara che la chiamata provenisse da un numero di cellulare che non risulta riconducibile all'intermediario convenuto. Deve, quindi, ritenersi sussistente la colpa grave del ricorrente. Quest'ultimo, inoltre, contesta l'avvenuto superamento dei massimali giornalieri in data 7 agosto 2025, dato che l'ammontare dei bonifici in quella giornata è stato di € 13.104,32. In atti non è presente copia del contratto; tuttavia, è presente una comunicazione del mese di settembre 2025, rilasciata dall'intermediario, avente ad oggetto i limiti in questione: da questa risulta che il limite giornaliero per i pagamenti fosse fissato ad € 10.000,00. Ciò nonostante, dai log allegati emerge che, in data 7.8.2025, prima della terza operazione dispositiva disconosciuta, è stata autorizzata una modifica dei limiti autorizzativi dei bonifici, da € 10.000,00 ad € 20.000,00 in modalità conforme a SCA, mediante PIN e Token. Il ricorso pertanto non può trovare accoglimento.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE