

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(MI) DELL'ANNA MISURALE	Membro designato dalla Banca d'Italia
(MI) PERON	Membro di designazione rappresentativa degli intermediari
(MI) SCARANO	Membro di designazione rappresentativa dei clienti

Relatore (MI) BARTOLOMUCCI

Seduta del 20/01/2026

FATTO

Il ricorrente, insoddisfatto dell'interlocuzione intercorsa nella fase di reclamo, adiva questo Arbitro deducendo di aver subito una frode, in data 11/11/2025, realizzatasi sul proprio smartphone, e all'esito della quale era stato fraudolentemente disposto un bonifico per € 5.000,00.

Faceva presente che, in quei giorni, avesse presumibilmente cliccato su un link malevolo o subito la compromissione di un account; ricordava solamente di aver ricevuto un messaggio della propria banca, che gli comunicava il prossimo arrivo di un SMS contenente il codice segreto per l'attivazione di un nuovo bancomat.

Precisava che, durante le ore serali, si fosse accorto che la schermata dello smartphone fosse bianca e funzionasse ad intermittenza, riportando la scritta "in caricamento", non risultando neppure possibile riavviare il device; soggiungeva che, solo dopo diverso tempo, lo smartphone avesse ripreso a funzionare, ma l'app bancaria risultava non funzionante e anch'essa riportava un avviso di temporanea indisponibilità.

Lamentava che, una volta effettuato l'accesso dall'app della moglie, avesse constatato l'avvenuta disposizione di un bonifico a favore di un tale a lui totalmente sconosciuto, finalizzata senza il recapito di alcun alert o richiesta di autenticazione.

Chiedeva, pertanto, il rimborso dell'importo di € 5.000,00.

Si costituiva l'odierno resistente il quale rilevava che tutte le operazioni fossero state compiute in conformità alla normativa e disposte dall'app installata sullo smartphone in uso al cliente, previamente associato all'account con doppio fattore di autenticazione.

Affermava che anche l'accesso prodromico al bonifico istantaneo e la fase dispositiva vera e propria fossero stati finalizzati mediante processo conforme a SCA, con validazione di un fattore di possesso e di un fattore di conoscenza.

Sottolineava che, dalla narrazione del ricorrente, fosse possibile desumere la sua colpa grave, dal momento che nella denuncia avesse riferito unicamente di un generico malfunzionamento dello smartphone durante l'utilizzo di una app di gioco, salvo ammettere nel ricorso di aver cliccato su un link decettivo; soggiungeva che controparte non avesse neppure circoscritto l'arco temporale e che, pur accennando all'ipotesi di un controllo da remoto del device, non avesse provato l'effettiva presenza di un malware, avendo documentato unicamente l'avvenuta formattazione del dispositivo.

Evidenziava, in ogni caso, che alle ore 20:37, il cliente avesse pure ricevuto conferma sia dell'inserimento che dell'esecuzione del bonifico istantaneo a mezzo notifica push in app, nonché a mezzo SMS al numero di cellulare certificato.

Rappresentava, da ultimo, che la filiale, informata dal cliente il giorno successivo, avesse attivato immediatamente la procedura di recall alle ore 08:43, conclusasi con esito negativo.

Chiedeva, pertanto, il rigetto in via principale del ricorso ovvero – in caso di riconoscimento di eventuali profili di responsabilità – di riconoscere sussistente un concorso di colpa ai sensi dell'art. 1227 cod. civ.

Alle controdeduzioni dell'intermediario replicava il ricorrente, il quale ribadiva che la truffa si fosse realizzata esclusivamente per il malfunzionamento dell'app bancaria e la mancata attivazione dei sistemi antifrode ad opera della banca; sosteneva che soltanto dopo l'interlocuzione con il servizio di assistenza telefonica gli fosse stato suggerito di attivare il fattore di autenticazione biometrico.

Confermava di non aver mai fornito le credenziali a terzi; evidenziava il carattere anomalo dell'operazione, poiché il bonifico contestato era stato disposto a favore di conto radicato all'estero, mentre i suoi precedenti pagamenti erano sempre stati disposti dal pc, con l'indicazione della causale, e per provvedere alle spese familiari.

Faceva pure presente che, sempre a causa di un errore operativo commesso dalla banca, nelle settimane seguenti, l'importo di € 5.000,00 relativo al bonifico in rilievo, fosse stato addebitato due volte sul rapporto di conto corrente, creando temporaneo disagio e timore.

Le repliche del ricorrente venivano riscontrate dall'intermediario, il quale – richiamando integralmente le argomentazioni addotte in sede di controdeduzioni ed insistendo per il rigetto del ricorso – precisava che il bonifico istantaneo in esame non fosse stato disposto a favore di rapporto estero, ma effettuato a favore di un conto corrente radicato in Italia.

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 sconosciute.

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 oggetto consista in un bonifico istantaneo eseguito in data 11.09.2025, alle ore 20:37, per un ammontare di € 5.000,00.

L'intermediario premette che l'accesso e l'operazione di bonifico dell'11/09/25 siano stati finalizzati sul dispositivo in uso al cliente e previamente certificato presso i sistemi della banca, per mezzo di procedura di enrollment del 23/04/25, che aveva previsto l'utilizzo di un doppio fattore di autenticazione. In particolare, la banca evidenzia l'attivazione mediante inserimento di una password e di un OTP inviato via SMS al numero di telefono certificato, attraverso i quali il cliente avrebbe potuto creare il proprio "Smart PIN" (un codice segreto impostato dallo stesso cliente) associandolo al dispositivo, poi riutilizzato per finalizzare l'operazione.

Dalle tracciate informatiche emerge sia l'inserimento della password, sia la ricezione dell'SMS contenente l'OTP sul numero di telefono del cliente. Ne deriva che la procedura di enrollment sia stata finalizzata mediante un fattore di conoscenza (la password), e un fattore di possesso (il device in uso al cliente sul quale è stato ricevuto l'OTP SMS).

Per quanto riguarda il login prodromico all'operazione di bonifico oggetto di ricorso, l'intermediario precisa innanzitutto che l'accesso sia avvenuto tramite User ID, Device e indirizzo IP già previamente

utilizzati nei mesi antecedenti alla realizzazione della frode oggetto di ricorso, e coincidenti con quelli riportati nei Log relativi alla fase di enrollment.

A tal fine, versa in atti estratto “storico” degli accessi effettuati dal cliente, da cui poter verificare la coincidenza dell’user ID, dell’NDG associato al cliente, e del device anche per gli accessi effettuati nei mesi antecedenti alla data dell’11/09/25; con riferimento a quest’ultimo, la documentazione evidenzia che, prima della disposizione di pagamento, sia stato eseguito alle ore 20:32 un login, con utilizzo del device certificato, dall’user ID del cliente con NDG associato allo stesso.

Dalle evidenze prodotte risulta che il fattore di possesso sia integrato dall’utilizzo del device previamente registrato e certificato presso i sistemi in uso alla banca, mentre il fattore di conoscenza emerge dall’inserimento dello “SMART PIN”, ossia il codice segreto impostato dal cliente durante la fase di enrollment finalizzata nei mesi antecedenti alla realizzazione della truffa (ipotesi ammessa dalle Q&A EBA 2018_4141).

Alla medesima conclusione deve pervenirsi con riguardo alla fase dispositiva del bonifico in esame; i log, infatti, evidenziano l’utilizzo del device previamente registrato e certificato presso i sistemi in uso alla banca (elemento di possesso), nonché l’inserimento dello “SMART PIN”, ossia il codice segreto impostato dal cliente durante la fase di enrollment finalizzata nei mesi antecedenti alla realizzazione della truffa (elemento di conoscenza).

Attesa la conformità a SCA del pagamento contestato, 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).

Al riguardo non può sottacersi che lo stesso ricorrente abbia ammesso come nei giorni precedenti abbia presumibilmente cliccato su un link decettivo o effettuato l’accesso ad “un account compromesso”; ha pure allegato alcuni malfunzionamenti del sistema che avrebbero impedito di verificare (ed eventualmente impedire) l’esecuzione dell’operazione disconosciuta.

Riguardo alle evidenze attestanti i malfunzionamenti riferiti, il cliente ha prodotto in atti unicamente uno screenshot riportante un avviso generico di caricamento, nonché il rapporto di intervento rilasciato dal tecnico che ha proceduto alla formattazione dello smartphone.

In base alla laconicità delle allegazioni del ricorrente e delle evidenze documentali fornite, il Collegio ritiene che lo scenario presumibile entro il quale collocare lo schema truffaldino sia quello per il quale il cliente, dopo aver cliccato su un link decettivo o aver effettuato l’accesso su una pagina web truffaldina, abbia installato una applicazione che ha reso possibile l’accesso al suo dispositivo da parte di terzi soggetti, ovvero abbia in ogni caso comunicato codici personali mediante inserimento dei dati su siti truffaldini.

Tale circostanza sembrerebbe confermata dal fatto che lo smartphone non è stato funzionante per un lasso di tempo considerevole, durante il quale terzi avrebbero potuto agire indisturbati, e che l’applicazione della banca, anche a seguito del riavvio del cellulare, non risultava più funzionante.

Deve, quindi, ritenersi che la condotta del cliente sia connotata da colpa grave; in senso contrario non può rilevare né la mancata attivazione del servizio di sms alert, trattandosi di una sola operazione, né la presunta anomalia dell’operazione, poiché (per quanto tale elemento non possa comunque avere

rilievo in sé) la banca ha comunque dimostrato che il bonifico sia stato disposto a favore di un conto radicato in Italia e non all'estero, come pure sostenuto dal ricorrente.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE