

COLLEGIO DI NAPOLI

composto dai signori:

(NA) CARRIERO	Presidente
(NA) BENEDETTI	Membro designato dalla Banca d'Italia
(NA) COCCIOLI	Membro designato dalla Banca d'Italia
(NA) MIOLA	Membro di designazione rappresentativa degli intermediari
(NA) VERDICCHIO	Membro di designazione rappresentativa dei clienti

Relatore GIANFRANCO COCCIOLI

Seduta del 11/12/2025

FATTO

I ricorrenti, infruttuoso il prodromico reclamo, chiedono all'Abf che venga riconosciuto in loro favore il diritto al rimborso di € 21.004,00, oltre € 13,20, quale commissione per bonifico estero.

Sostengono di essere titolari del conto corrente acceso presso una filiale dell'intermediario resistente, sul quale, in data 16/01/2025, alle ore 03:00 circa, veniva eseguito un bonifico bancario estero di € 21.004,00, oltre € 13,20 a titolo di commissione in favore del Sig. M.D., apparentemente con l'app di *Home Banking* installata esclusivamente sull'utenza mobile ad esso collegata.

Deducono di non avere autorizzato tale operazione e di non conoscere chi ne risulta beneficiario.

Nel ricorso si precisa ulteriormente che la conoscenza dell'operazione era avvenuta soltanto il successivo 28/01/2025, alle ore 18:55 circa, allorché, nel prelevare presso uno sportello ATM, era richiesto un estratto di conto corrente,

Verificata la sottrazione dell'ingente somma di danaro e contattato il Servizio Clienti della banca, che, preso atto della segnalazione, provvedeva all'immediato blocco del conto, in data 29/01/2025 era presentata denuncia penale e ne veniva trasmessa copia con richiesta di rimborso alla controparte che, tuttavia, non l'accoglieva, adducendo una generica motivazione, nonostante la manifesta l'inefficienza del sistema di sicurezza.

L'intermediario, previa sua costituzione, eccepisce che la denuncia non contiene una precisa e circostanziata ricostruzione della vicenda che risulta priva di dettagli indispensabili ai fini di verificare le

modalità di consumazione dell'allegata frode.

Evidenzia che la denuncia generica è considerata negativamente dai collegi dell'Abf e dal Collegio di Coordinamento, potendo essere sintomo di reticenza funzionale all'occultamento della reale dinamica dei fatti .

Precisa, quanto al sistema di sicurezza, che il servizio "*Rapporti a distanza tra Banca e Cliente*" prevede l'accesso alle funzioni di *inquiry* e dispositive mediante un sistema di autenticazione "forte" in linea con la normativa europea PSD2, assicurato da un numero cliente , dal codice statico noto solo al cliente costituito da un Pin e da un codice OTP, codice dinamico e temporaneo generato da Mobile Token.

Per disporre le operazioni, dopo avere effettuato la login come sopra e inserita l'operazione, ne è garantita la conferma mediante l'inserimento del PIN + codice OTP (One Time Password) generato da Mobile Token . Si tratta di autenticazione "a due fattori", riconosciuto come sistema forte anche dall'orientamento diffuso dei Collegi ABF.

La banca aggiunge che, al fine di prevenire possibili frodi in danno alla clientela, da tempo raccomanda la massima attenzione e cautela nell'utilizzo dei canali telematici, pubblicando avvisi specifici nella pagina di accesso al portale, sulla App e sugli schermi degli ATM, nei quali si avverte la clientela anche del fatto che nessun dipendente della Banca chiederà mai le credenziali di sicurezza, strettamente personali e, pertanto, non comunicabili mai a terzi. Inoltre, nell'estratto del conto corrente al 30/06/2022 , inviato a tutta la clientela, era allegata la comunicazione delle "*regole e comportamenti per operare in sicurezza*", nella quale erano riportati i suggerimenti per evitare di incorrere in comunicazioni fraudolente via telefono, e-mail o SMS.

L'operazione disconosciuta è stata inserita ed autorizzata con le credenziali di sicurezza del ricorrente, come dimostrato nei LOG. Il tipo di operatività disconosciuta si rende possibile solo nel caso in cui sia stato il cliente stesso a rivelare in qualche modo le credenziali di sicurezza dell'home banking, via email, sms o via telefono, o sia stato raggirato da una telefonata di *phishing*, comunicando e/o inserendo le proprie credenziali di sicurezza, e permettendo a soggetti estranei di accedere alle informazioni personali del suo conto corrente. Dalle verifiche effettuate non è emerso alcun malfunzionamento o compromissione dei sistemi: l'operazione risulta correttamente autenticata, registrata e contabilizzata (così come previsto dall'art. 10 del D. Lgs. n. 11/2010), come dimostrato nelle evidenze LOG attività da App (all. 2).

Infine, riguardo alla richiesta di rimborso delle spese legali, la banca segnala che nessuna assistenza di tipo professionale è espressamente richiesta per la presentazione di un ricorso ABF; in merito alla richiesta di risarcimento danni, precisa che deve ritenersi non accoglibile, in virtù di un orientamento consolidato dei Collegi ABF - anche di Coordinamento e persino della giurisprudenza di merito e di legittimità – perché, ai sensi dell'art. 2697 c.c., non è data prova dell'an e del quantum debeatur nè del nesso di causalità tra presunta condotta illegittima della Banca ed asserito danno subito dal ricorrente. Nelle repliche e controrepliche le parti hanno sostanzialmente confermato le primigenie difese.

DIRITTO

Il ricorso merita parziale accoglimento.

A fronte del disconoscimento delle operazioni effettuate , incombe sul prestatore di servizi di pagamento l'onere di provare che esse siano state autenticate, correttamente registrate e contabilizzate ai sensi dell'art. 10, comma 1, del d.lgs. 11/2010, *ratione temporis* qui applicabile , a tenore del quale: "Qualora l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento è stata autenticata,

correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti”. Ai sensi del secondo comma dell’articolo richiamato, la dimostrazione che l’operazione è stata eseguita correttamente, secondo quanto ne dice il primo comma, non esonera il prestatore di servizi di pagamento dall’obbligo di rispondere in caso di operazioni sconosciute, dovendo egli anche provare che l’utente ha agito con frode, dolo o colpa grave.

Va anche tenuta presente la disciplina del d. lg. 27 gennaio 2010, n. 11, risultante dalla modifica apportata ad esso dal d.lgs. 15 dicembre 2017, n. 218 di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2) in vigore dal 13.01.2018.

In particolare, la c.d. strong customer authentication (cd. SCA) è disciplinata dagli artt. 97 e 98 della PSD2, dall’articolo 10 bis del D. Lgs. n. 10/2011 e dalle norme tecniche di regolamentazione, emanate dall’EBA e recepite con Regolamento Delegato Ue 2018/389 della Commissione Europea, applicabile a far data dal 14 settembre 2019, nonché dai criteri interpretativi forniti dall’EBA e, in particolare, dal parere dell’EBA del 21 giugno 2019.

In tal senso si è espresso il Collegio di Coordinamento (decisione n. 22745 del 10 ottobre 2019), secondo cui l’onere probatorio previsto nei commi 1 e 2 dell’art. 10 del decreto richiamato deve necessariamente essere assolto dal PSP con riguardo ad ambedue i profili (autenticazione ed esecuzioni delle operazioni di pagamento, nonché colpa grave dell’utilizzatore), da considerarsi necessari e complementari.

Alla stregua di ciò, come chiarisce ulteriormente il Collegio di Coordinamento nella predetta decisione, la previsione di cui all’art. 10, comma 2, del d. lgs. n. 11/2010, in ordine all’onere posto a carico del PSP della prova della frode, del dolo o della colpa grave dell’utilizzatore, va interpretata nel senso che la produzione documentale diretta a fornire la dimostrazione dell’autenticazione” e della formale regolarità dell’operazione contestata non esaurisce, di per sé, l’onere probatorio, in quanto è indispensabile che l’intermediario provveda specificatamente ad indicare una serie di elementi di fatto caratterizzanti le modalità esecutive dell’operazione, sulla cui base possa trarsi la prova della colpa grave dell’utente.

Se ne arguisce che, nel caso in cui l’intermediario costituito abbia fornito prova dell’autenticazione e della regolarità formale dell’operazione, il collegio possa affermare la sussistenza della colpa grave sulla base di prove dirette oppure di elementi presuntivi, in grado di determinare inferenze logiche, tanto più incisive se sostenute dall’*id quod plerumque accidit*.

Invero, la possibilità che la prova della colpa grave derivi da presunzioni è legittimata dall’art. 2729 cc che, pur se inserito nel codice civile, ha natura processuale, perché fornisce al giudice uno strumento di valutazione da utilizzare ai fini della decisione, stabilendo che egli non deve ammettere che presunzioni gravi, precise e concordanti. La stessa corte di cassazione ha avuto modo di esprimersi in senso positivo circa la verifica della sussistenza della colpa grave in fattispecie analoghe sulla base di elementi presuntivi, purché aventi le caratteristiche predette di gravità, precisione e concordanza come impone la disposizione richiamata (cfr. Cass. civ., Sez. II, 18 gennaio 2010, n. 654).

Ciò precisato in linea generale, va detto che, nel caso di specie, può considerarsi compiutamente assolto l’onere relativo al primo profilo probatorio. L’intermediario, infatti, ha fornito piena dimostrazione della corretta autenticazione, registrazione e contabilizzazione delle operazioni in esame che si sono svolte nel contesto di un sistema di sicurezza (autenticazione forte o SCA) conforme alle rigorose indicazioni contenute nelle normative di riferimento (artt. 97 e 98 della “PSD2”, art. 10 bis del d.lgs. 10/2011 e nelle norme tecniche di regolamentazione emanate dall’EBA e recepite con Regolamento Delegato UE 2018/389 della Commissione Europea, applicabile a far data dal 14 settembre 2019, nonché nei criteri interpretativi forniti dall’EBA).

Dalle evidenze informatiche messe a disposizione del Collegio si ricava che l’operazione contestata risulta eseguita con sistema di autenticazione a due fattori (SCA), con modalità di autorizzazione che consistono nell’inserimento dei dati del bonifico in App su device certificato con conferma tramite PIN .

Dalla strumentazione impiegata ai fini dell'esecuzione del bonifico si ricava che è stato utilizzato anche l'otp (password temporanea) generato dal Mobile Token.

Chiarito che, in effetti, il bonifico è stato eseguito in data 16.1.2025 in piena notte alle ore 03:14, come si desume anche dai log allegati, occorre precisare al riguardo che, sulla base delle evidenze informatiche depositate dalla banca, non contestate in maniera circostanziata dalla parte ricorrente e, dunque, suscettibili di essere poste a fondamento di questa decisione, ai sensi dell'art. 115 cpc, emerge che il bonifico in contestazione è stato autorizzato dal device già associato al profilo del ricorrente, utilizzato in precedenza per attività mai disconosciute dai ricorrenti, a dimostrazione della regolarità del sistema.

Tuttavia, l'intermediario non ha dedotto e comprovato esistenza ed attivazione di un sms alert. Vero che si tratta di un'unica operazione, non può disconoscersi però che, avendo parte ricorrente precisato di essersi accorta della truffa soltanto il 28.gennaio 2025, mentre la sottrazione è avvenuta la notte del 16 precedente, l'attivazione del servizio di alert immediato avrebbe potuto richiamare l'attenzione di parte ricorrente sull'utilizzo ad opera di terzi non autorizzati degli strumenti di pagamento, anche ai fini di un'eventuale revoca dell'ordine di bonifico.

Sul punto, soccorre la decisione n.24366/2019 del Collegio di Coordinamento ABF che ha avuto modo di chiarire che *"Fra i doveri di protezione dell'utente gravanti sull'intermediario rientra l'onere di fornire il servizio di sms alert o assimilabili da cui l'intermediario può essere esonerato solo dimostrando l'esplicito rifiuto dell'utente ad avvalersene. Gli effetti della mancata adozione del servizio di alert dovranno essere valutati alla stregua delle circostanze di fatto del caso concreto"*.

Si precisa, al riguardo, che - sulla base degli orientamenti condivisi dai Collegi territoriali dell'Arbitro - è stata confermata la posizione assunta dal Collegio di Coordinamento sul servizio di sms-alert, ritenuto fondamentale presidio di sicurezza a tutela dell'utente, anche in considerazione dell'obbligo di buona fede nell'esecuzione del contratto; pertanto, la mancata attivazione del servizio di sms-alert o altro servizio assimilabile – con una valutazione di equivalenza tra i due servizi da condurre caso per caso (ad es. notifica tramite app dell'intermediario o tramite e-mail) – costituisce generalmente un profilo di responsabilità dell'intermediario (da inadeguata organizzazione imputabile esclusivamente al medesimo intermediario), da cui questi può andare esente solo dimostrando l'esplicito rifiuto dell'utente ad avvalersene.

Pertanto, non va trascurato che una più efficace organizzazione del servizio da parte dell'intermediario avrebbe potuto consentirgli di intraprendere incisivamente un tentativo di recupero, di cui in atti non vi è prova.

E questa inerzia è tanto più grave, ove si consideri che l'importo del bonifico è particolarmente rilevante, mentre i movimenti del conto sono generalmente di esigua entità, come dimostra la documentazione prodotta, sicché sarebbe stato agevole comprendere che l'operazione disconosciuta era fortemente anomala.

Per contro, la circostanza che la vicenda sia stata approssimativamente ricostruita nella denuncia, senza che in merito siano stati forniti ragguagli precisi e circostanziati in grado di far comprendere come abbia potuto il terzo utilizzare le credenziali, di cui unici custodi erano i ricorrenti, genera dubbi sulla loro correttezza, come dimostra anche la circostanza che nella denuncia, chiarito che poco prima vi erano stati mal funzionamenti del telefono, non risulta indicato il compimento di atti diretti a verificarne l'origine, pur essendovi consapevolezza che il telefono, in quanto dotato di app della banca, poteva formare oggetto di intrusioni dannose da parte di terzi finalizzate alla sottrazione dal conto di danaro. Ed in proposito vanno richiamati gli orientamenti condivisi dei Collegi che, con riferimento agli utilizzi fraudolenti *on line* non circostanziati dall'utilizzatore, hanno avuto modo di precisare che, ove l'intermediario offre la prova dell'autenticazione delle transazioni disconosciute, con conseguente dimostrazione che il sistema di pagamento risulta conforme alla *Strong Customer Authentication* (SCA) e senza indizi di anomalia delle operazioni e/o ulteriori elementi, le mancate allegazioni del cliente in

ordine a circostanze di fatto della frode, asseritamente subita, rappresentano un elemento da cui il Collegio può trarre il proprio convincimento, insieme ad altre circostanze, circa la configurabilità di una sua colpa.

In conclusione, il collegio ritiene che vi siano concorrenti responsabilità nella determinazione causale dell'evento, sicché, tenuto conto di tutte le circostanze sopra evidenziate, appare rispondente alla reale entità delle colpe di ciascun litigante riconoscere in favore di parte ricorrente un terzo del richiesto, pari alla somma di € 6.301,00, oltre i chiesti interessi legali dal reclamo.

Non ha fondamento la domanda relativa agli altri supposti pregiudizi anche non patrimoniali: come precisato dalla giurisprudenza anche della Cassazione e dal conseguente costante orientamento dei collegi, va escluso un danno *in re ipsa*, sicché chi ne invoca il riconoscimento deve dimostrarlo.

A ciò va aggiunto che la liquidazione equitativa di cui all'art. 1226 cc, secondo la sua piana formulazione, non può essere riconosciuta se non in caso di impossibilità di fornire la prova del danno. Si tratta all'evidenza di norma eccezionale, in quanto derogatoria rispetto alla regola generale dettata dall'art. 2697 cc che pone a carico delle parti l'onere di provare i fatti oggetto delle rispettive domande ed eccezioni, in chiara applicazione del principio dispositivo che permea di sé l'intera disciplina delle controversie civili.

Consequentemente deve farsene interpretazione restrittiva ai sensi dell'art. 14 delle preleggi. Pertanto non può predicarsene l'applicazione, se la prova, come qui, poteva essere fornita.

Il ricorrente domanda altresì la rifusione delle spese di assistenza professionale. In proposito il Collegio evidenzia che le "Disposizioni sui sistemi di risoluzione stragiudiziale delle controversie in materia di operazioni e servizi bancari e finanziari" non prevedono la necessaria presenza di un legale per assistere il cliente davanti all'Arbitro Bancario Finanziario.

Ma va considerato che la recente decisione n. 4580 del 2025 del collegio di Coordinamento non esclude che, in relazione a particolari situazioni, possa ammettersi l'esigenza di una difesa tecnica, con conseguente rimborsabilità della relativa spesa, chiarendo che all'uopo vanno prese in considerazione le circostanze specifiche del caso concreto.

Orbene, tenuto conto che nella fattispecie in disamina vi è un palese concorso di colpe e che la difesa non era assolutamente necessaria, come dimostra la constatazione che l'impostazione difensiva si è fondata sostanzialmente su quanto oggetto di denuncia proposta dalla parte sostanziale, ritiene il collegio di escludere la possibilità di riconoscere le chieste spese.

P.Q.M.

In parziale accoglimento del ricorso, il Collegio accerta il diritto del ricorrente al risarcimento del danno per l'importo di € 6.301,00, oltre interessi legali dalla data del reclamo nei sensi di cui in motivazione.

Il Collegio dispone inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di € 200,00 quale contributo alle spese della procedura e al ricorrente la somma di € 20,00 quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE