



COLLEGIO DI BOLOGNA

composto dai signori:

(BO) TENELLA SILLANI	Presidente
(BO) PAGNI	Membro designato dalla Banca d'Italia
(BO) BULLO	Membro designato dalla Banca d'Italia
(BO) LUCARELLI	Membro di designazione rappresentativa degli intermediari
(BO) DI NELLA	Membro di designazione rappresentativa dei clienti

Relatore LORENZA BULLO

Seduta del 20/10/2025

FATTO

Parte ricorrente espone quanto segue:

- in data 16/01/2025 riceveva una chiamata da un'utenza fissa riferibile all'odierno convenuto e parlava con un sedicente operatore del medesimo convenuto;
- l'interlocutore lo informava dell'esecuzione di alcune operazioni sospette sulla sua carta di credito, già bloccata, e della disposizione di bonifici immediati da parte di un *device (smartphone)* di cui indicava marchio e modello – I*7;
- l'interlocutore gli riferiva che avrebbe bloccato tali bonifici per 24 ore e che avrebbe rimosso le autorizzazioni dal suddetto dispositivo mobile;
- riceveva, quindi, degli sms che lo avvisavano dell'avvenuta rimozione delle autorizzazioni al suddetto dispositivo e lo invitavano, altresì, a seguire le istruzioni del proprio interlocutore, identificandolo con il nome ed il cognome con cui lo stesso si era presentato al telefono;
- successivamente, nel corso della telefonata, l'interlocutore gli spiegava che, per potere completare il blocco delle operazioni, era necessario seguire un iter specifico *e, pertanto, lo induceva ad effettuare diverse disposizioni di bonifico per stornare altrettante operazioni non autorizzate*, dettandogli per telefono i nomi e i cognomi dei beneficiari e i relativi IBAN;

- in particolare, in data 16/01/25 e 17/01/25 *effettuava n. 65 bonifici, per un importo complessivo di € 30.000,00;*
- in corrispondenza della disposizione dei bonifici, riceveva degli sms (33 totali) che lo informavano dell'avvenuto blocco delle operazioni sospette;
- la ricezione di tali sms avveniva all'interno della chat di messaggistica dell'intermediario convenuto, nella quale si trovavano anche messaggi genuini;
- gli sms non contenevano errori grammaticali o sintattici;
- un'operatività di € 30.000,00 in due giorni è del tutto incoerente rispetto a quella sua ordinaria; tale anomalia avrebbe dovuto essere rilevata dall'intermediario convenuto che, di conseguenza, avrebbe dovuto attivare un sistema di blocco automatico delle operazioni;
- era vittima di un episodio di truffa molto sofisticato del tipo spoofing: in particolare, l'impiego di tecniche di sms spoofing combinate e coordinate con tecniche di caller ID spoofing creava un incolpevole affidamento sulla veridicità dell'allerta di violazione del suo conto corrente, rendendogli del tutto impercettibile la truffa ed escludendo la sua colpa;
- il suo interlocutore conosceva il suo numero di telefono cellulare riferibile al conto corrente ed il numero di carta, sicché può affermarsi che l'intermediario non attuava misure idonee a prevenire e scongiurare la perdita dei dati dei clienti;
- l'intermediario convenuto deve essere ritenuto responsabile anche in base all'art. 2050 c.c. in combinato disposto con l'art. 15 del D.Lgs. n. 196/2003, dal momento che non ha adottato tutte le misure idonee a proteggere i suoi dati personali e, pertanto, ad evitare il danno: l'intermediario che gestisce servizi di home banking, quale titolare del trattamento dei dati, deve impedire, infatti, la violazione dei medesimi e la loro fraudolenta captazione da parte di terzi;
- in sede di risposta al reclamo, l'intermediario si limitava a formulare un'offerta di rimborso di € 9.000,00, così ammettendo la propria negligenza nell'approntare idonei sistemi di sicurezza, ma senza dare conto di alcun accertamento svolto sulle operazioni disconosciute.

Parte ricorrente chiede pertanto all'Arbitro, accertata la responsabilità contrattuale ed extracontrattuale dell'intermediario convenuto, di condannarlo al risarcimento del danno quantificato in euro 30.000,00, somma pari alle operazioni disconosciute oltre ad interessi dalla data dell'operazione al saldo e rimborso delle spese del procedimento pari ad euro 20,00.

L'intermediario resiste alla pretesa contro deducendo quanto segue:

- le operazioni oggetto di frode risultano essere 61; sono state eseguite con la modalità del bonifico istantaneo, eccetto una inserita con la modalità "bonifico Italia", per un totale di € 29.700,00;
- il ricorrente è titolare del c/c cointestato n. *836, al quale è collegato il servizio di *home banking*, intestato al ricorrente e collegato alla sua utenza telefonica mobile, attraverso il quale è possibile effettuare operazioni dispositive;
- la fattispecie oggetto di ricorso non ricade nell'ambito di applicazione del regime di protezione previsto dal D.Lgs. n. 11 del 2010, *in quanto i bonifici sono stati autorizzati personalmente dal ricorrente;*
- in ogni caso, *le operazioni contestate sono state correttamente autorizzate mediante un sistema di autenticazione forte*: per effettuare il login all'app di home banking, occorre l'inserimento delle credenziali di sicurezza del cliente (numero cliente e pin) e l'inserimento di un codice OTP generato da mobile token; per disporre le operazioni, poi, è necessario inserire il pin e un codice OTP, che è generato in app da mobile token, che il cliente deve "tappare" per autorizzare l'operazione;

- predispone avvisi specifici sul tema delle frodi informatiche sul proprio sito internet, in app, sugli schermi degli sportelli ATM, nonché attraverso comunicazioni specifiche inviate alla clientela in allegato agli estratti conto;
- il comportamento tenuto dal ricorrente è connotato da colpa grave, dal momento che: il ricorrente dava credito – senza effettuare alcun tipo di verifica o controllo – a quanto riferito dal proprio interlocutore telefonico circa l'esecuzione di bonifici sospetti sul suo conto e ne seguiva acriticamente le istruzioni; gli sms ricevuti si inserivano in una chat di messagistica solo apparentemente a sé riconducibile, sono formulati in termini generici e caratterizzati da un tono elementare non coerente con le normali comunicazioni banca-clienti; appare del tutto anomala – e in grado di generare sospetti in una persona mediamente accorta – la circostanza che per bloccare delle operazioni in uscita si debbano eseguire bonifici; il ricorrente avrebbe potuto rendersi agevolmente conto della falsità degli sms che lo informavano dell'avvenuto blocco delle operazioni sospette con la semplice consultazione della lista movimenti in app;
- la tecnica del c.d. caller ID spoofing deve considerarsi oggi nota, come dimostra l'attenzione su di essa posta dall'AGCOM e dalla polizia giudiziaria;
- durante l'inserimento di disposizioni di pagamento, nelle app dei clienti compare un apposito alert che raccomanda la massima attenzione nel disporre operazioni durante conversazioni telefoniche con persone che si presentano come operatori bancari;
- in corrispondenza dei bonifici per cui è ricorso, inviava sms e notifiche alert al ricorrente;
- avviava prontamente l'azione di recall verso la banca corrispondente, la quale, tuttavia, può addebitare il conto corrente del suo cliente solo se autorizzata dallo stesso oppure a seguito di provvedimento di sequestro dell'Autorità giudiziaria;
- “al solo fine di salvaguardare il rapporto con i clienti, nonché di concludere la vertenza *“pro bono pacis”*, reitera la propria disponibilità – già dichiarata in sede di risposta al reclamo – a *rimborsare l'importo di € 9.000,00 (comprensivo di € 20,00 per spese di presentazione ricorso)*.”

L'intermediario conclude pertanto: a) *in via principale*, per il rigetto del ricorso in quanto infondato nel merito; b) *in via subordinata*, di accoglierlo nel limite della somma proposta dalla Banca al Cliente in sede di riscontro al reclamo.

Seguono *repliche e contro repliche* in forza delle quali:

parte ricorrente insiste per l'accoglimento del ricorso, precisando quanto segue:

- i log prodotti in sede di controdeduzioni sono del tutto parziali, non certificati e illeggibili, con conseguente mancata prova della SCA;
- in particolare, i log si presentano sotto forma di estrazione, parziale, di dati su un file in formato PDF e non Excell; non consentono di verificare la consegna effettiva dei codici OTP e il relativo inserimento; mostrano poi l'alternanza di invio di sms (canale cellulare) e notifiche push (canale app) senza però mostrare chi ne sia stato l'effettivo destinatario e soprattutto perché vi sono due diversi processi di creazione di OTP e due diverse modalità di consegna;
- nei log, in molti casi, si è in presenza di doppie notifiche generate, per la stessa operazione, a distanza di pochi secondi, ciò che fa presumere che le notifiche push siano state inviate anche ad un ulteriore dispositivo;
- i log, inoltre, evidenziano chiari indici di anomalia e fraudolenza nella operatività del conto corrente, in particolare ripetuti fallimenti di accesso alla fase di login, che avrebbero dovuto essere accertati e bloccati dalla banca convenuta;

- le operazioni sono state poste in essere a distanza di pochi minuti l'una dall'altra e con frequenza anomala rispetto a quella ordinaria, con l'effetto di rilevare un palese attacco informatico al suo conto on line.

parte resistente insiste per il rigetto richiamando sinteticamente le argomentazioni già svolte nelle controdeduzioni e ribadisce l'inapplicabilità della disciplina normativa di cui al D.Lgs. n. 11/2010 *dal momento che il ricorrente ha eseguito personalmente i bonifici* e precisa che dai log prodotti si evince non solo il codice OTP inviato al cliente, ma, anche, *che gli accessi e le operazioni sono stati eseguiti dal dispositivo del cliente, come d'altronde confermato da quest'ultimo in denuncia*. Riafferma la propria disponibilità alla corresponsione, a titolo di rimborso, dell'importo di € 9.000,00.

DIRITTO

Parte ricorrente contesta l'esecuzione di n. 65 bonifici, eseguiti parte in data 16/01/2025 e parte in data 17/01/2025, per un totale complessivo, a detta del ricorrente, di circa euro 30.000,00.

Il Collegio rileva, tuttavia, che dall'estratto conto allegato al ricorso, nelle date del 16/01/2025 e 17/01/2025, risultano contabilizzati e quindi arrivati a destinazione *n. 60 bonifici istantanei* (di cui n. 59 di € 490,00 ciascuno e n. 1 di € 300,00), per un totale di € 29.210,00, escluse le spese per bonifico istantaneo. In particolare, n. 30 bonifici risultano essere stati eseguiti in data 16/01/25 e n. 30 bonifici risultano essere stati eseguiti in data 17/01/25.

L'intermediario convenuto, *nelle controdeduzioni*, afferma invece che i bonifici eseguiti sono in realtà n. 61, per un totale complessivo di € 29.700,00 (escluse spese per bonifico istantaneo); effettivamente, dai logs prodotti dall'intermediario convenuto (all. 5bis alle controdeduzioni) emerge un numero complessivo di bonifici pari a 61, per un totale di € 29.700,00, escluse le spese per bonifico istantaneo (n. 60 bonifici di € 490,00 cad.; n. 1 bonifico di € 300,00). In particolare, n. 30 bonifici sono stati eseguiti il 16/01/25 a partire dalle ore 19.09 sino alle ore 22.16, mentre n. 31 bonifici sono stati eseguiti in data 17/01/25 a partire dalle ore 7.03 sino alle ore 9.51 a favore di vari nominativi.

Dalle tracciatore in atti, oltre ai citati 61 bonifici andati a buon fine, risultano altresì anche altri n. 5 bonifici in data 17/01/25 che però non sono andati a buon fine in quanto rifiutati (all. 5bis controdeduzioni).

In denuncia, diversamente da quanto affermato nel reclamo e nel ricorso, è lo stesso ricorrente a dichiarare in modo espresso che i bonifici sono stati eseguiti personalmente dallo stesso sia pure a ciò indotto dalla truffa perpetrata in suo danno. Tale dichiarazione confessoria del cliente assume, secondo l'orientamento dei Collegi ABF, valore di prova legale ai sensi dell'art. 2730 c.c.

Parte resistente, sin dalle controdeduzioni, eccepisce l'inapplicabilità al caso in esame della disciplina di diritto speciale di cui al D. Lgs. n. 11/2010 e s.m.i. in quanto tutte le operazioni disconosciute sono state personalmente ed integralmente eseguite dal ricorrente, come lo stesso ha peraltro poi riconosciuto anche in denuncia: difetta pertanto l'"assenza di consenso del pagatore" di cui all'art. 5 del citato D. Lgs. n. 11/2010 e s.m.i. affinché si possa trattare di "operazioni non autorizzate" per le quali vale la disciplina di settore sopra citata.

Come è noto e ribadito dal Collegio di Milano nella decisione n. 5542/2024 relativa anch'essa ad un episodio di social hacking " là dove sia *direttamente l'utilizzatore, pur indotto da istruzioni manipolative di terzi truffatori, a disporre o autorizzare le operazioni di pagamento, non trova applicazione la disciplina relativa alle operazioni non autorizzate, poiché – per contro – l'operazione è pacificamente autorizzata dall'utilizzatore (art. 5 d.lgs. n. 11/2010)*. Ciò comporta che l'intermediario è esonerato dall'onere di provare i) *l'autenticazione forte ex art. 10-bis d.lgs. n. 11/2010 (v. ad es. Coll. Milano dec. n. 1864/2023; Coll. Roma, dec. n. 702/2023) e ii) la colpa grave del ricorrente ex art. 12, comma 3, d.lgs. n. 11/2010.*"

Parte resistente afferma che il ricorrente è intestatario del servizio di *home banking*, con cui può effettuare operazioni dispositive sul conto corrente di cui è titolare assieme alla sig.ra P*L*. Il servizio di home banking è collegato all'utenza telefonica n.*801 del ricorrente, come dimostra la Scheda Cliente in atti. Dalla lettura dei logs depositati in atti si evince inoltre che tutta l'attività di *login in app* prodromica alle operazioni dispositive di bonifico nei giorni 16 e 17 gennaio 2025 è sempre stata effettuata con il dispositivo identificato dal codice *928B, dispositivo collegato in modo univoco al ricorrente e al suo conto. Il suddetto device n. *928B, riportato nelle tracciatore (colonna *Device Name* e *Descrizione Device*) corrisponde a quello utilizzato dal ricorrente anche per operazioni non disconosciute: il dispositivo come sopra identificato, infatti, risulta essere stato *altresì utilizzato per operazioni in app in date anteriori e successive alle giornate in cui sono stati disposti i bonifici per cui è ricorso* (16/01/25 e 17/01/25), come si desume dalla lettura dei logs riportati nell'all. 5 alle controdeduzioni.

Il suddetto numero di device (*928B) è il *solo* riportato nei logs: ne consegue l'irricevibilità dell'ipotesi formulata dal ricorrente di avvenuta associazione di un ulteriore dispositivo all'app: anche i 5 tentativi di accesso effettuati alle ore 16:20 del 16/01/25 sono tutti riconducibili al codice ID utente n. *905 e al device *928B. Anche il suddetto codice ID utente *905 risultante nei logs depositati in atti corrisponde a quello riportato nei dati cliente indicati nelle controdeduzioni.

Alla luce della documentazione in atti, risulta pertanto adeguatamente comprovata l'associazione di un unico dispositivo all'app, quello del ricorrente che peraltro ammette di aver personalmente eseguito i bonifici del 16 e 17 gennaio 2025 poi disconosciuti. Sulla base delle dichiarazioni e della documentazione presentata, le operazioni per cui è ricorso risultano pertanto tutte personalmente autorizzate dal cliente: non trova dunque applicazione la disciplina di settore di cui al Dlgs 11/2010 con la conseguenza che l'intermediario non deve fornire né prova della sca, né della colpa grave del cliente per andare esente da responsabilità.

I Collegi ABF escludono infatti l'applicazione del regime di protezione previsto dal D.Lgs. n.11/2010 in caso di operazioni disposte ed autorizzate *personalmente* dal titolare dello strumento di pagamento e ciò anche se alla base dell'autorizzazione personale, come nel caso in esame, sussiste un consenso viziato dagli artifici e raggiri posti in essere da un truffatore. Rientrano in questa fattispecie, in particolare, le operazioni eseguite dal pagatore seguendo le indicazioni del frodatore, pur senza la consapevolezza di disporre una transazione (ad esempio, le c.d. operazioni "sotto dettatura"). Tuttavia, fermo che in caso di operazioni compiute direttamente dal cliente l'intermediario è esonerato dalla prova di autenticazione e non è configurabile una responsabilità oggettiva a suo carico, *resta la possibilità del Collegio di verificare comunque una eventuale responsabilità concorrente del Prestatore dei Servizi di Pagamento (PSP) secondo le norme di diritto comune*, qualora emerga dalla documentazione in atti un apporto causale dell'intermediario alla frode. Ciò si ritiene si verifichi, in particolare, nei casi: di mancata disponibilità (anche temporanea) del numero verde del PSP, che impedisca all'utente di accertare in via preliminare la genuinità delle indicazioni fornite dal frodatore; di

mancata identificazione del tentativo di frode in corso da parte del dipendente del PSP, cui il pagatore si sia rivolto esponendo le richieste del frodatore; di mancato rilievo di indici di frode nel caso in cui il cliente sia stato indotto dal frodatore a disporre dei pagamenti nella convinzione di effettuare degli accrediti in conto, mentre la ricezione di alert o il blocco delle transazioni lo avrebbero reso consapevole dell'effettiva natura delle operazioni realizzate, ipotesi tutte non integrate nel caso in esame.

Tali principi sono stati recentemente ribaditi anche dal Collegio di Coordinamento nella decisione n. 8671/2024: *“..... Come si è premesso, i pagamenti interamente eseguiti dal titolare dello strumento di pagamento non rientrano, secondo il consolidato orientamento dell'Arbitro, nella fattispecie della responsabilità oggettiva del prestatore di servizi di pagamento per le operazioni non autorizzate dai clienti: fattispecie che, come ha sottolineato la Corte di Giustizia nella decisione del 2 settembre 2021, causa C-337/20 (DM, LR contro Caisse régionale de Crédit agricole mutuel (CRCAM) – Alpes-Provence), è disciplinata in via esclusiva dal d. lgs n. 11/2010. Ciò non impedisce, tuttavia, che proprio in quanto sottratti al perimetro di operatività della normativa ora citata, i danni subiti dal cliente per i pagamenti da lui “autorizzati” possano, in astratto, essere risarciti ai sensi dell'art. 1218 c.c., qualora sia dimostrata la negligenza dell'intermediario nell'adempimento di obblighi contrattuali. Ciò può verificarsi, in particolare, se sia accertata l'omessa adozione di misure di sicurezza e di monitoraggio adeguate a contrastare scenari di truffa dotati di una tipicità sociale (per esempio, in caso di mancata valorizzazione di indici di frode, là dove il cliente sia stato indotto dal truffatore a disporre dei pagamenti nella convinzione di effettuare accrediti in conto, mentre la ricezione di alert o la sospensione delle transazioni gli avrebbe consentito di acquisire consapevolezza della frode e di evitarne il perfezionarsi). Nel caso di specie, tuttavia, non si ravvedono evidenti profili di negligenza nella condotta dell'intermediario, mentre il fatto colposo della parte ricorrente - recatasi di persona a effettuare i versamenti in filiale, presso uno sportello presidiato da un dipendente e omettendo di esporre a quest'ultimo le richieste del frodatore - assorbe il rilievo causale di qualsiasi inadempimento della banca”.*

Applicando i suddetti principi al caso in esame, il Collegio rileva quanto segue:

i bonifici sono, a detta del ricorrente, l'esito di una truffa iniziata in data 16.1.2025 con una *telefonata da un'un'utenza fissa riconducibile alla banca convenuta* con la quale il ricorrente è stato informato dell'esecuzione di operazioni sospette sul suo conto, in particolare di svariati bonifici immediati, da parte del possessore di un *device (smartphone)* I*7; detta truffa è durata quantomeno dalle 16.20 (primi bonifici tentati ma non andati a buon fine) del 16.1.2025 sino alle ore 10 circa del 17.1.2025 quindi per circa 18 ore. Già da tale lungo lasso temporale di asseriti artifici e raggiri, comprensivo di una notte, il Collegio desume un elemento di colpa grave del ricorrente, non giovando a suo favore alcun effetto sorpresa della truffa.

Il Collegio rileva altresì che non essendo prodotta in atti dal ricorrente evidenza della chiamata ricevuta, non può desumersi né ora, né durata della telefonata né prova della stessa: *manca pertanto la prova dell'esistenza di una fattispecie (insidiosa) di vishing caller ID spoofing*. Nel corso della asserita ma non provata telefonata, l'interlocutore avrebbe poi riferito di aver bloccato i bonifici sospetti per 24 ore e che avrebbe rimosso le autorizzazioni dal suddetto dispositivo mobile I*7: il ricorrente deposita in atti alcuni sms ricevuti i quali lo avvisavano dell'avvenuto blocco del servizio di Bonifico istantaneo per 24 ore, nonchè dell'avvenuta rimozione del *suddetto device I*7* e lo invitavano, altresì, a seguire le istruzioni del sedicente interlocutore della banca, identificandolo con il nome ed il cognome con cui lo stesso si era presentato al telefono.

Con riguardo ai messaggi si rileva quanto segue:

- in ricorso parte ricorrente sostiene di avere ricevuto 33 sms totali ma produce soltanto due screen shot;
- parte ricorrente sostiene che i messaggi si sono collocati all'interno di una chat di messaggistica della banca in cui erano presenti anche sms genuini; di tale ultima circostanza, tuttavia, non viene fornita evidenza;
- come anche rilevato dalla convenuta, i messaggi provengono da un mittente solo apparentemente riconducibile alla banca, dal momento che il nome dell'intermediario convenuto è preceduto dalla parola "alert";
- il contenuto dei messaggi si presenta piuttosto scarno; non è presente spaziatura dopo il segno di interpunzione punto; pare di difficile comprensione e anomala la dicitura "Storno blocco numero" seguita da un numero tra parentesi.

Stando sempre a quanto dichiarato in denuncia, il ricorrente ha seguito le istruzioni del truffatore presentatosi come addetto della Banca ed ha personalmente eseguito i bonifici per cui è ricorso, essendo stato indotto a credere che ciò fosse finalizzato a bloccare le operazioni sospette.

Alla luce di quanto sopra dichiarato e documentato, la fattispecie va dunque ricondotta ad un episodio di *social hacking* e non di *spoofing* con esecuzione delle operazioni da parte di terzi frodatori.

Nel caso di *social hacking*, cui è riconducibile anche il caso in esame, le disposizioni eseguite da parte ricorrente non sono riconducibili a quelle delle operazioni non autorizzate ex art. 10 d.lgs.11/2010, dovendo, piuttosto, essere inquadrare nel contesto delle operazioni autorizzate dall'utilizzatore (ex art. 5). Così Coll. Bologna, dec. n. 4691/2025: *"Venendo all'esame del merito, occorre ricordare che, secondo l'orientamento consolidato dei Collegi ABF, quando l'operazione è eseguita per intero dal cliente, con inserimento della disposizione di pagamento e di tutti i fattori di autenticazione, la stessa non è soggetta al regime di responsabilità previsto dalla Direttiva PSD2, e tuttavia può essere applicata la disciplina generale del codice civile, e il risarcimento può essere ottenuto qualora sia dimostrata la negligenza dell'intermediario o comunque un concorso di responsabilità di questi nell'accaduto. Nella pronuncia n. 8671/2024, il Collegio di Coordinamento ha confermato questi principi...."*

Come si è visto poc'anzi e come ribadito dal citato Collegio di Coordinamento resta tuttavia salva la possibilità di individuare, anche in tal casi, una responsabilità concorrente dell'intermediario *secondo le norme di diritto comune*, qualora emerga dalla documentazione in atti un apporto causale dell'intermediario alla frode o comunque emergano profili di negligenza dello stesso in relazione agli obblighi di protezione verso il cliente.

Al riguardo il Collegio rileva che se da un lato l'intermediario produce evidenza di sms alert e notifiche push parlanti inviati al cliente in corrispondenza dei bonifici, nonostante quanto affermato in senso contrario dal ricorrente, dall'altro lato rileva invece che nel caso in esame risulta integrato l'indice di anomalia di cui alla lett. a) n.2 dell'art. 8 (Rischio di frode) del DM 112/2007 (*tre o più richieste di autorizzazione sulla stessa carta, effettuate nelle 24 ore, presso un medesimo punto vendita*).

Il citato DM 112/2007 (*Regolamento di attuazione della l. n. 166/2005, sulla "Istituzione di un sistema di prevenzione delle frodi di pagamento"*), sebbene faccia testuale riferimento alla prevenzione delle frodi solo sulle carte di pagamento, è ritenuto dal Collegio ABF applicabile – quanto agli indici di frode ivi previsti - anche con riguardo ad operazioni eseguite con altri strumenti di pagamento *quali ad esempio i bonifici*, come nel caso in esame o le ricariche online: ciò in ragione dell'unicità della *ratio* sottesa a tale normativa.

Pertanto, applicando la citata lett a) n.2 dell'art. 8 del suddetto DM ai bonifici del caso in esame, detto indicatore di anomalia va letto come segue: *"tre o più richieste di autorizzazione sullo stesso conto di addebito, effettuate nelle 24 ore, a favore del medesimo beneficiario"*.

Nel caso di specie, in base alle tracciatore prodotte dall'intermediario, sono stati disposti, a distanza ravvicinata tra loro:

- n. 30 bonifici istantanei in data 16/01/2025 e
- n. 31 bonifici istantanei in data 17/01/2025.

Per quanto concerne i soggetti beneficiari di tali disposizioni, *i beneficiari totali dei bonifici sono stati 15* : di questi, ben 14 beneficiari hanno ricevuto non meno di *4 bonifici ciascuno, eseguiti o tentati*.

Di conseguenza, l'indice di anomalia di cui alla lett. a) n. 2 del suddetto DM non solo è integrato ma anche reiterato e per numerose volte; a ciò si aggiunga l'elevato numero di bonifici (61), per giunta tutti istantanei, posti in essere in meno di 24 ore per un importo complessivo che ammonta a totali euro 29.700,00: tali circostanze integrano un'operatività macroscopicamente anomala, non coerente con le precedenti abitudini del cliente e comunque tale da richiedere l'attivazione di presidi automatici di blocco o allerta. Ne consegue che l'elevato numero dei bonifici, le modalità di esecuzione, il loro carattere irrevocabile, la reiterazione di indici di frode sono tali da far ravvisare nel caso in esame un concorso di responsabilità dell'intermediario che ha comunque l'obbligo di aggiornare ed elevare il livello di sicurezza dei sistemi di pagamento e del relativo monitoraggio (in tal senso v. Collegio di Milano, decisione n. 1744/2023).

Alla luce delle considerazioni sopra svolte, il Collegio ritiene pertanto giustificato ripartire la responsabilità tra le parti e tenuto conto della condotta gravemente colposa del ricorrente da un lato e dell'inadeguatezza dei presidi antifrode dell'intermediario dall'altro, appare equo riconoscere al cliente un rimborso di euro 9.000,00, somma peraltro offerta dall'intermediario sia in sede di reclamo che in sede di controdeduzioni, somma pari al 30,30% del totale delle operazioni disconosciute per le quali vi è prova, oltre agli interessi dal reclamo al saldo (e non come chiesto dal ricorrente dall'esecuzione dei bonifici).

PER QUESTI MOTIVI

Il Collegio – in parziale accoglimento del ricorso – dichiara l'intermediario tenuto in favore della parte ricorrente alla restituzione dell'importo complessivo di euro 9.000,00 (novemila/00), oltre interessi legali dalla data del reclamo.

Dispone, inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di Euro 200,00 (duecento/00) quale contributo alle spese della procedura e alla parte ricorrente quella di Euro 20,00 (venti/00) quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE