

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) RIZZO	Membro designato dalla Banca d'Italia
(MI) DELL'ANNA MISURALE	Membro designato dalla Banca d'Italia
(MI) FORMAGGIA	Membro di designazione rappresentativa degli intermediari
(MI) GILIBERTI	Membro di designazione rappresentativa dei clienti

Relatore (MI) FORMAGGIA

Seduta del 07/05/2026

FATTO

Il ricorrente, nel ricorso presentato, deduce di essere stato vittima di un episodio di *phishing*; che infatti gli veniva richiesto il pagamento di € 6,50, su una piattaforma *online* denominata A*, per un presunto pedaggio autostradale non pagato; che però gli veniva addebitata la diversa somma di € 776,35, importo del tutto difforme rispetto a quello visualizzato sul portale del *merchant* A*; che l'operazione veniva avviata mediante servizio di terza parte, in un contesto ingannevole, in assenza di una volontà dispositiva consapevole; che veniva informato l'intermediario della natura fraudolenta dell'operazione, ma quest'ultimo non adottava alcuna misura idonea a sospenderne o bloccarne l'esecuzione; che l'intermediario non ha adottato presidi di sicurezza adeguati a rilevare l'anomalia dell'operazione, risultante invece correttamente intercettata come fraudolenta da altri istituti.

Non ha concluso formulando specifiche domande ma, denunciando il comportamento dell'intermediario per non aver disposto presidi di sicurezza, monitoraggio e gestione e misure idonee a bloccare l'esecuzione dell'operazione, nonché la mancata dimostrazione da parte dello stesso della colpa grave del cliente, oltre alla presenza di un'operazione non autorizzata, ha vantato il diritto alla restituzione delle somme indebitamente addebitate.

L'intermediario, nelle controdeduzioni depositate, rileva in via preliminare che il cliente non ha prodotto alcuna allegazione in merito alla presunta truffa; che, nello specifico, non vi è prova della richiesta di pagamento del pedaggio da parte della società autostradale, né del presunto *phishing*, né del sito, né del pagamento richiesto; che il ricorso è altresì inammissibile in quanto il cliente (come

dichiarato nel disconoscimento e nel reclamo) ha ammesso di aver fatto accesso ad un sito non verificato, dove ha consapevolmente autorizzato un pagamento, non verificando che trattavasi di un beneficiario non corrispondente e di un importo differente; che la transazione disconosciuta, anche se per distrazione ed errore, risulta autorizzata dal cliente e, per tale motivo, non rientrando il caso in esame nella fattispecie delle “operazioni non autorizzate”, non sussiste la invocata tutela nei confronti dei titolari; che il cliente è stato vittima di *phishing*; che l'operazione è stata correttamente contabilizzata, registrata e autenticata in quanto posta in essere con il corretto inserimento delle credenziali (nello specifico, con il device certificato e il fattore biometrico); che la contestazione di presunta responsabilità della resistente per non aver bloccato la transazione, oramai autenticata, è infondata e priva di pregio, atteso che, come noto e previsto dalle norme di settore (artt. 5 e 17 D. Lgs. 11/2010), una volta autenticata una transazione di pagamento tramite carta di credito la stessa non può più essere revocata dall'intermediario; che sussiste la colpa grave del cliente in quanto lo stesso dando credito con colpevole credulità ad un presunto messaggio (di cui non fornisce prova) con il quale l'asserita A* gli chiedeva di accedere ad uno sconosciuto sito *internet* per pagare la somma di € 6,50 - ha inserito i dati della carta in tale sito e ha autorizzato il pagamento di CHF 719,99 in favore di sconosciuto *merchant*.

Conclude chiedendo il rigetto del ricorso in quanto la transazione è stata autorizzata dal titolare stesso, nonché per mancanza di allegazioni sulla truffa asseritamente subita; il rigetto del ricorso per infondatezza in fatto e diritto, mancanza di prova, colpa grave del ricorrente; in subordine, ove si ravvisasse una corresponsabilità, che ne venisse definita la ripartizione in misura proporzionale alle effettive responsabilità delle parti, in ogni caso con applicazione della franchigia di legge.

DIRITTO

In fatto si osserva che oggetto del ricorso è una sola operazione, effettuata il 23/11/2025 alle ore 13:02, in Franchi svizzeri, per un importo pacificamente corrispondente ad € 776,35. Trattasi di operazione e-commerce, che, dalle evidenze prodotte dall'intermediario, risulta autorizzata in APP, attraverso i fattori device+biometrico. Il cliente non ha prodotto evidenza della presentazione della denuncia, di cui non viene fatta menzione né nella rappresentazione dei fatti né nella documentazione in atti. Secondo le dichiarazioni rese dal cliente nel modulo di disconoscimento e nel reclamo, questi aveva ricevuto un messaggio da A* per un pedaggio non pagato di € 6,50, con il quale gli veniva chiesto di accedere al sito a* per pagare, ma, una volta entratovi, per pagare appunto l'importo di € 6,50, aveva ricevuto la richiesta di autorizzazione via APP per € 776,35, che nella distrazione del momento aveva approvato. L'intermediario fornisce una versione diversa, eccependo invero, in via preliminare, che l'operazione era stata eseguita personalmente dal cliente e, quindi, debitamente autorizzata.

In diritto si osserva che, alla data dell'operazione contestata, trovava applicazione il D.lgs. 27 gennaio 2010, n. 11 come modificato dal D.Lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU (PSD II), entrato in vigore il 13/01/2018; tale disciplina deve ritenersi integrata con le novità sui bonifici istantanei introdotte dal Regolamento 2024/886, in vigore dal 9-10-2025, con particolare riguardo all'obbligo di prevedere il servizio gratuito di verifica del beneficiario (cd. *Verification of Payee - VoP*).

Secondo l'orientamento dei Collegi, se il concorso causale dell'utente in fase dispositiva e/o autorizzativa è parziale (ad es. con l'inserimento di uno dei fattori di autenticazione), 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 PSP. La prova di autenticazione delle operazioni, a carico dell'intermediario, rappresenta, in aderenza al dato normativo, un *pruis* logico rispetto ad ogni ulteriore accertamento, compreso quello sulla colpa grave del cliente. In sostanza, solo nel caso in cui risulti pacifico o dimostrato che le operazioni contestate siano state compiute direttamente e interamente dal cliente (con inserimento della disposizione di pagamento e di tutti i fattori di autenticazione), l'intermediario è esonerato dalla prova di autenticazione. Diversamente, ove vi siano operazioni non compiute interamente dal cliente, o comunque questi lo contesti, occorre l'accertamento della sussistenza della SCA (*Strong Customer Authentication*), con riferimento alle singole operazioni e ad ogni fase attraverso cui si sono realizzate, sempre con onere della prova a carico dell'intermediario. Infatti - ancora secondo l'orientamento consolidato dei Collegi l'autenticazione forte 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.

La SCA si realizza con il ricorso ad almeno due dei seguenti tre fattori: conoscenza, inerenza, possesso. Tali elementi devono essere reciprocamente indipendenti e appartenere a categorie diverse. In caso di difetto di piena prova sull'autenticazione, per ogni fase, delle transazioni disconosciute, la domanda deve essere accolta, posto che la mancanza anche parziale della prova di autenticazione è risolutiva e dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili al cliente.

Resta ovviamente ferma la possibilità di valutare in concreto se l'utente abbia agito in modo fraudolento o non abbia adempiuto agli obblighi di cui all'art. 7 con dolo o colpa grave, ai sensi dell'art. 12 D. Lgs. 11/2010.

Non essendo poi configurabile una responsabilità oggettiva a carico dell'intermediario, spetta al Collegio verificare se, in concreto, vi sia stata una responsabilità concorrente del PSP secondo le norme di diritto comune, qualora emerga dalla documentazione in atti un apporto causale dell'intermediario alla frode (quali ad esempio, la mancanza o temporanea indisponibilità del numero verde del PSP, o il mancato rilievo di indizi di frode).

L'intermediario fornisce LOG ed altre evidenze e, negli atti, si riporta al loro contenuto, dandone in sostanza una spiegazione.

A questo proposito si rammentano i principi generali espressi dai collegi in merito alla valenza da attribuire alle informazioni presenti nei *log* prodotti dagli intermediari per provare l'autenticazione forte del cliente nelle operazioni di pagamento disconosciute (artt. 10, comma 1 e 10-*bis* del D.lgs. 11/2010), nei casi in cui dalla tracciatura informatica non risulti in modo esplicito uno dei fattori di autenticazione inseriti (conoscenza, possesso o inerenza). Tenuto conto che la PSD2 è

tecnologicamente neutrale e non prevede un sistema informatico standard per l'inserimento e la tracciatura dei fattori di autenticazione forte, i collegi ritengono che, per valutare l'assolvimento dell'onere della prova della SCA, possono essere valutati (oltre ai log) anche ulteriori elementi esplicativi, quali la legenda e/o quanto rappresentato dal PSP (Prestatore dei Servizi di Pagamento) nelle proprie difese in relazione al caso concreto, purché consentano di verificare i singoli passaggi registrati dal sistema informatico come prova di autenticazione.

I collegi ritengono inoltre che eventuali dichiarazioni confessorie del cliente possano assumere valore di prova legale ai sensi dell'art. 2730 c.c..

Sulla base di tali principi consolidati nell'orientamento dei collegi, vanno esaminate le evidenze emergenti dai LOG e dagli argomenti esplicativi forniti dall'intermediario con riguardo alle varie fasi attraverso le quali si sono estrinsecate le operazioni qui contestate.

Con riferimento alla fase di installazione dell'APP, l'intermediario afferma che, nel caso in esame, l'APP di *home banking* è stata installata sul *device* del titolare mediante due fattori: 1) elemento di possesso, dato da cellulare/OTP; 2) elemento di conoscenza, dato da *password + userid*.

Il cliente ha scaricato l'APP sul proprio *device* il giorno 15/10/2025, associato al *DeviceId* *55e7. Ha ricevuto sul *device* associato l'SMS contenente l'OTP da digitare per associare univocamente l'APP al *device*.

Nel caso in esame non vi è stato alcun *enrollment* dell'APP su *device* del truffatore.

Al riguardo, sulla base delle evidenze prodotte dall'intermediario, risulta che in effetti fattori di autenticazione siano stati: la Password di accesso a internet banking; l'OTP-SMS.

L'intermediario ha poi evidenziato anche che l'APP installata sul *device* era già utilizzata per autorizzare accessi e operazioni, e che la medesima APP ed il medesimo *device* erano stati utilizzati per autorizzare ed autenticare la transazione contestata.

Con riferimento, precisamente, all'operazione contestata, sulla base delle evidenze prodotte risulta che essa è stata autenticata tramite: *device id* *55e7 in uso al cliente (*Enrollato Smartphone*); fattore biometrico (*FINGERPRINT_FACEID*).

Deve con ciò ritenersi raggiunta la prova a carico dell'intermediario della sussistenza della SCA.

Ciò posto, il Collegio è tenuto a verificare la condotta delle parti e i profili rilevanti per la valutazione di sussistenza della colpa, ed in proposito si svolgono le seguenti considerazioni.

Innanzitutto, si richiamano le già riportate dichiarazioni rese sul fatto dal ricorrente nel modulo di disconoscimento e nel reclamo; esse non sono accompagnate dalla produzione del messaggio truffaldino. In proposito il cliente dichiara di aver ricevuto il messaggio dalla società A* e non dall'intermediario, ma nulla specifica sul canale tramite il quale ha ricevuto il messaggio truffaldino (se via *email*, SMS o altro), cosa che non rende possibile stabilire se la fattispecie sia riconducibile a *phishing* o a *smishing*.

L'intermediario afferma di avere bloccato la carta e produce evidenza da cui risulta che in effetti il blocco è stato disposto alle ore 13:34 del 23/11/2025:

Il cliente non contesta l'avvenuto superamento del *plafond*, né produce copia del contratto, cosa che rende impossibile stabilire i limiti operativi eventualmente previsti.

Quanto alla presenza di notifiche, è in atti evidenza del servizio di *push alert*, che risulta in stato "Attivo", nonché degli *alert* inviati al cliente tramite notifica Push; da tali evidenze è possibile ricondurre le notifiche al *device* del cliente avente chiave *55e7.

Ma in ogni caso, trattandosi nella specie di un'unica operazione contestata, l'accertamento sulla sussistenza dell'*alert* è superflua: in tali ipotesi, così come anche nel caso di più transazioni avvenute a distanza di pochi minuti l'una dall'altra, e complessivamente in un arco di tempo limitato, la ricezione dell'*alert* non avrebbe potuto, in concreto, limitare il pregiudizio del cliente.

Da quanto emergente in atti, non risulta la sussistenza di indici di anomalia e/o di rischio frode, che avrebbe potuto riscontrarsi in presenza di più operazioni (ex D.M. 112/2007).

Le osservazioni svolte portano a ritenere che nessuna responsabilità possa addebitarsi all'intermediario, a fronte, invece di una grave negligenza del cliente, la cui domanda non può dunque essere accolta, con conseguente rigetto del ricorso.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE