

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

La ricorrente, nel ricorso presentato, afferma che in data 20/12/2025 alle ore 17:49 aveva ricevuto un messaggio whatsapp da un account business con logo ufficiale B* (nota piattaforma di prenotazioni online); che il messaggio le chiedeva di confermare la carta di pagamento inserita in fase di prenotazione sul sito B*; che il messaggio conteneva il suo nome utente e numero di telefono, nonché gli estremi della prenotazione; che cliccando sul *link* contenuto nel messaggio visionava la prenotazione precedentemente effettuata, con i dati della stessa correttamente inseriti; che il sito chiedeva di confermare il metodo di pagamento inserito in fase di prenotazione; che successivamente aveva ricevuto notifica dell'addebito di due transazioni del valore di € 189,00 per un totale di € 378,00; che, contattata la struttura dove aveva effettuato la prenotazione, si avvedeva di essere stata vittima di una truffa; che aveva quindi provveduto a bloccare la carta, a disconoscere le operazioni e a presentare denuncia presso le Autorità.

Chiede, stante la sofisticatezza della truffa il rimborso delle due transazioni di € 189,00 per un totale di € 378,00.

L'intermediario, nelle controdeduzioni, rileva che la denuncia presentata dalla cliente contiene la dichiarazione per cui è stata ella stessa ad effettuare le operazioni cliccando il link contenuto nell'sms; che le operazioni erano state comunque correttamente contabilizzate, registrate e autenticate e non hanno subito le conseguenze di malfunzionamenti; che non risulta agli atti che la ricorrente abbia

tentato di recuperare le somme dalla piattaforma di prenotazioni o dall'hotel presso cui doveva ancora essere effettuato il soggiorno.

Conclude chiedendo il rigetto del ricorso, infondato in fatto e in diritto, respingendo ogni responsabilità dell'intermediario nell'accaduto.

DIRITTO

In fatto si osserva che oggetto del ricorso sono 2 operazioni, consistenti in acquisti *online*, dell'importo di € 189,00 ciascuna, per un totale quindi di € 378,00, compiute il 20/12/2025 rispettivamente alle ore 17:56 e 18:01.

È in atti la denuncia presentata in data 24/12/2025, dove la ricorrente descrive la truffa negli stessi termini del ricorso, specificando di aver personalmente inserito le informazioni di pagamento richieste, quali il numero della carta di debito, la data di scadenza e il CVV, e di aver successivamente avviato il processo di verifica. Precisa, quanto alle modalità della truffa, che aveva ricevuto un messaggio su W* con il quale le veniva chiesto di confermare la carta di pagamento utilizzata per una precedente prenotazione di un alloggio vacanze, attraverso un link contenuto nel messaggio stesso; di avere cliccato sul link contenuto nell'SMS civetta, dove si apriva una schermata con logo ufficiale di un sito che offre servizi di prenotazione; che aveva quindi inserito i dati della sua carta nella convinzione di confermare la carta di pagamento precedentemente usata in fase di prenotazione di un alloggio vacanze; che dopo aver ricevuto gli *alert* relativi all'addebito, si insospettiva in quanto la cifra non corrispondeva all'importo della prenotazione effettuata; che contattando l'intermediario, si avvedeva di essere stata vittima di una truffa.

In diritto si osserva che, pur attribuendo valore confessorio a tali dichiarazioni della ricorrente (rammentandosi a questo proposito che i Collegi ritengono che le dichiarazioni confessorie del cliente possano assumere valore di prova legale ai sensi dell'art. 2730 c.c.), tuttavia quanto dalla stessa disposto con l'operazione concretizzatasi non coincide con l'operazione che essa intendeva fare, sicché si rende comunque necessario l'accertamento della sussistenza della SCA, ossia ad esaminare la prova di autenticazione delle operazioni ai sensi del D.Lgs. 11/2010.

Ed invero, 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. 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.

Le fonti normative regolanti la materia sono rinvenibili negli artt. 97 e 98 della PDS2, nell'articolo 10 bis del D. Lgs. 11/2010, 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 (v. in particolare il parere dell'EBA del 21 giugno 2019).

La prova di autenticazione delle operazioni, a carico dell'intermediario, rappresenta, in aderenza al dato normativo, un *prius* logico rispetto ad ogni ulteriore accertamento, compreso quello sulla colpa grave del cliente.

Secondo il consolidato orientamento dei Collegi, 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), e da questi volute, l'intermediario è esonerato dalla prova di autenticazione. Diversamente, ove vi siano operazioni non compiute interamente dal cliente, 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, 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. Gli elementi devono essere reciprocamente indipendenti e appartenere a categorie diverse. In caso di difetto di piena prova sull'autenticazione, per ogni fase, delle transazioni sconosciute, 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 il fatto che, comunque, non è configurabile una responsabilità oggettiva a carico dell'intermediario, sicché 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 sconosciute (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.

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 estrinsecati le operazioni qui contestate.

Sia con riguardo alla prima che alla seconda operazione, l'intermediario afferma che l'autenticazione è avvenuta tramite codice OTP inviato al numero di cellulare certificato della cliente. Dalle evidenze prodotte risulta che in effetti l'sms OTP è stato inviato in data 20/12 alle ore 17:54:21 al numero corrisponde a quello indicato dalla cliente nel modulo di ricorso.

Produce inoltre evidenza dell'inserimento del codice CVV, del mancato inserimento del codice PIN, che l'operazione è avvenuta in modalità 3DS (senza digitazione del PIN : uso PIN=0).

Sulla base delle suddette evidenze, e dalle stesse argomentazioni della banca nelle controdeduzioni, risulta dunque che l'operazione sia stata autenticata tramite inserimento del codice OTP ricevuto tramite SMS, elemento integrante il fattore del possesso, ed inserimento dei dati della carta tra cui il CVV, e ciò, secondo il consolidato orientamento dei Collegi, non costituisce un elemento di conoscenza ai fini della SCA.

Il Collegio di Milano, in particolare, ha ritenuto (si veda, *ex multis*, pronuncia n. 22660/21), a proposito di un caso analogo di operazioni realizzate tramite la tecnologia 3D Secure che *“Dalla documentazione fornita dall'intermediario emerge che l'operazione di pagamento contestata è stata eseguita via internet con tecnologia 3D Secure, in base a un meccanismo a due fattori, basato sull'inserimento dei dati della carta e del CVV, unitamente al codice dinamico OTP. Si osserva al riguardo che, in base alla regolamentazione vigente, l'inserimento dei dati statici stampati sulla carta, ivi incluso il CVV, non costituisce un elemento riconducibile alla categoria della conoscenza o del possesso, e quindi utile per l'autenticazione forte, come puntualizzato dall'EBA nella “Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2”. Il Collegio, quindi, ritiene che, sebbene la modalità di autenticazione applicata nella fattispecie sia stata, in passato, ritenuta dai Collegi ABF conforme alle prescrizioni normative in materia di SCA, oggi la autenticazione avvenuta sui dati statici della carta, pure incautamente forniti dall'utilizzatore al truffatore, non possa essere più considerata una procedura sicura di autorizzazione dell'operazione, in mancanza di ulteriori elementi di carattere dinamico: questo è peraltro l'orientamento emergente a livello di interpretazione e di applicazione resa dai Collegi territoriali di questo Arbitro, nei tempi più recenti (cfr. tra le altre Collegio di Roma, decisione n. 11271/2020 e Collegio di Bologna, decisione n. 22586/2020). Ne consegue che il Collegio non può che evidenziare come l'intermediario non abbia adottato, quantomeno nell'operazione per cui è causa, gli standard di sicurezza corrispondenti alla disciplina oggi applicabile, funzionali ad evitare il verificarsi di questo particolare tipo di frode.”*

L'intermediario produce altresì i log “tracciati della banca”, che tuttavia non sono di alcuna utilità, perché non ne viene offerta una descrizione né vengono allegati elementi che ne permettano l'analisi, sicché non è possibile individuare con certezza le righe corrispondenti alle operazioni contestate.

Pertanto deve concludersi che, in difetto di piena prova sull'autenticazione delle transazioni disconosciute il ricorso deve essere accolto integralmente, posto che, secondo l'orientamento consolidato dei Collegi, la mancanza anche parziale della prova di autenticazione è risolutiva e

dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili al cliente. La prova di autenticazione rappresenta infatti, come già rilevato, in aderenza al dato normativo, un *prius* logico rispetto alla prova della colpa grave dell'utente. Quanto osservato ha dunque valore assorbente e supera ogni valutazione sulla condotta delle parti.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 378,00.

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 alla parte ricorrente la somma di € 20,00, quale rimborso della somma versata alla presentazione del ricorso. La decisione è stata assunta all'unanimità.

IL PRESIDENTE