COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) MODICA	Membro designato dalla Banca d'Italia
(MI) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(MI) FORMAGGIA	Membro di designazione rappresentativa degli intermediari
(MI) CESARE	Membro di designazione rappresentativa dei clienti

Relatore (MI) FORMAGGIA

Seduta del 09/09/2025

FATTO

La ricorrente afferma che alle ore 16:45 del 15/01/2025 riceveva un SMS da un altro intermediario presso cui detiene un conto corrente; che con l'SMS le veniva comunicato di contattare il numero *985 se non fosse stata lei ad effettuare il pagamento di € 4.900,00; che, preoccupata, contattava il numero indicato; che l'interlocutore, fingendosi un funzionario di banca, la informava di alcuni tentativi di frode che interessavano il suo conto; che la ricorrente riferiva all'interlocutore di essere titolare di un conto anche presso l'intermediario oggi convenuto; che il sedicente operatore la invitava ad effettuare un bonifico dell'importo pari a € 9.980,00 e di fornirgli i codici di accesso all'*home banking* dell'intermediario; di avere quindi a questi fornito le informazioni richieste ed in particolare i codici di autorizzazione che le arrivavano sul suo dispositivo; che il truffatore effettuava così delle operazioni sul conto corrente della ricorrente; che, controllati i movimenti dall'*home banking*, la ricorrente si avvedeva quindi di essere stata vittima di una truffa, sicché contattava prontamente il servizio clienti al fine di bloccare le carte e procedeva a presentare denuncia presso le Autorità in data 16/01/2025 e relative integrazioni rispettivamente in data 18/01/2025, 20/01/2025 e 08/02/2025; che in data 23/01/2025 le veniva negato il rimborso richiesto; che anche in data 15/04/2025 l'intermediario respingeva una seconda richiesta di rimborso inoltrata in data 23/03/2025.
Chiede il rimborso delle operazioni disconosciute.

L'intermediario afferma che la cliente è stata vittima di *vishing*; che le operazioni sono state correttamente contabilizzate, registrate e autenticate in quanto poste in essere con il corretto inserimento delle credenziali; che non sono stati riscontrati malfunzionamenti o intrusioni nei propri sistemi informatici; che sussiste la colpa grave della cliente in quanto ha contattato personalmente il numero di telefono non riferibile all'intermediario, ha fornito i dati di accesso al conto corrente, ha condiviso i codici OTP ricevuti, ha condiviso tutte le informazioni nonostante il messaggio truffaldino fosse riconducibile ad un intermediario diverso e nonostante la banca metta a disposizione della clientela suggerimenti riguardanti le truffe.
Chiede il rigetto del ricorso.

La cliente replica che l'intermediario nulla aveva addotto sulla possibilità di revoca del bonifico ed il suo silenzio induceva a supporre che non ne consentisse la revoca.

L'intermediario controreplica che quando la cliente ha contattato il servizio clienti il bonifico era già stato eseguito ed era quindi divenuto irrevocabile; che la banca aveva attivato la procedura di richiamo dell'operazione ma non aveva ricevuto alcuna risposta dalla controparte. Insiste nel rigetto del ricorso.

DIRITTO

Si dà atto che le operazioni contestate sono 2, e precisamente un bonifico ordinario di € 10.000,00 eseguito il 15/01/2025 alle ore 19:32 (orario UTC 18:32) e un pagamento *online* di € 2.858,00 eseguito sempre il 15/01/2025 alle ore 19:56 (orario UTC 18:56). L'importo complessivo di cui è chiesto il rimborso è dunque pari ad € 12.858,00.
Si osserva, per inciso, che nell'ambito della medesima frode è stato eseguito un ulteriore pagamento (di € 9.980,00) da altro conto corrente detenuto dalla cliente presso un altro intermediario; questa diversa operazione è stata oggetto di separato ricorso, rigettato dal Collegio di Milano in quanto si trattava di operazione eseguita dalla cliente personalmente (decisione n. 7156/25 del 22/07/2025).
Per la tipologia delle operazioni oggetto del presente procedimento è necessaria la sussistenza della *strong customer authentication* (SCA), le cui fonti normative 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 (in particolare, il parere dell'EBA del 21 giugno 2019).
Nello specifico, l'autenticazione forte (SCA) 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 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. La prova di autenticazione rappresenta infatti, in

aderenza al dato normativo, un *prius* logico rispetto alla prova della colpa grave dell'utente.
Esaminando atti e documenti riguardanti il caso oggetto del presente procedimento, va sottolineato che dalle dichiarazioni rese dalla cliente nella denuncia risulta che la stessa ha fornito al sedicente operatore le credenziali di accesso all'*home banking* e anche i codici autorizzativi delle operazioni che le arrivavano di volta in volta sul suo cellulare.
Secondo l'orientamento consolidato 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.
Tale essendo il contesto normativo, si deve procedere, nel caso in oggetto, ad esaminare la prova di autenticazione delle operazioni ai sensi del D.Lgs. 11/2010. La prova deve riguardare ogni fase delle operazioni, quindi anche quelle prodromiche.
Si premette che, con riferimento alle azioni antecedenti all'esecuzione delle operazioni contestate, l'intermediario spiega il metodo di accesso all'area riservata tramite sito *web* o App e precisa che è necessario inserire le credenziali statiche *username* e *password* (fattore di conoscenza) scelte dal cliente ovvero, per quanto riguarda l'accesso tramite app, esso può essere eseguito tramite i dati biometrici (impronta digitale e/o riconoscimento facciale) del dispositivo impiegato per accedere (fattore di inerenza). Oltre all'inserimento delle credenziali statiche, è richiesta l'autenticazione forte mediante OTP trasmessa via SMS al numero di cellulare indicato dal cliente in sede di apertura del rapporto, validato dalla banca e univocamente associato al conto, la prima volta che i clienti accedano all'area riservata ovvero qualora siano trascorsi più di 180 giorni dall'ultimo accesso avvenuto con autenticazione forte. L'intermediario specifica anche che, in assenza di autenticazione forte, l'accesso è limitato alla visualizzazione del saldo del conto e delle operazioni contabilizzate negli ultimi 90 giorni, mentre l'esecuzione di qualsiasi azione è subordinata all'inserimento di un secondo fattore di autenticazione.
Nel caso in esame, con riferimento alla fase di *login* all'area riservata, l'intermediario si avvale dell'esenzione dalla SCA *ex* art. 10 Regolamento delegato UE 2018/389, che autorizza i PSP a non applicare la SCA qualora non siano trascorsi più di 180 giorni dall'ultima volta che il cliente ha effettuato un accesso con doppio fattore. In tal caso, però, l'accesso è limitato alle informazioni previste dal suddetto art.10.
L'intermediario produce evidenze dimostrative che sono stati effettuati dei primi accessi con l'inserimento di *username* e *password*; che alle ore 19:29 è stato registrato un accesso da *web* con autenticazione forte caratterizzata da inserimento di *username* e *password* (fattore di conoscenza) e inserimento del codice OTP ricevuto tramite SMS (fattore di possesso) inviato al numero di cellulare della cliente univocamente associato al conto; precisa che le OTP depositate con all. 6 presentano orari differenti da quelli indicati negli Allegati 3, 4 e 5 poiché la registrazione è eseguita con orario UTC (-1 ora rispetto ai log informatici); che il codice OTP è stato inviato al numero di telefono corrispondente a quello indicato dalla cliente in denuncia.
Da tali evidenze emerge che, per quanto riguarda l'accesso all'area riservata effettuato alle ore 19:29, la SCA è stata provata.
Per quanto riguarda la fase di modifica dei massimali della carta di debito, l'intermediario produce evidenze dimostrative che la richiesta di aumento è stata autorizzata tramite SCA alle ore 19:34; che gli elementi autorizzativi sono consistiti nell'inserimento di *username* e

password (fattore di conoscenza) e nella digitazione del codice OTP ricevuto tramite SMS sul numero di cellulare della cliente (fattore di possesso); che l'SMS contenente il codice OTP chiariva l'operazione di aumento del limite di acquisto giornaliero che si stava per realizzare; che il numero di telefono, cui è stato inviato l'SMS contenente il codice OTP, corrisponde a quello indicato dalla cliente nella denuncia; che l'orario dell'SMS contenente il codice OTP è riportato utilizzando il fuso orario UTC.
Da tali evidenze emerge che, anche per quanto riguarda l'aumento dei massimali della carta di debito, la SCA è stata provata.
Per quanto riguarda la fase di accesso all'area riservata prodromico alla generazione del CVV dinamico, l'intermediario richiama le evidenze prodotte, dimostrative che è stato eseguito un accesso all'area riservata tramite *web* alle ore 19:54; che l'accesso è stato eseguito tramite inserimento di *username* e *password* (fattore di conoscenza) e inserimento del codice OTP (fattore di possesso); che il codice OTP è stato inviato al numero di telefono corrispondente a quello indicato dalla cliente in denuncia; che l'orario dell'SMS contenente il codice OTP è riportato utilizzando il fuso orario UTC.
Da tali evidenze emerge che, anche per quanto riguarda questa fase, la SCA è stata provata.
Analogamente, la fase di generazione del CVV dinamico risulta, sulla base delle evidenze prodotte, essere stata autorizzata mediante inserimento di *username* e password (fattore di conoscenza) e digitazione del codice OTP ricevuto tramite SMS sul numero di cellulare della cliente (fattore di possesso), elementi che consentono di ritenere provata la SCA.
Per quanto riguarda, poi, la prima operazione, consistente nel bonifico ordinario di € 10.000,00 eseguito alle ore 19:32 (orario UTC 18:32), l'intermediario, primariamente, spiega le modalità di disposizione di un bonifico, consistenti nell'inserimento dell'ordine di bonifico all'interno dell'area riservata dopo avervi fatto accesso con le modalità indicate; nella compilazione dei campi IBAN riguardanti il beneficiario, l'importo, la tipologia di bonifico e la causale; nella conferma dell'ordine di bonifico mediante inserimento della OTP ricevuta sul numero di cellulare univocamente associato al conto del cliente. Richiama, quindi, le evidenze dalle quali emerge che l'operazione è stata autenticata tramite inserimento di *username* e *password* (fattore di conoscenza) e inserimento del codice OTP inviato al numero corrispondente univocamente a quello indicato dalla cliente in denuncia (fattore di possesso). Dalle richiamate evidenze risulta provata la SCA.
Per quanto riguarda la seconda operazione, consistente nel pagamento *online* di € 2.858,00 eseguito alle ore 19:56 (orario UTC 18:56), l'intermediario premette una spiegazione dei passaggi necessari per effettuare un pagamento online con carta di debito: il cliente deve inserire nel POS virtuale il PAN della carta di 16 cifre, la data di scadenza della carta, il CVV dinamico, cioè un codice di 3 cifre che varia la propria numerazione dopo pochi minuti dalla visualizzazione e deve essere generato nell'area riservata; l'operazione viene successivamente confermata tramite inserimento di un codice OTP ricevuto tramite SMS sul numero di cellulare univocamente associato al conto della cliente.
Secondo l'intermediario, ai fini dell'autenticazione forte sono sufficienti l'inserimento del codice OTP ricevuto tramite SMS sul numero di cellulare della cliente, quale fattore di possesso, e l'inserimento del CVV dinamico, quale fattore di conoscenza o inerenza (a seconda delle modalità di accesso all'area riservata).
Con riferimento al caso di specie, l'intermediario precisa che il pagamento veniva eseguito *online* e senza utilizzazione della carta fisica alle ore 19:56, mediante inserimento delle credenziali statiche della carta (PAN e data di scadenza), del CVV dinamico generato, dell'OTP ricevuto tramite SMS sul numero di cellulare univocamente associato al conto

corrente della cliente indicato nella denuncia; elementi che dunque, secondo la sua tesi, confermano la sussistenza dell'autenticazione forte.
Ma, secondo l'orientamento assunto dal Collegio di Milano (*ex multis,* decisioni n. 7207/2024, n. 8153/2004), la valenza da attribuire al CVV dinamico (*password* + OTP) ai fini della prova della SCA non è quella di fattore di conoscenza come pretenderebbe l'intermediario, ma piuttosto di fattore di possesso, con la conseguenza che un doppio fattore di possesso non risulterebbe conforme alla SCA, alla luce delle indicazioni fornite dall'EBA nell'*Opinion* del 21 giugno 2019, presupponendo il sistema di autenticazione forte il ricorso a due fattori di autenticazione appartenenti a categorie diverse. Di conseguenza la prova della SCA, che rappresenta -in aderenza al dato normativo- un *prius* logico rispetto alla prova della colpa grave dell'utente, non può ritenersi raggiunta.
Pertanto, in conclusione, l'importo riguardante l'operazione di pagamento online pari ad € 2.858,00 va rimborsato alla ricorrente, stante la mancanza di prova della SCA, mentre l'importo di € 10.000,00 riguardante l'operazione di bonifico, avvenuta in presenza della SCA per ogni fase, non le va rimborsato.
La domanda della ricorrente va dunque accolta solo parzialmente, nei limiti dell'importo di € 2.858,00, che l'intermediario è tenuto a corrisponderle.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 2.858,00.
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.

IL PRESIDENTE

Firmato digitalmente da
ANDREA TINA