COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) TINA	Membro designato dalla Banca d'Italia
(MI) RIZZO	Membro designato dalla Banca d'Italia
(MI) DALMARTELLO	Membro di designazione rappresentativa degli intermediari
(MI) AFFERNI	Membro di designazione rappresentativa dei clienti

Relatore (MI) ANDREA TINA

Seduta del 17/09/2024

FATTO

Nel proprio ricorso la ricorrente ha riferito quanto segue:

- in data 24/10/2023 alle ore 12.48 riceveva un sms nella chat con l'intermediario, contenente altri messaggi genuini;
- l'sms conteneva la comunicazione: "*accesso non autorizzato alla sua area personale. Se non riconosce questo accesso richieda assistenza su http//:is***";*
- cliccava sul link e alle 12.59 veniva contatta telefonicamente da un numero privato: l'interlocutore si qualificava come 'addetto dell'ufficio prevenzione frodi dell'intermediario convenuto';
- quest'ultimo la informava di alcuni pagamenti fraudolenti e la invitava ad aprire l'home banking, senza chiedere alcun dato sensibile;
- accedeva quindi all'applicazione della banca e digitava i codici di accesso e il pin sul proprio dispositivo. Il presunto operatore la invitava a ripetere l'operazione, in quanto i codici di accesso risultavano errati;
- provvedeva a ripetere l'operazione una seconda volta, digitando i codici e il pin sul proprio telefono senza comunicare i codici o altri codici di sicurezza. A quel punto, veniva rassicurata sulla correttezza delle operazioni appena compiute e sulla conseguente cancellazione di tutti i pagamenti fraudolenti effettuati;
- alle ore 14.00 dello stesso giorno, si recava in filiale e si avvedeva di essere stata vittima di una truffa poiché l'operatore allo sportello la informava di svariati pagamenti istantanei CBILL dal c/c **717 in favore della Agenzia delle Entrate e

dell'ACI per un totale di € 5.924,66 [importi comprensivi delle spese di commissione];
- verificava che per nessuna di quelle operazioni avesse ricevuto notifiche o richieste di autorizzazione, a differenza di quanto accaduto per tutte le operazioni eseguite in precedenza tramite app della banca;
- procedeva a chiedere immediatamente il disconoscimento delle operazioni e al blocco della carta di credito n. ***600 collegata al conto, ma le veniva in quel momento negato;
- alle ore 16.00 dello stesso giorno riceveva una mail dall'operatore dell'intermediario con il quale si era interfacciata poco prima che la informava della modifica del plafond della carta di credito n. ***600 che da € 3.000,00 aumentava a € 4.500,00 e che erano state eseguite alcune transazioni di cui allegava gli estremi;
- dai movimenti allegati alla comunicazione dell'intermediario, si accorgeva che erano stati compiuti indebitamente con la propria carta n. ***600, n. 4 pagamenti indebiti per un totale di € 977,70, per cui, come per le operazioni precedenti, non riceveva alcuna richiesta di autorizzazione; anche per la modifica dei massimali non riceveva alcuna notifica o richiesta di conferma;
- in data 25/10/2023 si recava a presentare denuncia presso le Autorità, che veniva integrata in data 31/10/23 e 02/11/2023;
- in data 31/10/2023 il cointestatario del conto n. ***717 avviava la procedura online per il disconoscimento delle n. 26 operazioni di pagamenti non autorizzate;
- in data 06/02/2023 l'intermediario riscontrava negativamente la richiesta di disconoscimento delle operazioni.

La ricorrente ha, quindi, chiesto il rimborso dell'importo di € 6.902,36, corrispondente alle operazioni disconosciute.

Con le proprie controdeduzioni, l'intermediario resistente ha precisato quanto segue:
- la cliente e i sig. A. W. Sono cointestatari del conto corrente n. ***717, al quale è collegata la carta di credito n. ***600 intestata alla cliente. Il conto e la carta sono abilitati al servizio di *internet banking.* Tramite detto servizio sono state disposte in data 24/10/2023, con addebito sul citato conto corrente, le seguenti operazioni:
    - n. 26 pagamenti CBILL in favore di Agenzia delle Entrate e ACI per complessivi € 5.924,66 [comprensivi delle spese di commissione] =;
    - n. 4 operazioni di pagamento presso gli esercenti M*** e C*** per complessivi € 977,70= effettuate con la suddetta carta di credito.;
- in data 25/10/2023 la cliente ha denunciato l'accaduto, integrando successivamente la denuncia in data 31/10/2023 e 02/112023, e in data 31/10/2023 e 9/11/2023 i clienti hanno disconosciuto le suddette operazioni, sottoscrivendo i previsti moduli.
- in data 14/11/2023 e 06/02/2024 ha comunicato ai clienti di non poter accogliere le loro richieste di rimborso in quanto totalmente estranea all'accaduto e – per quanto riguarda le operazioni eseguite con carta di credito – di non essere riuscita a recuperare le somme sui circuiti di credito poiché le operazioni erano state eseguite in modalità di commercio elettronico sicuro con l'utilizzo dei codici associati alla carta affidati alla custodia della cliente;
- riguardo al servizio di internet banking, è richiesto l'inserimento simultaneo di password statiche e dinamiche, cioè il codice Titolare (password statica) il codice PIN (password statica) e il codice O-Key (OTP cioè la password dinamica). Una volta collegati al servizio online, per autorizzare le operazioni dispositive è necessario il codice dinamico, OTP;

- ha ottenuto la certificazione ISO/IEC 27001 che rappresenta la garanzia che il sistema di gestione adottato è in grado di offrire massimi livelli di sicurezza nell'utilizzo dei servizi della banca online e dei sistemi di pagamento elettronici;
- nello specifico risulta un'attività di enrollment di un nuovo dispositivo - probabilmente in uso ai truffatori - da cui sono stati disposti i pagamenti contestati;
- la condotta della ricorrente è stata connotata da colpa grave ove, dinanzi ad una truffa per nulla sofisticata e riconducibile ad un'ipotesi classica di spoofing, per sua stessa ammissione ha cliccato sul link decettivo e ha successivamente ceduto involontariamente le credenziali ai terzi truffatori, senza le quali la registrazione del nuovo device non sarebbe stata possibile;
- nel caso in esame, le operazioni disconosciute dai clienti sono state eseguite dopo essere state "autenticate, correttamente registrate e contabilizzate" e non hanno "subito le conseguenze del malfunzionamento delle procedure necessarie per la loro esecuzione o di altri inconvenienti.;
- al fine di dimostrare la corretta autenticazione delle operazioni e l'assenza di anomalie si produce l'estratto delle registrazioni elettroniche effettuate in occasione dell'operatività disconosciuta dai clienti;
- i 26 pagamenti sono stati confermati con l'autenticazione della titolare tramite OTP, previo inserimento del PIN. Il codice OTP, generato da APP installata sul device previo inserimento del PIN, porta all'esecuzione dell'operazione di pagamento;
- i 4 pagamenti eseguiti in modalità e-commerce sono stati autorizzati per la carta ***600; le operazioni sono state confermate con autenticazione del titolare tramite OTP, senza nessuna anomalia;
- le operazioni sono state, quindi, impartite con il corretto inserimento di tutte le credenziali possedute dalla cliente e la banca ha dovuto darne esecuzione in adempimento degli obblighi assunti contrattualmente nei confronti della stessa;
- la procedura di autenticazione adottata nel caso di specie è conforme ai requisiti della Strong Customer Authentication;
- ha allertato la cliente, inviando alla stessa un messaggio SMS e PUSH con il quale veniva informata dell'attività di *enrollment* da altro dispositivo, oltre che, mentre l'attività truffaldina era ancora in corso, della variazione dei limiti operativi della carta di credito;
- ha fornito nel tempo alla propria clientela numerose comunicazioni relative alle insidie delle truffe a distanza e circa le precauzioni da adottare per evitare il loro compimento;
- dinanzi a truffe del tipo riconducibile a quella in cui è incorsa la cliente, il consolidato orientamento dell'Arbitro è nel senso del rigetto della richiesta restitutoria, in ragione del grado di diffusione e notorietà di tale schema di frode informatica, facilmente eludibile adottando un comune standard di diligenza.
- deve quindi escludersi ogni responsabilità della resistente per l'accaduto, dovendosi ricondurre la perdita patrimoniale subita unicamente alla sfera di responsabilità della cliente, per non aver custodito diligentemente le credenziali di sicurezza.

DIRITTO

La questione rimessa all'esame del Collegio attiene all'esecuzione di n. 30 operazioni di pagamento on line effettuate con il servizio homebanking della ricorrente, per l'importo complessivo di € 6.902,36, in data 24 ottobre 2023. La ricorrente riferisce, in sintesi, di essersi accorta delle operazioni di pagamento dopo aver ricevuto un sms che la informava

di un accesso non autorizzato alla sua area personale. Le operazioni disconosciute sono assoggettate alle disposizioni del D.lgs. n. 11/2010 nella versione oggi vigente.
Al riguardo, giova precisare che, per l'ipotesi di disconoscimento di operazioni da parte della cliente, l'art. 10 del D.lgs. n. 11/2010 prevede un particolare regime di ripartizione dell'onere probatorio, che, come noto, si articola in una precisa e graduata sequenza così riassumibile: in prima battuta (comma 1), il prestatore di servizi di pagamento deve provare che l'operazione 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; quindi, assolto con successo questo primo onere, necessario ma di per sé ancora insufficiente a dimostrare che l'operazione sia stata effettivamente autorizzata dal titolare, il prestatore deve ulteriormente dimostrare, ai fini dell'esonero dalla responsabilità (comma 2) che l'uso indebito del dispositivo è da ricondursi al comportamento fraudolento, doloso o gravemente colposo dell'utilizzatore rispetto agli obblighi di condotta imposti a quest'ultimo dall'art. 7 dell'anzidetto decreto.
Ciò premesso, per quanto attiene al primo profilo sopra individuato, l'intermediario resistente, ha fornito piena prova in ordine corretta autenticazione delle operazioni disconosciute secondo i criteri SCA. Viene dunque in rilievo la valutazione della condotta della ricorrente. Al riguardo, la ricorrente non ha fornito elementi in ordine ai fatti e alle circostanze nell'ambito delle quali sono state eseguite le operazioni disconosciute; circostanza che, secondo l'orientamento dei Collegi territoriali, consente di presumere, a fronte della corretta autenticazione secondo SCA delle operazioni di pagamento, una condotta gravemente colposa del titolare dello strumento di pagamento.
Ciò nonostante, le richieste della ricorrente devono trovare parziale accoglimento.
Occorre, infatti, osservare che nel caso di specie si tratta di n. 30 operazioni di pagamento (4 acquisti on line e 26 C-BILL) effettuate in un arco temporale ristretto di meno di un'ora, dalle 13.07 alle 14.02 del 24 ottobre 2023, dovendosi, pertanto, ritenere integrato l'indice di rischio di cui all'art. 8, lett. b, n. 1, del D.M. 112/2007 (setto o più richieste di autorizzazione sulla stessa carta, effettuate nelle 24 ore). Di conseguenza, sebbene non sia possibile una piena valutazione della condotta tenuta dalla ricorrente, a fronte del carattere evidentemente anomalo delle operazioni disconosciute, l'intermediario resistente avrebbe dovuto approntare sistemi automatici di monitoraggio e di blocco delle operazioni, dalla settima operazione (inclusa) in poi. Ne consegue, pertanto, il diritto della ricorrente al rimborso dell'importo corrispondente alle operazioni successive alla sesta operazione disconosciuta, comprensive di commissioni, pari a € 5.529,00.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 5.529,00.
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
FLAVIO LAPERTOSA