COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) TENELLA SILLANI	Membro designato dalla Banca d'Italia
(MI) CETRA	Membro designato dalla Banca d'Italia
(MI) FERRARI	Membro di designazione rappresentativa degli intermediari
(MI) AFFERNI	Membro di designazione rappresentativa dei clienti

Relatore (MI) FERRARI

FATTO

La parte ricorrente rappresenta quanto segue:

- premette di essere correntista dei due intermediari convenuti;
- nella notte tra il 27 e il 28 maggio 2020, veniva ricoverato in ospedale. Il 28 maggio, intorno alle 19:00, apprendeva tramite il servizio di messaggistica degli intermediari, che ignoti avevano posto in essere delle operazioni fraudolente sui propri conti correnti;
- a quel punto, per il tramite del suo difensore, il cliente procedeva a presentare denuncia e a disconoscere le operazioni, bloccando le proprie utenze e le proprie carte. Inoltre, conferiva un incarico a un'esperta per eseguire una perizia informatica, al fine di far luce sull'accaduto;
- per quanto riguarda specificamente i rapporti in essere presso l'intermediario A, il cliente riferisce di essersi accorto della truffa in corso, allorquando riceveva degli sms con dei codici OTP dall'intermediario, mentre solitamente il cliente si avvale, per disporre operazioni dispositive, di un'apposita applicazione, tramite la quale viene generato l'OTP, dopo aver inserito codice utente e password. Allarmato dalla situazione, il cliente accedeva all'App, senza riscontrare anomalie;
- intorno alle 18:30, mentre il cliente entrava nel reparto di cardiologia, riceveva diversi sms alert anche dall'intermediario B, di cui si avvedeva solo alle 18:40, una volta entrato nella propria stanza. Tuttavia, accedendo all'applicazione, tutto

sembrava regolare, in quanto le operazioni fraudolente non erano ancora state contabilizzate e non erano visibili;
- la perizia eseguita per conto del cliente consente di capire che il cliente è stato vittima di un attacco informatico, in quanto diverso è il sistema operativo, diverso l'indirizzo IP, così come la geolocalizzazione. Pertanto, risulta difficile capire come gli intermediari non si siano attivati per bloccare le operazioni in questione;
- dal canto suo, il cliente si attivava immediatamente bloccando la propria utenza e contattando i familiari per concordare il da farsi;
- il 29.5.2020, l'avvocato del cliente si recava presso la filiale dell'intermediario A per disconoscere le operazioni, apprendendo che erano stati modificati al ribasso – da parte di operatori della filiale – i limiti di operatività tramite home banking, senza alcuna giustificazione;
- anche per quanto concerne l'intermediario B, il cliente provvedeva tempestivamente al blocco e al disconoscimento. Le operazioni fraudolente riguardavano diversi pagamenti tramite carta di credito e, una volta raggiunto il massimale, un giroconto di Euro 2.461,00;
- nonostante l'intermediario non abbia fornito i log delle operazioni, tuttavia dalla perizia prodotta dalla cliente è emerso che dal 19.5.2020 alle ore 10:47 ha avuto inizio un'attività anomala sul dispositivo del cliente, con un totale di 19.016 eventi di *log* sull'uso delle applicazioni. Ciò induce a ritenere che il *device* sia stato violato e sottratto al controllo del cliente;
- in sede di riscontro al disconoscimento, l'intermediario A si è limitato a replicare che tutto si sarebbe svolto in maniera corretta, senza fornire prova dell'autenticazione delle operazioni, né rispondere nei tempi previsti dal contratto;
- peraltro, nell'art. 7 del contratto di internet banking, è specificato che l'intermediario si riserva la facoltà di inibire l'uso del servizio in caso di uso anomalo o non conforme, anche senza preavviso. Nonostante le evidenti anomalie che connotano il caso di specie, l'intermediario A non ha ritenuto di porre in essere alcuna azione cautelativa;
- allo stesso modo, nemmeno l'intermediario B ha assolto alcuno dei suoi obblighi derivanti dalla normativa e dal contratto. In particolare, l'intermediario non ha bloccato le carte di pagamento nonostante i sospetti di frode e nonostante fosse stato lo stesso intermediario ad ammettere le anomalie riscontrate.

Il cliente chiede pertanto: nei confronti dell'intermediario A, il rimborso di € 26.990,00, oltre al rimborso delle spese per la consulenza pari a € 3.660,00, oltre spese legali, rivalutazione e interessi fino al soddisfo; nei confronti dell'intermediario B, il rimborso di € 7.271,00 oltre al rimborso delle spese per la consulenza pari a € 3.660,00, oltre spese legali, rivalutazione e interessi fino al soddisfo.

L'intermediario A eccepisce che:
- non è stata riscontrata alcuna anomalia nei sistemi della banca, né tantomeno manomissioni;

- non c'è dubbio, come risultante dalla perizia tecnica prodotta dal cliente, che i bonifici disconosciuti siano stati autorizzati da un altro dispositivo, ma per permettere l'attivazione di questa seconda App sono necessari tre diversi codici OTP (OTP standard, sms e *dynamic linking*);
- dalle evidenze informatiche risulta che il dispositivo dell'utente abbia ricevuto il codice sms e aperto la sua App; si deve quindi comprendere come i codici siano usciti dal dispositivo dell'utente. L'ipotesi di un *malware*, sostenuta dal perito incaricato dal cliente, non convince;
- infatti, l'App dell'intermediario integra il sistema di *root detection* e, in caso di dispositivo compromesso, impedisce l'apertura dell'applicazione (e quindi la generazione dell'OTP). Inoltre, dai *log* dell'applicazione si evince che prima di ogni azione effettuata dal frodatore, tra cui quella di attivazione del token, è presente l'apertura dell'App sul dispositivo dell'utente. Infine, l'intermediario riporta il testo dei messaggi recanti i codici OTP, con l'indicazione dell'orario e del fatto che questi siano stati effettivamente inviati al numero del cliente;
- risulta quindi che la cessione dei codici di accesso per l'apertura da altro dispositivo, dal quale sono state effettuate le operazioni, provenga direttamente dall'utenza del cliente. Non spetta all'intermediario dimostrare perché ciò sia accaduto, ma è evidente che trattasi di condotta che non può che essere ascritta alla responsabilità del cliente. Non può venire in discussione quindi la fase di esecuzione delle operazioni contestate, quanto quella prodromica di cessione dei codici di accesso;
- l'intermediario allega altresì il documento che dettaglia il processo di gestione e monitoraggio degli incidenti connessi ad operazioni fraudolente, dal quale si evince come l'intermediario abbia ormai da tempo adottato un sistema informatico che consente di prevenire in modo efficace tali episodi.

Chiede pertanto il rigetto del ricorso.

L'intermediario B eccepisce che:

- entrambe le carte di pagamento del cliente erano state dal medesimo registrate al portale titolari del sistema 3D *secure code*, tramite abbinamento alle carte del proprio numero telefonico certificato;
- le transazioni online effettuate con la carta di credito e con la carta prepagata sono andate a buon fine proprio a seguito del corretto inserimento dei seguenti codici identificativi e, in particolare: a) le credenziali statiche (numero di sedici cifre della carta, data di scadenza, nome del cliente e CVV2, che è presente sulle carte stesse e quindi noto esclusivamente ai clienti) e le credenziali dinamiche (OTP inviato via sms);
- come prova del corretto inserimento di ciascuna password, l'intermediario produce i *log* dai quali si può evincere la dicitura Ucaf 2, che attesta l'avvenuto inserimento del codice OTP di conferma e la transazione approvata. Pertanto, chi ha disposto le transazioni era a conoscenza di tutte le credenziali statiche delle carte;

- pertanto, appare inverosimile che il solo accesso al dispositivo mobile possa essere sufficiente per un soggetto terzo per portare a termine le transazioni senza i dati completi degli strumenti di pagamento;
- il cliente ha colpevolmente omesso di fornire indicazioni precise su dove e come fosse custodito il telefono negli orari in cui si sono perfezionate le operazioni contestate, per cui non è chiaro se abbia consentito a qualcuno di usare il suo dispositivo mobile o abbia in qualche modo messo a conoscenza di altri i propri codici;
- l'intermediario ha inviato al recapito del cliente sia i codici OTP che gli alert a notifica degli avvenuti pagamenti e, rilevata una movimentazione anomala con le carte, oltre ad aver bloccato numerose tra le transazioni in corso, ha notificato al cliente una richiesta di ricontatto dopo aver tentato, senza riuscirci, di contattarlo direttamente.
- appare poi inverosimile che lo *spyware* cui si fa riferimento nella perizia del cliente, risalente al 2016, sia rimasto silente sino a maggio 2020. Pertanto, la supposta clonazione del telefono pare non supportata da alcun elemento oggettivo;
- quanto al giroconto contestato, è stato effettuato tramite l'App, che consente di autorizzare le operazioni direttamente dal proprio *smartphone*, previo inserimento di un codice pin personale a cinque cifre noto solo al cliente. Tale processo di attivazione dell'App sul telefono avviene mediante le credenziali di accesso all'home banking e codice pin scelto dal cliente. Tale processo è funzionale ad associare in modo univoco il *token software* a un certo device (possesso). Una volta associato il token, per effettuare operazioni il cliente deve inserire un codice statico, tramite il quale viene creato il codice dinamico OTP, che consente di processare la disposizione;
- dalle evidenze prodotte dall'intermediario, risulta che il malfattore abbia effettuato l'accesso nell'area riservata dell'home banking previo inserimento dei codici, abbia poi eseguito il reset della SCA e poi regolarmente disposto il giroconto;
- si ritiene quindi che in qualunque modo i frodatori abbiano reperito i codici di accesso del titolare, tale evenienza non riguarda problematiche legate alla responsabilità dell'intermediario.

Chiede pertanto il rigetto del ricorso.

DIRITTO

Nel caso dell'intermediario A (primo intermediario), il Collegio rileva che le operazioni sono state autenticate tramite un sistema di tipo forte. Tuttavia, la concatenazione delle circostanze è tale da consentire al Collegio di affermare che l'intermediario non abbia predisposto tutti i presidi di sicurezza necessari per evitare la sottrazione in modo fraudolento di somme al ricorrente. D'altro canto, si può al contempo affermare che il ricorrente non abbia tenuto un comportamento improntato alla massima prudenza, nella custodia del proprio telefono. L'insieme delle circostanze così esposte e considerate

consente di affermare in capo ad entrambe le parti una responsabilità per i fatti oggetto di controversia. Al ricorrente dovrà quindi essere riconosciuto un accoglimento parziale della sua pretesa in misura pari al 50% delle somme sottratte in modo fraudolento. Questo Collegio non reputa invece ammissibile la richiesta di rimborso delle spese di perizia in quanto ridondante e priva di utilità per i risultati qui ottenuti.

Nel caso delll'intermediario B (secondo intermediario), il Collegio rileva che le operazioni sono state autenticate tramite inserimento delle credenziali statiche della carta e inserimento del codice dinamico OTP. A tal proposito, si rileva che l'EBA nella propria *Opinion* del 21 giugno 2019 sulla SCA ai sensi della PSD2, ha evidenziato che l'autenticazione a mezzo di dati statici della carta e OTP, quanto meno a far data dal 14 settembre 2019, deve ritenersi non più in linea con gli standard richiesti dalla normativa comunitaria. Invero, ai sensi del Regolamento delegato (UE) n. 2018/389, secondo il parere espresso dall'EBA, mentre l'OTP ricevuto tramite sms integrerebbe un elemento di possesso, i dati riportati sulla carta (numero carta di credito, scadenza dello strumento e CVV), non costituirebbero né un elemento di possesso, né un elemento di conoscenza. Limitatamente a tale intermediario, questo Collegio reputa pertanto ammissibile la richiesta di rimborso. Non reputa invece ammissibile la richiesta di rimborso delle spese di perizia in quanto ridondante e priva di utilità per i risultati qui ottenuti.

PER QUESTI MOTIVI

Il Collegio, in parziale accoglimento del ricorso, dispone che il primo intermediario corrisponda alla parte ricorrente la somma di € 13.500,00, oltre interessi legali dal reclamo al saldo, e che il secondo intermediario corrisponda alla parte ricorrente la somma di € 7.271,00, oltre interessi legali dal reclamo al saldo.
Il Collegio dispone inoltre, ai sensi della vigente normativa, che gli intermediari in solido corrispondano 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