COLLEGIO DI BARI

composto dai signori:

(BA) TUCCI	Presidente
(BA) PORTA	Membro designato dalla Banca d'Italia
(BA) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(BA) COSTANTINO	Membro di designazione rappresentativa degli intermediari
(BA) PANZARINO	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - FABIO GIROLAMO PORTA

Seduta del 07/02/2024

FATTO

La ricorrente, titolare di un conto corrente abilitato all'operatività on line intrattenuto presso l'intermediario convenuto, chiede il rimborso della somma di euro 18.000,00 fraudolentemente sottratta da terzi malfattori in data 18/04/2023, corrispondente a due operazioni di bonifico istantaneo eseguite a distanza, mediante addebitate sul predetto rapporto in difetto di autorizzazione.
In particolare, la ricorrente espone in fatto: di essersi collegata al sito internet dell'intermediario alle ore 15:45 del 18/04/2023 e di aver visualizzato la consueta videata di accesso all'area riservata ove digitava negli appositi campi i dati personali (username e password); di aver visualizzato un messaggio che preannunciava un contatto telefonico da parte di un operatore dell'istituto di credito entro 48 ore per fornire assistenza; di aver reiterato senza successo la procedura di accesso; di essere stata contattata, dopo pochi minuti, da un sedicente operatore dell'intermediario il quale segnalava la necessità di effettuare una procedura di aggiornamento, cui la medesima avrebbe dato seguito, accorgendosi che in alcuni passaggi fosse l'interlocutore a operare da remoto sul suo pc; di aver resettato il proprio telefono mobile, su espressa richiesta del falso operatore, rilevando nel corso della procedura la ricezione di un SMS relativo a una disposizione di bonifico di € 9.000,00 che destava sospetto; di aver pertanto contattato la filale dell'intermediario avvedendosi della frode perpetrata in suo danno.
Ritenendo di essere rimasta vittima di una truffa informatica perpetrata con la tecnica del "man in the browser", la medesima riferisce di aver sporto denuncia presso gli organi di

polizia il giorno seguente, depositandone copia presso l'intermediario ai fini del disconoscimento dei predetti bonifici formalmente effettuato in data 25/05/2023.
La ricorrente afferma di non aver rivelato ad alcuno le proprie credenziali di accesso al sito della banca constatando, piuttosto, che i malfattori fossero già in possesso di tutti i suoi dati personali. Ritiene plausibile che questi siano riusciti a ricostruire la sua identità digitale interferendo con il proprio computer munito di antivirus e a intercettare il collegamento al sito della banca bloccandone l'accesso.
Insoddisfatta dell'esito del reclamo notificato alla controparte in data 23/06/2023, la ricorrente, ascrivendo la responsabilità dell'accaduto all'intermediario per non aver predisposto idonei presidi di sicurezza a tutela dei servizi erogati, ha adito l'Arbitro chiedendo il rimborso della somma complessivamente sottratta, pari a € 18.000,00, e la refusione delle spese di assistenza difensiva quantificate forfettariamente in € 1.000,00, oltre accessori.
Instaurato il contraddittorio, l'intermediario descrive la tipologia della truffa di cui sembra essere rimasta vittima la ricorrente ricostruendone le modalità. In particolare espone che la ricorrente si sarebbe collegata con il proprio computer al sito della banca tramite browser, visualizzando una pagina web apparentemente riconducile a quella dell'intermediario, ove avrebbe inserito le proprie credenziali di accesso all'home banking senza successo. Rappresenta che la cliente potrebbe aver digitato un indirizzo erroneo o essere stata dirottata su un sito "esca", non coincidente con quello della banca e che, nonostante la correttezza delle credenziali inserite, la medesima non si sarebbe insospettita proseguendo con altri due tentativi di accesso parimenti non andati a buon fine. A questo punto, la cliente sarebbe stata contattata da un sedicente operatore dell'intermediario, il quale fingendo di guidarla in una procedura di aggiornamento, in realtà avrebbe eseguito l'accesso da remoto compiendo i due bonifici controversi.
Evidenzia come la ricorrente abbia ammesso in sede di denuncia di aver seguito le indicazioni del truffatore e di aver notato che in alcuni casi fosse quest'ultimo ad operare direttamente a distanza. Obietta che la ricorrente non si sarebbe peritata di contattare prontamente il Servizio clienti a fronte dei 3 tentativi falliti di accesso, fidandosi delle istruzioni impartite dal sedicente operatore. Eccepisce poi come parte ricorrente pur sostenendo di essersi avvalsa di "un pc munito di antivirus", non avrebbe provato tale circostanza, benché fosse suo onere, ai sensi degli artt. 2 e 3 del contratto di apertura di conto corrente, installare sui dispositivi efficaci programmi antivirus.
L'intermediario si oppone dunque alla domanda della ricorrente rilevando che le operazioni di pagamento controverse sarebbero state eseguite senza alcuna anomalia o irregolarità rilevate dai sistemi informatici, mediante autenticazione della legittima titolare con un sistema dinamico multifattoriale conforme a SCA, del quale descrive in termini generali il funzionamento.
In particolare riferisce che per accedere al Servizio di Internet Banking, è necessario inserire l'User ID fornito dalla Banca e non modificabile dal cliente; il PIN, che solo il cliente conosce e può modificare; l'OTP Login, generato da dispositivo *** Pass Code o da token dell'intermediario per accedere all'Area Riservata; infine, l'OTP Dispositivo generato da dispositivo *** Pass Code o da token dell'intermediario per confermare gli ordini di pagamento disposti dal cliente. Nel caso che occupa, la cliente avrebbe scelto, quale strumento di autenticazione, il dispositivo ***Pass Code. All'uopo, la resistente allega taluni tracciati informatici nell'ambito dei quali la sigla "SCAPSD2=S" presente nella "colonna N" dimostrerebbe che le transazioni in parola sono state eseguite in modalità SCA; afferma inoltre che lo schema di autenticazione associato al profilo della ricorrente prevede abilitazioni dispositive a tre fattori (PSW, OTP PIN e OTP P), come dimostrato dalla sigla "S44" presente nella "colonna N DATI ZEB" dei log prodotti, sia per l'accesso

tramite Pc che tramite device mobile. Precisa che il dispositivo ***Pass Code può essere installato su un unico dispositivo mobile scelto dall'utente (cellulare o tablet). Pertanto, ritiene che i codici OTP utilizzati per autenticare i bonifici siano stati generati su un device mobile della cliente e dalla stessa comunicati al malfattore, che operava direttamente sull'home banking da PC essendo riuscito ad effettuare l'accesso da remoto al computer della ricorrente, secondo le risultanze di cui ai log allegati.
La resistente ascrive pertanto la responsabilità del fatto occorso, alla colpa grave della ricorrente, la quale avrebbe imprudentemente cooperato con il truffatore seguendo tutte le istruzioni ricevute, malgrado le e-mail informative sull'esecuzione dei bonifici recapitate alla stessa; la medesima avrebbe infatti seguitato nel coadiuvare il malfattore, consentendogli di resettare il personal computer e il cellulare della ricorrente, cancellando ogni traccia della telefonata ricevuta e degli accessi effettuati. Eccepisce di aver fornito alla clientela informazioni utili in merito ai comportamenti da adottare per riconoscere ed evitare le varie tipologie di frodi. Chiede pertanto al Collegio di pronunciarsi per il non accoglimento del ricorso in quanto infondato.

DIRITTO

La ricorrente invoca l'accertamento del proprio diritto a ottenere il rimborso dell'importo complessivo di euro 18.000,00 corrispondente a due operazioni di pagamento a mezzo bonifici istantanei eseguiti a distanza da ignoti malfattori, all'esito di una truffa perpetrata attraverso il preliminare invio di un sms esca seguito da una telefonata di un soggetto spacciatosi falsamente come operatore dell'intermediario.
La materia oggetto di vertenza trova specifica regolamentazione nelle disposizioni del d.lgs. 27 gennaio 2010, n. 11, di recepimento della direttiva 2007/64/CE, come modificato dal d.lgs. 218/2017, che ha recepito la nuova Direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015 sui servizi di pagamento nel mercato interno (PSD2). Le operazioni controverse risultano poste in essere anche sotto la vigenza del Regolamento Delegato (UE) n. 2018/389 della Commissione che definisce i requisiti per l'autenticazione forte previsti dalla citata direttiva.
La disciplina richiamata prevede che il rischio di utilizzazione fraudolenta degli strumenti di pagamento ricada, in prima battuta, sull'intermediario, il quale può sottrarsi all'obbligo di rimborso delle somme fraudolentemente sottratte fornendo la prova del dolo ovvero della colpa grave dell'utilizzatore, ai sensi del combinato disposto degli artt. 7 e 12, comma 4, d.lgs. n. 11/2010, e della Sez. IV, § 2, del Provvedimento Banca d'Italia 5.7.2011.
In particolare, ai sensi dell'art. 10 del d.lgs. n. 11 del 27 gennaio 2010, "qualora l'utilizzatore dei servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, è onere del prestatore dei servizi di pagamento provare che l'operazione di pagamento 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". Ai sensi del comma 2, "quando l'utilizzatore di servizi di pagamento neghi di avere autorizzato un'operazione di pagamento eseguita, l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utilizzatore medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'art. 7" del medesimo decreto legislativo. Da ultimo, il d.lgs. n. 218/17 ha introdotto nell'art. 10, comma 2, d.lgs. n. 11/2010 la precisazione secondo cui "è onere del prestatore di servizi di pagamento,

compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, fornire la prova della frode, del dolo o della colpa grave dell'utente" (cfr. ABF Coll. Coord., nn. 3947/2014; 3498/2012; 991/2014. Nella giurisprudenza di legittimità, cfr. Cass. n. 2950/2017 e n. 9158/2018).

Nel caso in esame, dalla documentazione agli atti si evince che le operazioni disconosciute consistono in n. 2 operazioni di bonifico compiute in data 18 aprile 2023 (in modalità istantanea) utilizzando il servizio di internet banking, ciascuna per l'importo di € 9.000,00 (nel giro di 6 minuti l'una dall'altra) alle ore 16:02 e alle ore 16:08.

A sostegno della regolarità formale delle menzionate transazioni in regime di SCA, l'intermediario fornisce una descrizione generale del processo autorizzativo adottato funzionante mediante inserimento delle seguenti credenziali: Codice Identificativo Utente (User ID) fornito dalla Banca e non modificabile dal cliente; Password di Accesso (PIN): codice alfanumerico che solo il cliente conosce e può modificare; OTP Login (password generata da dispositivo *** Pass Code o *** token per accedere all'Area Riservata); OTP Dispositivo (password generata da dispositivo *** Pass Code o *** token per confermare gli ordini di pagamento disposti dal cliente). Al riguardo afferma che in sede di sottoscrizione del contratto, la ricorrente ha scelto, quale strumento di autenticazione, il dispositivo *** Pass Code, consistente in un software che genera codici temporanei (OTP) installabile su un unico dispositivo mobile scelto dall'utente (cellulare o tablet).

Ebbene, in relazione alla fase di login l'intermediario sostiene che la modalità di autenticazione associata al profilo della ricorrente e al relativo contratto di home banking n. ***383, la quale prevede abilitazioni dispositive a tre fattori (PSW, OTP PIN e OTP P) per "interfaccia PC internet" e per l'"interfaccia mobile"; tale circostanza troverebbe conforto nel codice "S44" valorizzato nei tracciati elettronici prodotti dai quali dovrebbe evincersi che la cliente si è connessa all'home banking da WEB (colonna K "TIPO") e che la connessione è avvenuta tramite personal computer (colonna L "USERAGENT").

Dalle schermate prodotte può riscontrarsi una prima attività di login alle ore 15:52 del 18/04/2023 ed una seconda alle successive ore 16:00 da Web tramite lo stesso computer utilizzato nei giorni precedenti dalla cliente. Emerge inoltre che i predetti accessi siano stati autorizzati tramite "schema S44" (vale a dire con tre fattori di autenticazione: PSW, OTP PIN e OTP P); tuttavia non si riscontrano riferimenti ai fattori di autenticazione utilizzati.

In relazione alla fase dispositiva, l'intermediario deduce che il primo bonifico di € 9.000,00 sarebbe stato autorizzato alle ore 16:02 ed il secondo, del medesimo importo, alle ore 16:08, entrambi eseguiti in regime di SCA ricavabile dalla presenza della stringa "SCAPSD2=S" in corrispondenza della colonna N, denominata "DATI ZEB", nei log allegati unitamente alla legenda esplicativa.

Alla stregua delle anzidette evidenze sembrerebbe che le operazioni disconosciute siano state autenticate con un sistema di autenticazione multifattoriale; tuttavia anche rispetto a questa fase del processo elettronico sotteso alla prestazione del servizio di internet banking non è dato riscontrare quali fattori siano stati in concreto utilizzati tra quelli enunciati dal PSP (cfr. ABF Coll. Bari, Dec. n. 5142/2023; Coll. Napoli, Dec. n. 13995/2022). La valutazione della conformità a SCA di tutte le fasi che caratterizzano la procedura di autenticazione forte (accesso all'area riservata, riconoscimento, autorizzazione e disposizione di ogni singola operazione), come non si è mancato di affermare, costituisce - in aderenza al dato normativo - un prius logico giuridico rispetto all'esame di eventuali profili di colpa ascrivibili all'utilizzatore nella gestione dello strumento di pagamento (cfr. ABF Bari, Dec. n. 6257/2022; Coll. Torino, Dec. n. 14600/2021). Difettando la prova completa della procedura elettronica illustrata in termini generali dalla resistente non è possibile ritenere che le transazioni in questione siano avvenute

all'interno di un ambiente adeguatamente presidiato, in aderenza agli standard esigibili dalla regolamentazione pro tempore vigente in materia, come declinati dall'EBA a mente degli orientamenti del 21 giugno 2019 elaborati in tema di autenticazione forte (cfr. ABF Coll. Bari, Dec. n. 3965/2023; Coll. Napoli, Dec. n. 13995/2022, cit.). L'intermediario ha infatti mancato di fornire la prova concludente della regolare autenticazione di tutte le operazioni controverse, oltre che del dolo o colpa grave della cliente (cfr. ABF Roma, Dec. nn. 3750/2021, 16121/2021; Cass., Sez. VI, sent. n. 26916/2020; Cass. Sez. I, sent. n. 16333/2016).
Per quanto innanzi, alla stregua delle normative e dei principi innanzi citati, ricorrono le condizioni per porre a carico dell'intermediario le conseguenze economiche delle transazioni disconosciute e, dunque, per accogliere la domanda di restituzione della somma illecitamente sottratta in danno della ricorrente, pari a euro 18.000,00.
Inoltre, secondo l'orientamento consolidato dell'Arbitro (cfr. Coll. Coordinamento, Dec. nn. 3498/2012, 6174/2016) alla ricorrente che ne ha fatto domanda documentandone l'esborso spetta anche la refusione delle spese di assistenza difensiva, quale risarcimento del pregiudizio patito per la condotta dell'intermediario, che il Collegio liquida in via equitativa come da dispositivo.

P.Q.M.

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda alla ricorrente la somma di € 18.000,00. Dispone altresì che l'intermediario corrisponda la somma di € 350,00 a titolo di contributo alle spese di assistenza professionale.
Il Collegio dispone infine, 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 al ricorrente la somma di € 20,00 quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
ANDREA TUCCI