Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI BOLOGNA

composto dai signori:

(BO) MARINARI	Presidente
(BO) LOMBARDI	Membro designato dalla Banca d'Italia
(BO) BULLO	Membro designato dalla Banca d'Italia
(BO) MIRABELLI	Membro di designazione rappresentativa degli intermediari
(BO) D ATRI	Membro di designazione rappresentativa dei clienti

Relatore ETTORE MARIA LOMBARDI

[redacted]

FATTO

Nel proprio ricorso, la parte ha riferito che il 13 gennaio rimaneva vittima di una frode informatica e della conseguente sottrazione dell'importo di 17.600,00 euro ad opera di ignoti, in quanto aveva ricevuto, tramite mail, la comunicazione di un accesso al proprio servizio di *home banking* e dell'autorizzazione di una operazione. Così, accedeva immediatamente al proprio servizio *home banking*, rilevando l'esecuzione di una operazione di bonifico in favore di un soggetto a lui sconosciuto, e provvedeva a contattare immediatamente la propria filiale comunicando l'accaduto e bloccando il proprio conto corrente. Si avvedeva della ricezione nel proprio *smartphone* di alcuni sms apparentemente provenienti dall'intermediario, che si andavano ad inserire nella chat ufficiale e da cui rilevava la registrazione di un nuovo dispositivo cellulare collegato al proprio servizio di conto corrente *on line*. Il ricorrente ha affermato, quindi, di non aver mai cliccato sul link contenuto nel messaggio del 15 dicembre 2022 il cui testo non presentava evidenti elementi di inattendibilità, in quanto privo di errori grammaticali, e contenente

l'indicazione dell'intermediario nella stringa del link, ma ha fatto seguito un contatto telefonico con un sedicente operatore che si presentava come assistente per l'installazione della app offrendogli aiuto alla soluzione del problema, pertanto si determinava a rispondere installando con il suo aiuto l'app. L'operazione di bonifico disconosciuta veniva effettuata da terzi non autorizzati nella successiva data del 13 gennaio 2023 e, quindi, a quasi un mese dal contatto telefonico e dagli sms ricevuti, senza alcuna interazione da parte sua e senza che rilevasse mal funzionamenti ai propri apparati o anomalie operative al conto *on line*. Il ricorrente afferma che la responsabilità della banca per la captazione dei dati (o codici) dei correntisti è stata inquadrata dalla giurisprudenza sotto il profilo della responsabilità civile per attività pericolose conseguente alla violazione dei dati personali, e che un ulteriore profilo di responsabilità per l'intermediario attiene al mancato e tempestivo blocco della operazione disconosciuta. L'operazione eseguita ha una connotazione internazionale e quindi evidentemente anomala rispetto alla sua normale operatività, e, poi, il bonifico fraudolento ha come destinatario un conto corrente intrattenuto presso il medesimo istituto di credito, circostanza che imponeva all'intermediario il blocco o l'immediato *recall* degli importi. Inoltre, nel proprio reclamo del 1 marzo 2023 formulava delle richieste documentali in merito alle quali l'intermediario non ha fornito alcun riscontro.

Il ricorrente ha, così, chiesto al Collegio di «*[D]ichiarare l'intermediario […] tenuto alla consegna della documentazione anche informatica richiesta con reclamo […]. Accertata la responsabilità contrattuale ed extracontrattuale-ex art. 2050 c.c. […] delle operazioni disconosciuti pari a complessive […]»] 17.600,00 euro oltre ad interessi e rivalutazione dalla data delle operazioni e fino al loro effettivo rimborso, nonché di ogni onere collegato […]».*

Dal proprio canto, l'intermediario, nel controdedurre, ha affermato che il ricorrente è titolare del conto corrente n. ***8400, su cui è attivo il servizio di internet banking, e che, per quanto attiene alla richiesta documentale ha fornito alla parte ricorrente tutto ciò che aveva diritto di richiedere, specificando espressamente di rimanere a disposizione per fornire ogni eventuale ulteriore documentazione alla Pubblica Autorità, posto che quanto richiesto impattava sulla sicurezza informatica aziendale o sui diritti dei dipendenti e non poteva essere fornito su semplice richiesta del cliente. La resistente ha sostenuto che i messaggi ricevuti dal cliente indirizzavano a un sito estraneo alla banca, tanto l'episodio truffaldino non avrebbe prodotto alcun effetto se il ricorrente avesse contattato l'intermediario per segnalare o chiedere chiarimenti sull'anomalo messaggio ricevuto e sull'*enrollment* del *device* dei truffatori da lui consentito quasi un mese prima della truffa. Il 15 dicembre 2022 è stata disposta un'operazione di *login* attraverso un nuovo dispositivo mobile ed è stato, poi, effettuato l'*enrollment* dell'app su tale dispositivo mobile, operazione autorizzata con successo tramite *SecureCall* su numero certificato con digitazione del PIN dispositivo noto solo all'utente. Il 13 gennaio 2023 è stata disposta un'operazione di bonifico ordinario di 17.600,00 euro, e, per stessa ammissione del ricorrente, emerge che lo stesso abbia inconsapevolmente aderito a un attacco di *phishing*, ritenendo di operare sul sito dell'intermediario. Al ricorrente è imputabile una violazione degli obblighi di custodia dei propri dati identificativi e dispositivi on line, e pertanto il danno lamentato è ascrivibile, interamente ed esclusivamente, alla sua condotta. L'operazione disconosciuta non era, per sua natura, né annullabile né richiamabile. Quanto alla sua presunta anomalia, il monitoraggio della "normalità" delle operazioni disposte dai clienti non rientra tra i compiti della banca, né tra i suoi obblighi contrattuali. L'intermediario ha, quindi, chiesto di *«[…] volere dichiarare improcedibile il ricorso per mancanza di un preventivo reclamo ovvero, nel merito, di volerlo rigettare per*

l'assoluta assenza di responsabilità in capo alla banca […]».

In sede di repliche, la parte ricorrente ha affermato che controparte non spiega come il messaggio civetta abbia potuto inserirsi nel canale di comunicazione della banca, atteso che il link è riferibile all'intermediario contenendo al suo interno il nome dello stesso. La banca, poi, ha versato in atti solo una parte della documentazione richiesta, in quanto controparte non ha allegato alcuna prova della dichiarata attività di recupero del bonifico "banca su banca". In effetti, è frequente nei nuovi attacchi informatici che vi sia una latenza tra attacco con *enrollment* di nuova app e operazione dispositiva (in alcuni casi anche oltre i 30 gg), per non allertare i sistemi di controllo con più operazioni di diverso tipo in una stessa data, e l'intermediario afferma che vi è stato l'*enrollment* di una nuova app su altro *device* ma di questo fornisce dettagli informatici parziali e non prova le modalità con cui i codici a ciò necessari siano stati inviati e effettivamente inseriti dal ricorrente per l'autenticazione forte di tale procedura. Dai log allegati dalla banca, inoltre, emerge che due distinti dispositivi hanno operato contemporaneamente (c.d. *aliasing*) sul conto e l'intermediario non è in grado di provare quale sia la SCA attribuibile al cliente per la nuova app perché vi sono due distinti processi di *enrollment* in pochi minuti andati entrambi a buon fine. Di conseguenza, non è possibile stabilire quale sia il dispositivo realmente utilizzato per l'operazione fraudolenta. L'intermediario, infine, non ha provato in alcun modo la cessione di codici ad un terzo ed in particolare quella relativa alla certificazione della nuova applicazione e del parametro biometrico, attività dalle quali è discesa la successiva attività fraudolenta dell'hacker. Difatti, l'operazione disconosciuta è stata eseguita da altro *smartphone*, attraverso una nuova app ed un dato biometrico a lui non riferibile.

In sede di controrepliche, parte resistente ha precisato che, in sede di controdeduzioni è stato documentato come il dispositivo attraverso cui è stato perpetrato l'evento incriminato fosse stato enrollato il 15 dicembre 2022 attraverso *SecureCall* su numero certificato; che per la definizione del processo di *enrollment*, al fine di consentire la corretta registrazione dell'app su di un nuovo dispositivo devono essere inseriti al suo interno il Codice Utente, la Data Importante nota solo all'utente ed il PIN dispositivo. Previa chiamata *SecureCall*, con inserimento corretto del PIN dispositivo, si può accedere al proprio servizio di *homebanking*; che per quanto riguarda il tentativo di recupero delle somme, allega il riscontro ricevuto tramite messaggio swift interbancario dalla banca su cui sono state trasferite le somme da parte della frodatrice; la filiale ha provato più volte a contattarla senza ricevere risposta.

DIRITTO

Le operazioni contestate sono state poste in essere sotto il vigore del d.lgs. 27 gennaio 2010, n. 11, come modificato dal d.lgs. 15 dicembre 2017, n. 218 di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2), che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE, e di adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta.

Alla luce delle informazioni e della documentazione acquisita, la operazione per cui è ricorso può essere sintetizzata con un bonifico di 17.600,00 euro. A parte il blocco dello

strumento che parte ricorrente afferma di aver richiesto il 16 gennaio 2023, dalla documentazione allegata dall'intermediario risulta che che il 15 dicembre 2022 è stato effettuato l'*enrollment* di un nuovo dispositivo da parte del cliente che risultava avere già attivo il servizio di *SecureCall*. Pertanto, l'accesso è stato scandito da due eventi, ovvero, *in primis*, la fase di *login* effettuato sull'app, ove viene richiesto l'inserimento delle credenziali (Codice Utente o Alias, Data Importante – nota solo all'utente e impostata in fase di primo accesso al Servizio –, PIN Dispositivo), e, *in secundis*, completata questa prima fase, l'utente non ha ancora avuto accesso al servizio, in quanto, a tal fine, deve necessariamente completare il processo di *enrollment*, che prevede l'autenticazione mediante SCA (chiamata *SecureCall* sul numero di telefono associato all'utente ed inserimento del PIN dispositivo associato al numero *SecureCall*).

Dalle evidenze allegate emerge dunque che, il 15 dicembre 2022, alle ore 16:03:48, è stata effettuato il login su un nuovo dispositivo mobile (*Galaxy A120e*), autorizzato mediante Codice Utente, Data importante e Pin Dispositivo, ove alle ore 16:04:59, è stato effettuato l'*enrollment* dell'app sul dispositivo Mobile summenzionato; tale operazione è stata autorizzata con successo tramite *SecureCall* su numero certificato del ricorrente (cfr. modulo di ricorso) con digitazione del PIN dispositivo. Il campo "*operation phase*" reca anche la dicitura "OTP", sebbene l'intermediario nulla specifichi sul punto.

L'intermediario ha altresì prodotto il log della *SecureCall*, da cui si evince la richiesta di inserimento del PIN dispositivo, "*seguito dal tasto cancelletto*". Per quanto attiene alla validità della *SecureCall* quale fattore di autenticazione forte, allora, dalla documentazione allegata si ravvisa la presenza dei due criteri di autenticazione e in particolare, la login app tramite codice utente, e il Pin, per il primo e secure call con digitazione del Pin, per il secondo (cfr., ex multis, Collegio di Bologna, decisione n. 8399 del 2023).

L'intermediario, dipoi, afferma che per l'accesso effettuato nell'app i due fattori di autenticazione ai fini della SCA sono, il possesso del dispositivo mobile registrato e associato al numero *SecureCall*, sul quale deve essere digitato il PIN dispositivo, e la conoscenza del PIN dispositivo, associato al numero *SecureCall*. Poiché anche l'operazione di bonifico sarebbe stata autorizzata tramite gli stessi due fattori di autenticazione forte, dalle evidenze allegate emerge che, il 13 gennaio 2023, alle ore 09:22, è stata disposta un'operazione di *login* attraverso canale app per mezzo del dispositivo mobile in precedenza all'"enrollment", e tale operazione è stata autorizzata mediante inserimento del PIN dispositivo all'interno dell'app. Alle ore 09:29, è stato disposto un bonifico ordinario di 17.600,00 euro. L'operazione è stata autorizzata mediante inserimento del PIN dispositivo all'interno dell'app.

Tuttavia, da quanto affermato dall'intermediario e dalle evidenze da questo allegate, non emerge con chiarezza se in fase di autorizzazione dell'operazione fraudolenta sia stata effettuata la chiamata "*SecureCall*". Inoltre, il campo "*operation phase*" dei log sopra riportati reca la dicitura "OTP", sebbene l'intermediario nulla specifichi sul punto.

Le carenze ora evidenziate comportanto, pertanto, che il Collegio non debba procedere alla valutazione della sussistenza degli indici di colpa grave in capo all'utilizzatore.

PER QUESTI MOTIVI

Il Collegio – in accoglimento del ricorso – dichiara l'intermediario tenuto in favore della parte ricorrente alla restituzione dell'importo complessivo di euro 17.600,00 (diciassettemilaseicento/00), oltre interessi legali dalla data del reclamo.

Dispone, inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di Euro 200,00 (duecento/00) quale contributo alle spese della procedura e alla parte ricorrente quella di Euro 20,00 (venti/00) quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

[redacted]