COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) ACHILLE	Membro designato dalla Banca d'Italia
(MI) CETRA	Membro designato dalla Banca d'Italia
(MI) PERON	Membro di designazione rappresentativa degli intermediari
(MI) BARGELLI	Membro di designazione rappresentativa dei clienti

Relatore (MI) PERON

Seduta del 20/07/2023

FATTO

Parte ricorrente rappresenta al Collegio di aver ricevuto, il 31.01.2023 alle ore 15:59, un messaggio *sms* dall'emittente della sua carta di pagamento, che lo informava del blocco di carta/conto per mancata verifica della sicurezza invitandolo a cliccare su un *link* per procedere allo sblocco. Cliccando sul *link* si apriva una pagina che sembrava effettivamente essere quella di accesso alla sua area riservata, nella quale inseriva il nome utente e la *password*. Dopo la digitazione delle credenziali, compariva un messaggio di errore per inserimento di credenziali errate e riceveva la telefonata del sedicente direttore di una filiale dell'intermediario, che lo invitava a seguire con lui una procedura per lo sblocco di carta/conto. Seguendo le istruzioni dell'interlocutore, accedeva all'area personale della sua carta di credito e successivamente all'*home banking* del proprio conto corrente, digitando un codice OTP ricevuto tramite *sms* dall'intermediario. Terminata la procedura di sblocco, parte ricorrente veniva congedato dall'interlocutore, che lo avvertiva che avrebbe ricevuto un'ulteriore chiamata il giorno successivo (mai ricevuta) per la conferma del buon esito della procedura. Avendo ricevuto, alle ore 18:43 del 31.01.2023, una e-mail dall'intermediario di conferma

dell'esecuzione dal suo conto corrente di un bonifico di € 3.600,00 (corrispondente all'intero importo giacente sul conto) in favore di soggetto a lui sconosciuto, si rendeva conto di avere subito una truffa. Presentava quindi denuncia e reclamo con esito negativo.

Con riguardo alle modalità della truffa parte ricorrente rappresenta al Collegio quanto segue: ***i)*** i messaggi truffaldini sono giunti nella medesima chat in cui l'intermediario e l'emittente della sua carta di credito inviano ordinariamente le loro comunicazioni; ***ii)*** l'utenza telefonica del sedicente operatore risulta intestata a una filiale dell'intermediario; ***iii)*** il codice *otp* ha generalmente una validità temporale assai limitata (al più qualche minuto), mentre nel caso in esame il bonifico disconosciuto è stato eseguito circa due ore e mezzo dopo la sua generazione: il codice *otp* risulta generato alle ore 16:15, mentre il bonifico è delle ore 18:42.

Alla luce di quanto sopra formula la seguente domanda: *"considerato che, nella presente fattispecie, i sistemi degli intermediari, che dovrebbero permettere ai clienti di operare in totale sicurezza, sono stati palesemente violati senza che alcuna responsabilità sia ascrivibile*" alla parte ricorrente, "*si chiede che gli venga rifusa l'intera somma sottrattagli*" pari a € 3.600,00.

L'intermediario controdeduce ritenendo evidente che il cliente ha comunicato al terzo frodatore i codici ricevuti sui propri contatti certificati (numero di cellulare ed indirizzo e-mail) le proprie credenziali e i codici necessari per l'*enrollment* del *device* dei frodatori. Precisa che: ***i)*** l'*app* può essere installata su un solo dispositivo certificato per volta, attivando una nuova "licenza smart OTP" grazie al corretto inserimento di nome utente, *password* e *otp* trasmesso via e-mail e *sms* ai contatti certificati dell'utente; ***ii)*** l'accesso all'*app* richiede l'inserimento simultaneo di nome utente, *password* e *pin* dispositivo, conosciuti solo ed esclusivamente dall'utente; ***iii)*** per autorizzare le operazioni dispositive è necessario digitare il *pin* dispositivo. Per tali ragioni ritiene evidente la colpa grave in cui è incorsa parte ricorrente, senza la cui attiva collaborazione, il frodatore non sarebbe mai riuscito a concludere il bonifico contestato, considerato altresì che la truffa in esame non risulta essere particolarmente sofisticata.

In ogni caso precisa che l'utenza del cliente è stata bloccata, subito dopo la chiamata del ricorrente, impedendo al truffatore di concludere ulteriori operazioni; e di aver avviato, in data 01.02.2023, la procedura di recall del bonifico contestato, che ha però avuto esito negativo. Osserva infine che l' *otp*, a cui si riferisce il cliente, è il codice necessario non per autorizzare il bonifico contestato bensì per attivare una nuova "licenza smart OTP".

Per tali ragioni chiede che vengano respinte tutte le contestazioni sollevate da parte ricorrente e in via subordinata qualora dovesse ravvisarsi un qualsivoglia responsabilità a suo carico chiede sin d'ora che si tenga conto del comportamento colpevole e imprudente tenuto da parte ricorrente essendo questo rilevante ai fini di un concorso di colpa ai sensi dell'art. 1227 c.c.

Nelle repliche parte ricorrente ribadisce la vulnerabilità del sistema di sicurezza dell'intermediario che ha consentito a terzi di inviare *sms* all'apparenza genuini, di chiamare da un'utenza regolarmente intestata alla banca e di utilizzare un codice *otp* a distanza di due ore e mezzo dalla sua generazione.

Osserva che vi è un'assoluta carenza probatoria circa l'autenticazione, la corretta registrazione e contabilizzazione delle operazioni disconosciute e la colpa grave dell'utente.
Rimarca che le caratteristiche della truffa e i canali adoperati dai frodatori hanno indotto l'utente a non insospettirsi e a fare conseguentemente affidamento sulla procedura da seguire, escludendosi ogni profilo colposo dalla sua condotta.
Nelle sue controrepliche l'intermediario eccepisce di aver adottato un sistema di autenticazione forte, di cui ha fornito ampia prova, costruito in modo tale da impedire l'utilizzo dell'internet banking a soggetti non autorizzati e, come nel caso di specie, può essere violato solo attraverso la divulgazione a terzi sconosciuti di tutti i codici di accesso delle *otp* necessarie per l'*enrollment* di un nuovo dispositivo mobile. Ritiene che come si evince anche dalla documentazione tecnica prodotta, la truffa non si sarebbe mai perfezionata se il cliente non avesse comunicato al terzo frodatore tutte le "proprie credenziali" e, in particolare, i codici *otp* necessari per l'installazione dell'*app*. Osserva che il messaggio truffaldino è stato apparentemente inviato dall'emittente, ossia da un soggetto completamente diverso rispetto alla banca e di aver più volte sensibilizzato la propria clientela sui temi della sicurezza e riservatezza dei dati, introducendo apposite e specifiche informative che sono state espressamente visionate dal ricorrente.

DIRITTO

La controversia in esame attiene all'accertamento del diritto di parte ricorrente ad ottenere il rimborso, da parte dell'intermediario resistente, della somma di € € 3.600,00, inerente un'operazione di bonifico disposta *on-line*, in data 31.01.2023 alle ore 18:42, e contestata come fraudolenta.
Tanto premesso, si osserva che le operazioni in esame sono disciplinate del D. Lgs. 27.1.2010 n. 11 di recepimento della Direttiva sui servizi di pagamento (Direttiva 2007/64/CE del 13 novembre 2007) e del relativo Provvedimento attuativo della Banca d'Italia del 5.7.2011. Come è noto, i principi fissati da tale impianto normativo, in materia di strong customer authentication (SCA), fissano due passaggi ineludibili che attengono al piano degli oneri probatori: *a)* è l'intermediario a dover provare (oltre all'insussistenza di malfunzionamenti) l'autenticazione, la corretta registrazione e contabilizzazione delle operazioni disconosciute, avendo presente che l'autenticazione forte (SCA) è richiesta sia nella fase di accesso al conto / *enrollment* dell'applicazione / registrazione della carta sul *wallet*, sia nella fase di esecuzione delle singole operazioni; *b)* è sempre l'intermediario a dover provare tutti i fatti idonei ad integrare la colpa grave dell'utilizzatore, unica ipotesi in cui, oltre al dolo, lo stesso può patire le conseguenze dell'utilizzo fraudolento dello strumento di pagamento. In quest'ambito dunque, costante giurisprudenza arbitrale, ritiene che l'eventuale negligenza del cliente possa solo venire in rilievo solo allorquando l'intermediario abbia fornito la prova piena della scrupolosa osservanza del sistema di SCA e della predisposizione di congegni di *alert* (cfr. *ex multis* Collegio di Milano, decisione n. 8262/2020).
Il caso in esame è una fattispecie di *sms spoofing*, misto a ID *caller spoofing*. Tale tipo di truffa è considerato come potenzialmente più decettivo rispetto al comune *phishing* o *vishing*, che si ritiene possano essere contrastato con l'uso di una diligenza minima, in

considerazione della loro diffusione e della generalmente scarsa idoneità a trarre in inganno i clienti.
Ciò posto, si impone dunque in prima battuta la verifica sul sistema di autenticazione predisposto dall'intermediario e sul rispetto dei requisiti di cui alla predetta disciplina, avendo egli l'onere di provare *(a)* 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*»; *(b)* che il sistema di autenticazione e l'autorizzazione delle operazioni di pagamento contestate sono conformi alla SCA, che 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.
Al riguardo, l'intermediario sostiene che l'operazione è stata correttamente contabilizzata, registrata e autenticata e ricostruisce come segue l'operatività fraudolenta:

a) registrazione di un nuovo dispositivo sull'*app*, con attivazione del servizio "*licenza smart OTP*";
b) accesso all'*app* dal nuovo dispositivo;
c) esecuzione dell'operazione disconosciuta.

Con riguardo al punto *a)* sopra indicato, l'intermediario rappresenta:

- che alle ore 16:16 del 31.01.2023 è stata attivata una nuova licenza "*smartOTP*" presumibilmente dal terzo frodatore sul proprio dispositivo mobile Android;
- che il frodatore, per attivare la nuova licenza *smartOTP*, ha dovuto inserire UTENZA + PASSWORD + OTP ricevuto via e-mail + OTP ricevuto via *sms* sul cellulare della cliente.

Tuttavia, il Collegio osserva che dalla documentazione in atti non è provata l'evidenza dell'inserimento di Utenza + Password; inoltre, sia l'OTP via e-mail che all'OTP via *sms* non riportano il testo del messaggio.
Con riguardo al punto *b)* sopra indicato, l'intermediario afferma che pochi secondi dopo l'attivazione della nuova licenza "*smartOTP*" i sistemi hanno registrato un accesso all'*home banking* tramite *app* proprio dal medesimo indirizzo IP ****56 che aveva attivato la nuova licenza. Secondo l'intermediario tale accesso è possibile previo inserimento di Utenza + Password + PIN DISPOSITIVO. Tuttavia, il Collegio rileva che, dall'esame dei *log*, non vi è alcuna evidenza dei fattori di autenticazione effettivamente impiegati, fermo restando che i fattori indicati dall'intermediario sono solo elementi di conoscenza.
Con riguardo al punto *c)* sopra indicato, l'intermediario afferma che l'esecuzione del bonifico, è avvenuta tramite *app* con inserimento del *pin* dispositivo, per autorizzare l'operazione che viene riepilogata mediante notifica in *app*. Tuttavia, dall'esame dei *log* si rileva che non vi è evidenza dell'inserimento dei fattori di autenticazione. Nella legenda è altresì specificato che il *pin* può essere inserito anche mediante credenziali biometriche, ma ad ogni modo non vi è evidenza dell'attivazione di forme di riconoscimento biometrico. Né vengono fornite ulteriori evidenze dalle quali individuare il secondo fattore richiesto (*pin* o altro fattore biometrico) ai fini della corretta autenticazione dell'operazione.
In forza dei rilievi sopra evidenziati circa l'assenza di evidenze in merito all'inserimento:

- di Utenza + Password, per l'attivazione della nuova licenza *smartOTP*;
- di Utenza + Password + PIN DISPOSITIVO per l'accesso all'app dal nuovo dispositivo;
- dei fattori di autenticazione per l'autorizzazione dell'operazione contestata,

non risulta raggiunta la prova che l'operazione contestata è stata eseguita a seguito di una corretta "autenticazione forte" (cfr., Collegio di Milano, decisione n. 5716/2023; Collegio Torino, decisioni n. 3653/2023 e n. 16048/2022).
Conseguentemente, anche a prescindere dalla dimostrazione di una condotta gravemente colposa di parte ricorrente (in relazione alla quale incidentalmente il Collegio osserva che l'*sms* civetta era inserito in una *chat*, contenente precedenti messaggi genuini provenienti dall'intermediario, e non presentava errori), rimangono a carico dell'intermediario le operazioni contestate, non essendo stati da questi assolti gli oneri probatori di cui è gravato con riguardo alla SCA.
Per tali motivi il Collegio accoglie integralmente il ricorso.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 3.600,00.
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