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 subito una truffa, per € 6.300,00. In particolare, a seguito della ricezione alle ore 17:50 del 30.01.2023, di un *sms* dall'emittente della carta, che la informava del blocco di carta/conto per mancata verifica della sicurezza cliccava sul *link* presente nel messaggio che la rimandava alla pagina di accesso all'area riservata, senza però riuscire a completare la procedura. Il giorno successivo riceveva un sms che le preannunciava la telefonata di un operatore che in effetti la contattava alle ore 14:05 del 31.01.2023, sulla sua utenza dal numero fisso ***901. Il soggetto, qualificatosi come operatore di una filiale dell'intermediario diversa dalla sua, le chiedeva di fornire il codice di accesso, ma non la password, e di disinstallare l'*app* dal suo *device*. Parte ricorrente seguiva quindi le istruzioni del sedicente operatore e alle ore14:17 e alle 14:19 del 31.01.2023 riceveva tramite e-mail le OTP per l'*enrollment* di un nuovo dispositivo, che non riferiva a terzi. Successivamente riceveva due *sms*, alle 14:28 del 31.01.2023 e alle ore 12:41 del 01.02.2023 che le confermavano un appuntamento telefonico per aggiornarla sugli sviluppi del processo. Difatti riceveva alle ore 14:40 un'altra telefonata dal sedicente operatore, che le preannunciava una telefonata

per il giorno successivo e il 01.02.2023 un sedicente operatore la chiamava per tranquillizzarla sull'esito dell'aggiornamento. Parte ricorrente dopo la telefonata si accorgeva di non poter concludere non essere riuscita, lo stesso giorno, a concludere un'operazione di acquisto POS. Mentre la mattina del 02.02.2023, consultando la sua casella e-mail, si accorgeva dell'addebito di € 1.900,00 per un bonifico a favore di persona sconosciuta, si recava quindi presso la filiale dell'intermediario, dove apprendeva che vi era stato un altro bonifico per € 4.400,00 circa il quale non aveva ricevuto alcuna notifica.

Alla luce di quanto sopra, parte ricorrente chiede la condanna dell'intermediario alla restituzione di € 6.300,00, oltre "*spese e compensi, poiché nonostante la pubblicazione sui propri canali di proclami in ordine alla sicurezza e innovativa delle proprie tecnologie non ha tutelato la cliente che mai ha fornito a terzi le proprie credenziali complete*".

L'intermediario, anzitutto eccepisce che la richiesta di rimborso di "*spese e compensi*" non è stata avanzata in sede di reclamo e, comunque, è infondata. Nel merito ritiene evidente che parte ricorrente abbia comunicato al terzo frodatore le proprie credenziali e i codici ricevuti sui propri contatti certificati (numero di cellulare ed indirizzo e-mail) necessari per l'*enrollment* del *device* dei frodatori. Precisa al riguardo che l'*app* può essere installata su un solo dispositivo certificato per volta, attivando una nuova "licenza smartOTP" grazie al corretto inserimento di nome utente, *password* e OTP trasmesso via e-mail e *sms* ai contatti certificati dell'utente. Inoltre: *i)* l'accesso all'*app* richiede l'inserimento simultaneo di nome utente, *password* e *pin* dispositivo, conosciuti solo ed esclusivamente dall'utente; ***ii)*** per autorizzare le operazioni dispositive è necessario digitare il *pin* dispositivo. Ritiene quindi, evidente la colpa grave in cui è incorsa la parte ricorrente senza la cui attiva collaborazione, il frodatore non sarebbe mai riuscito a concludere il bonifico contestato. Osserva altresì che la truffa in esame non risulta essere particolarmente sofisticata, che l'utenza di parte ricorrente è stata prontamente bloccata, impedendo al truffatore di concludere ulteriori operazioni; e di aver avviato, in data 02.02.2023, la procedura di *recall* del bonifico contestato, che ha però avuto esito negativo. L'intermediario fa altresì presente di aver informato per tempo parte ricorrente, mediante diversi canali, sulle caratteristiche delle truffe più diffuse e sui modi per difendersi da queste e di aver approntato idonei e adeguati presidi di sicurezza.

Per tali ragioni chiede che il ricorso di parte ricorrente venga interamente rigettato e in via subordinata chiede che "*laddove dovesse ravvisarsi una qualsivoglia responsabilità*" in capo all'intermediario si tenga conto anche del "comportamento colpevole ed imprudente" tenuto da parte ricorrente, "*rilevante ai fini di un concorso di colpa ai sensi dell'art- 1266 c.c.*".

Nelle repliche parte ricorrente eccepisce non aver fornito le proprie credenziali né i codici *otp* a terzi. Osserva che il messaggio decettivo sembrava affidabile, perché si collocava nella stessa chat dei messaggi genuini ricevuti dall'emittente e che il numero da cui veniva contattata corrisponde a quello di una filiale dell'intermediario. Precisa di non aver ricevuto alcun *alert* relativo alla prima operazione fraudolenta e che i frodatori carpivano tutte le informazioni necessarie, in maniera impersonale, accedendo al suo account e-mail. Ritiene la truffa subita sofisticata e che i sistemi di sicurezza dell'intermediario si sono rivelati inadeguati. Le spese legali sono necessitate dalla risposta negativa dell'intermediario circa il richiamo del bonifico non autorizzato.

L'intermediario nelle controrepliche eccepisce che i *log* estratti comprovano la disattenzione e superficialità della cliente, la quale - se ha notato la e-mail con il primo codice *otp* e quella successiva relativa all'esecuzione del secondo bonifico contestato - non ha inopinatamente letto l'e-mail relativa alla prima operazione, il cui invio è documentato. Ritiene che gravi unicamente sulla ricorrente la responsabilità e l'onere di non permettere la manomissione del proprio indirizzo di posta elettronica. Sostiene 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. Osserva che dalla documentazione tecnica prodotta, risulta che la truffa non si sarebbe mai perfezionata se la cliente non avesse comunicato al terzo frodatore tutte le "proprie credenziali" e, in particolare, i codici *otp* necessari per l'installazione dell'*app*. Ribadisce 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 dalla 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 € 6.300,00, inerente due operazioni di bonifico disposte *on-line*, in data alle ore 18:41 del 31.01.2023 e alle ore 18:40 del 01.02.2023 e contestate come fraudolente.

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 le operazioni sono state correttamente contabilizzate, registrate e autenticate 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 delle operazioni disconosciute.

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

- che alle ore 14:21 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 "*smart OTP*" i sistemi hanno registrato un accesso all'*home banking* tramite *app* proprio dal medesimo indirizzo IP ****75 che aveva attivato la nuova licenza. Tale accesso è possibile previo inserimento di Utenza + Password + PIN DISPOSITIVO. Il Collegio osserva che stando alla legenda esplicativa del *log* in atti, l'esito 000 indica che l'evento è confermato correttamente con inserimento di tutti i parametri di sicurezza previsti e per il *login* è richiesto UTENZA + PASSWORD + PIN dispositivo impostato dal cliente.
Tuttavia, si rileva al riguardo che, dall'esame dei *log*, l'esito dell'evento non indica 000, ma solo 0 (e, quindi, un risultato che non evidenzia l'inserimento corretto di tutti i parametri di sicurezza – cfr. (cfr. Collegio di Milano, decisione n. 5716/2023) e che non vi è evidenza dei fattori di autenticazione effettivamente impiegati, fermo restando che i fattori indicati dall'intermediario sono tutti elementi di conoscenza, mancando evidenza dei fattori di inerenza e possesso.
Con riguardo al punto *c)* sopra indicato, l'intermediario afferma che l'esecuzione dei bonifici, 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 delle due operazioni.

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 delle operazioni contestate,

non risulta raggiunta la prova che le operazioni contestate siano state eseguite 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 e la chiamata risultava proveniente da un numero di telefono effettivamente riconducibile all'intermediario), rimangono a carico dell'intermediario le operazioni contestate, non essendo stati da questi assolti gli oneri probatori di cui è gravato sia con riguardo alla SCA.
Per tali motivi il Collegio ritiene che l'intermediario debba integralmente rimborsare a parte ricorrente l'importo di € 6.300,00, relativo alle due operazioni contestate.
Con riguardo invece alla domanda di parte ricorrente di rimborso delle spese e competenze, l'intermediario ne eccepisce in via pregiudiziale l'inammissibilità perché non contenuta nel reclamo. Orbene, secondo l'orientamento dei Collegi, ai fini dell'eventuale accoglimento della domanda di rimborso delle spese di assistenza è necessario che**: *a)*** analoga richiesta sia contenuta nel reclamo; *b)* vi sia la prova delle spese sostenute. Nel caso di specie mancando entrambi tali elementi la domanda non può accogliersi (cfr. Collegio di Roma, decisione n. 2491/2023).

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 6.300,00.
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