

COLLEGIO DI MILANO

composto dai signori:

(MI) ACHILLE	Presidente
(MI) TINA	Membro designato dalla Banca d'Italia
(MI) CETRA	Membro designato dalla Banca d'Italia
(MI) SANTARELLI	Membro di designazione rappresentativa degli intermediari
(MI) PERSANO	Membro di designazione rappresentativa dei clienti

Relatore (MI) PERSANO

Seduta del 31/07/2023

FATTO

Nella presente controversia, la parte ricorrente afferma quanto segue:

- ha subito una truffa telefonica in data 12.01.2023 iniziata con un apparente sms inviato dall'intermediario N. in cui veniva comunicata la limitazione dell'operatività del conto;
- ha cliccato il link contenuto nell'sms e si è aperta una pagina web apparentemente riconducibile a quella della banca N. in cui ha inserito i dati di accesso al conto corrente online;
- ha ricevuto una chiamata da un sedicente operatore N. che gli ha preannunciato una seconda chiamata il giorno successivo, a conferma del ripristino della normale operatività;
- il 16.01.2023, non avendo più ricevuto chiamate, ha contattato l'intermediario e si è accorto di essere stato vittima di una truffa;
- i truffatori hanno disposto un bonifico dal proprio conto corrente di € 30.000,00;
- ha presentato denuncia alle Autorità e presentato reclamo alla banca che ha risposto negativamente senza provare l'autenticazione di tutte le fasi del processo;
- il comportamento tenuto dalla banca viola il principio di buona fede del contratto e gli obblighi di trasparenza previsti dal TUB.

Il ricorrente chiede, dunque, all'Arbitro, che venga accertato il proprio diritto ad ottenere il rimborso dell'importo di € 30.000,00, somma che ritiene essergli stata fraudolentemente sottratta.

Nelle proprie controdeduzioni, l'intermediario domanda il rigetto del ricorso, affermando quanto segue:

- il cliente è incorso in colpa grave; infatti, la frode non si sarebbe mai perfezionata qualora lo stesso avesse evitato di comunicare al terzo frodatore le credenziali personali di accesso all'home banking nonché gli OTP necessari per l'attivazione di una nuova licenza "smartOTP";
- l'operazione è stata correttamente contabilizzata, registrata e autenticata in quanto posta in essere con il corretto inserimento delle credenziali;
- l'intermediario ha attivato apposite campagne informative anti-frode, volte a sensibilizzare la clientela rispetto a forme di truffa analoghe a quella perpetrata nella specie;
- al termine di ogni operazione, il sistema della Banca invia all'indirizzo e-mail collegato all'utenza del cliente le relative e-mail di notifica dell'esecuzione delle operazioni, come è avvenuto anche nel caso di specie;
- a seguito della segnalazione del cliente, l'intermediario ha esperito un tentativo di recall del bonifico sconosciuto, che non ha tuttavia avuto esito positivo.

Successivamente, in sede repliche, il cliente, richiamati i propri scritti, replica quanto segue:

- la banca non ha provato l'avvenuta autenticazione a due fattori;
- la banca non ha fornito delucidazioni in merito al fatto che il bonifico è stato effettuato alle ore 18:38, dunque dopo il termine di "cut-off" delle operazioni in giornata e, nonostante questo, è stato eseguito immediatamente.

L'intermediario, per contro, in sede di controrepliche, ribadisce la propria posizione, precisando ulteriormente che:

- ha fornito prova del fatto che il cliente ha comunicato al frodatore gli OTP necessari per l'attivazione di una nuova licenza smartOTP;
- il cliente non ha adeguatamente prestato attenzione al fatto per cui dall'utenza telefonica utilizzata dal presunto truffatore, neppure riconducibile al numero di telefono di una filiale dell'intermediario, rispondeva un presunto operatore della diversa banca N;
- per il resto, l'intermediario ribadisce difese già svolte e insiste per l'accoglimento delle conclusioni in atti.

DIRITTO

La questione sottoposta all'esame del Collegio ha ad oggetto la contestazione di un'operazione di bonifico bancario di importo complessivo pari ad € 30.000,00, effettuata in data 12.01.2023 alle ore 18:38.

A detta data era vigente il D.lgs. 27 gennaio 2010, n. 11 come modificato dal D. Lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU.

In forza di tale disciplina, in caso di contestazione delle operazioni, grava sull'intermediario l'onere di provare, oltre all'insussistenza di malfunzionamenti, l'autenticazione, la corretta registrazione e la contabilizzazione delle operazioni, dovendo in particolare fornire

evidenza di aver applicato un c.d. “Sistema di autenticazione forte” (strong customer authentication o SCA), posto che ai sensi del comma 2-bis dell’art. 12 d. lgs. n. 11/2010, come inserito dal d. lgs. n. 218/2017, *“salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un’autenticazione forte del cliente. Il beneficiario o il prestatore di servizi di pagamento del beneficiario rimborsano il danno finanziario causato al prestatore di servizi di pagamento del pagatore se non accettano l’autenticazione forte del cliente”*. L’intermediario, inoltre, è anche tenuto a 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 (art. 12, co. 2-ter e s., d. lgs. n. 11/2010).

L’intermediario afferma che le operazioni sono state correttamente contabilizzate, registrate e autenticate.

Con riferimento alla strong customer authentication (c.d. SCA) le fonti normative sono rinvenibili negli artt. 97 e 98 della PDS2, nell’art. 10-*bis* del D. Lgs. 10/2011, nelle norme tecniche di regolamentazione emanate dall’EBA e recepite con Regolamento Delegato Ue 2018/389 della Commissione Europea, applicabile a far data dal 14 settembre 2019, nonché nei criteri interpretativi forniti dall’EBA (v. in particolare il parere dell’EBA del 21 giugno 2019). Nello specifico, l’autenticazione forte (SCA) è richiesta sia nella fase di (i) accesso al conto/ enrollment dell’app/registrazione della carta sul wallet, sia nella fase di (ii) esecuzione delle singole operazioni. La SCA 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.

L’intermediario ricostruisce l’operatività fraudolenta affermando che vi sarebbe stata la registrazione di un nuovo dispositivo sull’app, con attivazione del servizio “licenza smart OTP”; successivamente, da tale dispositivo vi sarebbe stato l’accesso all’app e, dunque, l’esecuzione dell’operazione disconosciuta.

Con riferimento alla registrazione del nuovo dispositivo sull’app con attivazione del servizio “smart OTP”, l’intermediario rappresenta che alle ore 06:32 PM (ossia, alle 18:32) del 12/01/2023 è stata attivata una nuova licenza “smartotp” presumibilmente dal terzo frodatore sul proprio dispositivo mobile Android (IP: ****18); il frodatore, per attivare la nuova licenza smartotp, ha dovuto inserire UTENZA + PASSWORD + OTP ricevuto via email + OTP ricevuto via SMS sul cellulare del cliente.

Quanto al processo di enrollment (per attivazione di un nuovo dispositivo), l’intermediario nella legenda prodotta chiarisce che esso prevede sempre l’inserimento di UTENZA + PASSWORD + OTP ricevuto via email + OTP ricevuto via SMS. Specifica, inoltre, che in data 12/01/2023 è stata eseguita l’attivazione di un nuovo device da IP che è lo stesso utilizzato per effettuare l’accesso prima e disporre, poi, le transazioni.

Si rileva, tuttavia, che da quanto in atti, non vi è alcuna evidenza dell’inserimento di Utenza + Password.

Quanto, poi, all’inserimento del primo codice OTP, l’intermediario allega evidenza nella quale è indicato l’invio all’indirizzo email del cliente, in data 12.01.2023 alle ore 18:30, di un “primo codice di attivazione nuovo dispositivo”; al riguardo l’intermediario afferma che trattasi del codice OTP inviato al cliente tramite email; si osserva, ad ogni modo, che

l'evidenza non riporta il testo dell'email con la quale sarebbe stato comunicato il codice OTP.

Quanto all'inserimento del secondo codice OTP, l'intermediario allega evidenza nella quale è indicato l'invio di un presunto "SMS OTP" al cellulare del cliente alle ore 18:31 del 12.01.2023; si osserva ad ogni modo che dall'evidenza non è possibile evincere il contenuto dell'sms che dovrebbe contenere il codice OTP.

Con riferimento alla prova dell'autenticazione forte nella fase di accesso all'app, 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 ****18 che ha attivato la nuova licenza.

Quanto all'accesso all'app, la legenda specifica che, ai fini del login, l'applicazione richiede l'inserimento di Utenza + Password + PIN dispositivo.

Si rileva al riguardo che, dall'esame dei log, non vi è evidenza dell'inserimento di Utenza + Password + PIN dispositivo, che, secondo l'intermediario, sarebbero richiesti a ogni accesso.

Nella legenda è altresì specificato che il PIN può essere inserito anche mediante credenziali biometriche, ma non vi è alcuna evidenza dell'attivazione di forme di riconoscimento biometrico.

Con riferimento alla prova dell'autenticazione forte nella fase di esecuzione del bonifico sconosciuto, nella legenda l'intermediario spiega che la transazione è avvenuta (tramite APP) con inserimento del PIN dispositivo, per autorizzare l'operazione che viene riepilogata mediante notifica.

Tuttavia, dall'esame dei log si rileva non vi è evidenza dell'inserimento dei fattori di autenticazione, malgrado nella legenda l'intermediario rappresenti che per autorizzare l'operazione l'applicazione prevede sempre l'inserimento del PIN dispositivo e di una notifica.

Dalle evidenziate lacune probatorie quanto all'autenticazione, alla corretta registrazione e alla contabilizzazione delle operazioni mediante un c.d. "Sistema di autenticazione forte" consegue che, ad avviso del Collegio, l'intermediario resistente non ha provato di aver adottato gli standard di sicurezza corrispondenti alla disciplina oggi applicabile come sopra individuata, dovendosi altresì ricordare che secondo il disposto dell'art. 10, co. 1, d.lgs. n. 11/2010 *"è onere del prestatore di 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"*.

A tale riguardo e in siffatto contesto, a differenza di quanto accade per la colpa grave dove si deve ammettere la possibilità di ricorrere alle presunzioni, per la SCA la prova non può essere indiziaria o indiretta, ma deve avere ad oggetto specificamente i singoli fattori di autenticazione, dovendo il prestatore di servizi di pagamento offrire puntuale evidenza di quali siano stati quelli in concreto ed effettivamente utilizzati, nonché del completo processo attraverso cui sono stati utilizzati (in questo senso, vd. ABF-Coll.- Milano n. 6881 del 5 luglio 2023 e n. 6933 del 6 luglio 2023).

Ciò premesso, rispetto alla mancanza anche parziale della prova di autenticazione, i Collegi sono unanimi nel ritenere che in tali casi il ricorso venga accolto integralmente, posto che il difetto di tale prova è risolutivo e dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili al cliente. La prova di autenticazione rappresenta infatti, in aderenza al dato normativo, un *prius* logico rispetto alla prova di colpa grave dell'utente.

Questo Collegio ritiene che la documentazione allegata dalla parte resistente non sia esaustiva circa la prova dell'avvenuta autenticazione delle operazioni contestate; da ciò consegue che ogni ulteriore valutazione in merito alla sussistenza o meno della colpa grave in capo al ricorrente è del tutto irrilevante e la domanda restitutoria deve essere accolta.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 30.000,00.

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
DAVIDE ACHILLE