Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MARINARO	Membro designato dalla Banca d'Italia
(RM) PATTI	Membro designato dalla Banca d'Italia
(RM) GENOVESE	Membro di designazione rappresentativa degli intermediari
(RM) SARZANA DI S. IPPOLITO	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - MARCO MARINARO

Seduta del 07/12/2022

Esame del ricorso n. 1065440/2022 del 08/07/2022

proposto da

nei confronti di 1030 -

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MARINARO	Membro designato dalla Banca d'Italia
(RM) PATTI	Membro designato dalla Banca d'Italia
(RM) GENOVESE	Membro di designazione rappresentativa degli intermediari
(RM) SARZANA DI S. IPPOLITO	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - MARCO MARINARO

Seduta del 07/12/2022

FATTO

La parte ricorrente espone quanto segue.

- In data 23.4.2022 ha ricevuto, nella chat ufficiale della banca, un sms che la informava di un accesso anomalo al proprio home banking, invitandola a cliccare su un link per effettuare i dovuti controlli.
- Cliccando sul link, le è apparsa la propria pagina di home banking alla quale accedeva tramite fattore biometrico (senza dunque comunicare alcun codice) e, nel frattempo, riceveva una telefonata da un sedicente operatore dell'intermediario.
- Poco dopo ha scoperto che, dal suo conto, era stata eseguita una ricarica per € 2.500,00 a favore della propria carta prepagata con la quale era stato successivamente perfezionato un acquisto di pari importo.
- La ricorrente ha dunque bloccato il conto e la carta, sporgendo querela.

L'intermediario resiste al ricorso ed eccepisce quanto segue.

- Dalle evidenze informatiche, la transazione contestata è stata autorizzata secondo un sistema multifattoriale senza la rilevazione di alcuna anomalia da parte dei presidi di sicurezza. Per la precisione, in fase di accesso ai servizi di internet banking, è richiesto:

- la digitazione di un codice utente e di una password;
- l'autorizzazione dell'operazione di accesso, previa ricezione della relativa notifica sul cellulare (e che, nel caso di specie, è regolata tramite impronta digitale).

- Nel giorno della truffa sono stati effettuati tre accessi ai servizi di internet banking della cliente. I primi due da uno smartphone riconducibile alla ricorrente e il terzo tramite web da parte del frodatore. Questi ha fruito della collaborazione della cliente, la quale ha autorizzato l'accesso tramite fattore biometrico.
- Durante il terzo accesso, il frodatore ha modificato il PIN on line della carta prepagata e ha eseguito la ricarica di € 2.500,00. Entrambe le operazioni – modifica del codice segreto e ricarica dello strumento di pagamento – sono avvenute sfruttando l'ausilio della cliente che le ha autorizzate tramite fattore biometrico.
- Una volta ricaricata la carta prepagata, il frodatore ha eseguito un acquisto per € 2.500,00 digitando il nuovo PIN on line e il codice OTP inviato con SMS "parlante" sul cellulare della ricorrente.
- Nel caso di specie, dunque, la frode risulta imputabile esclusivamente alla cliente che ha di fatto causato la violazione del sistema multifattoriale di autenticazione predisposto dall'intermediario.
- In conclusione, la ricorrente sembrerebbe essere rimasta vittima di un episodio combinato di smishing e di vishing, modalità fraudolente già note a diverse pronunce dell'ABF.

La ricorrente nelle repliche reitera quanto sostenuto nel ricorso e contesta il valore probatorio delle schermate auto-prodotte e modificabili allegate dall'intermediario.

La banca nelle controrepliche si riporta a quanto controdedotto, precisando che l'orientamento pacifico dell'ABF riconosce valore probatorio alle evidenze informatiche prodotte dagli intermediari.

DIRITTO

1.- L'operazione di pagamento online disconosciuta dalla parte ricorrente è stata eseguita in data 23 aprile 2022. Risulta pertanto effettuata dopo l'emanazione della direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015, (c.d. PSD 2 - Payment Services Directive 2), recepita con il d.lgs. n. 218 del 15.12.2017, entrato in vigore in data 13.01.2018, che modifica in più punti il d.lgs. n. 11 del 2010. Si rileva che tali operazioni sono altresì successive alla data di entrata in vigore del Regolamento Delegato (UE) n. 2018/389 della Commissione.

Sulla base di quanto previsto dalla direttiva (art. 115, par. 4), l'art. 5, comma 6, d.lgs. n. 218/2017 prevede tuttavia che "le misure di sicurezza di cui agli articoli 5-bis, commi 1, 2 e 3, 5-*ter*, 5-*quater* e 10-*bis* del decreto legislativo 27 gennaio 2010, n. 11, si applicano decorsi diciotto mesi dalla data di entrata in vigore delle norme tecniche di regolamentazione di cui all'articolo 98 della direttiva (UE) n. 2015/2366". In particolare, la Commissione – delegata ad adottare tali norme tecniche di regolamentazione, ai sensi dell'art. 98, par. 4, della direttiva – ha emanato il 27.11.2017 il regolamento delegato (UE) n. 2018/389 che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione

forte del cliente e gli standard aperti di comunicazione comuni e sicuri. Il regolamento, ai sensi dell'art. 38, par. 2, si applica a decorrere dal 14.09.2019 e cioè diciotto mesi dopo la pubblicazione sulla Gazzetta Ufficiale dell'Unione Europea, avvenuta in data 13.03.2018. Ne consegue che anche le norme del d.lgs. n. 11/2010 riferite alle misure di sicurezza, così come modificate dal d.lgs. n. 218/2017, hanno efficacia a partire dal 14.09.2019.

Esse risultano dunque applicabili alla vicenda oggetto del ricorso in esame.

2.- In estrema sintesi, la nuova normativa fa ricadere sull'intermediario la responsabilità delle operazioni disconosciute laddove quest'ultimo non abbia predisposto un c.d. "sistema di autenticazione forte" (in inglese *strong customer authentication* o SCA). Un simile sistema deve essere applicato, stando alla previsione dell'art. 10-*bis*, dai prestatori di servizi di pagamento anche quando l'utente dispone un'operazione di pagamento elettronico ovvero effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi. Quanto alla responsabilità del pagatore, 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".

3.- Orbene, il concetto di "autenticazione forte" trova la propria definizione all'art. 1, comma 1, lett. q-*bis*), d.lgs. n. 11/2010 (lettera introdotta dal d.lgs. n. 218/2017): "un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione".

Il concetto è oggi ribadito e precisato, specie per quanto concerne la conformità di singole fattispecie concrete alle suddette categorie dell'autenticazione forte, *dall'Opinion of the European Banking Authority on the elements of strong customer authentication under* PSD2 del 21 giugno 2019.

L'EBA ha chiarito, per esempio, che, mentre l'OTP ricevuta tramite sms integra un elemento di possesso idoneo ai fini della strong customer authentication, i dati riportati sulla carta (numero, scadenza e CVV), non costituiscono né un valido elemento di possesso (par. 28), né un valido elemento di conoscenza (par. 33). Al par. 43 di tale documento si legge, in particolare, che "*a number of existing approaches within e-commerce, for card payments in particular, would not be compliant with SCA. This includes approaches in which card details printed in full on the card are used as stand-alone elements or used in combination with a communication protocol such as EMV® 3-D Secure or with only one compliant SCA element (such as SMS OTP)*".

Alla luce di un simile orientamento, con riguardo alle operazioni successive al 14.09.2019, questo Collegio ritiene che l'inserimento dei dati della carta, al fine di dar corso alle operazioni di pagamento, non integri un idoneo fattore di autenticazione (così, per esempio, Collegio di Roma, decisione n. 8493/2020, decisione n. 15221/2021 e decisione n. 21761/2021).

4.- La parte ricorrente contesta un pagamento online eseguito tramite carta prepagata in data 23.4.2022 per un importo di € 2.500,00.

Dal contenuto del ricorso, il caso di specie sembrerebbe ascrivibile a un episodio di sms spoofing seguito da un attacco di vishing.

Dal contenuto della querela, appare inoltre evincersi la sequenza della truffa: il frodatore ha dapprima eseguito la ricarica della carta prepagata della ricorrente tramite un bonifico dal conto della stessa cliente; ha successivamente eseguito un pagamento on line con la suddetta carta.

La ricorrente allega l'sms civetta che: (i) s'inserisce nella catena dei messaggi genuini provenienti dall'intermediario; (ii) non appare contenere errori grammaticali (salvo il passaggio dalla forma di cortesia "suo" alla forma informale "tu") sebbene il link contenuto nel testo non sembri riconducibile all'intermediario.

Dopo il messaggio civetta risultano inviati in sequenza anche un primo messaggio parlante (genuino) ricevuto dall'intermediario, contenente il codice OTP dispositivo dell'operazione di 2.500,00 euro, seguito da un sms (falso) di avvenuto storno della medesima transazione.

5.- Con riguardo all'autenticazione dell'operazione contestata l'intermediario descrive il presidio SCA e allega evidenza informatica.

Dai log prodotti risulta che per l'autorizzazione delle operazioni è stato adottato il sistema 3DS di tipo dinamico, che prevede per ogni acquisto due fattori di autenticazione:

- il codice di sicurezza unico OTP ricevuto tramite SMS, da inserire al momento del pagamento;

- a tale codice si aggiunge un ulteriore fattore di autenticazione, rappresentato dal c.d. Pinonline (nel caso di specie precedentemente modificato dal truffatore), o da un sistema di riconoscimento biometrico (impronta digitale o riconoscimento facciale).

Si fa presente che non consta in atti l'evidenza dell'invio dell'OTP inviato al numero di telefono della ricorrente. Tuttavia, quest'ultima ha prodotto l'SMS "parlante" ricevuto sul suo cellulare, contenente la password OTP necessaria ad autorizzare l'operazione di pagamento.

In ordine alla conformità o meno di tale procedura di autenticazione ai requisiti della SCA, si rileva che secondo l'Opinion EBA del 21 giugno 2019 il codice OTP inviato tramite sms ovvero generato tramite token o push notification rientra nella categoria "possesso", mentre il codice PIN rientra nella categoria "conoscenza".

Tale modalità autorizzativa è stata ritenuta compliant alla SCA da altro Collegio ABF (Coll. Bologna, dec. n. 12607/2022).

6.- All'esito dell'esame istruttorio, ad avviso del Collegio nel caso di specie la parte ricorrente deve ritenersi essere rimasta vittima di una fattispecie delittuosa riconducibile al c.d. "sms spoofing".

Secondo l'orientamento condiviso fra i Collegi ABF, nelle fattispecie di spoofing non è generalmente ravvisabile la colpa grave del ricorrente, "a meno che non si rinvengano […] indici di inattendibilità o anomalia del messaggio; in tale caso, potrà essere ravvisato un concorso di colpa tra le parti in relazione, da un lato, alla negligenza grave dell'utente che agevola il compimento della truffa, similmente a quanto avviene negli episodi di phishing e, dall'altro lato, alle criticità organizzative del servizio di pagamento offerto dall'intermediario".

Pertanto, non sussistendo indici di inattendibilità o anomalie del messaggio tali da consentire di ritenere che cliente abbia tenuto una condotta gravemente colposa, la domanda restitutoria deve essere integralmente accolta.

PER QUESTI MOTIVI

Il Collegio dispone che l'intermediario corrisponda alla parte ricorrente la somma di euro 2.500,00.
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

Firmato digitalmente da
PIETRO SIRENA