COLLEGIO DI BOLOGNA

composto dai signori:

(BO) MARINARI	Presidente
(BO) MAIMERI	Membro designato dalla Banca d'Italia
(BO) BULLO	Membro designato dalla Banca d'Italia
(BO) CORRADI	Membro di designazione rappresentativa degli intermediari
(BO) PETRELLI	Membro di designazione rappresentativa dei clienti

Relatore PATRIZIA PETRELLI

Seduta del 11/06/2024

FATTO

Con ricorso depositato in data 22 gennaio 2024 parte ricorrente riferisce che: in data 05/10/2022 riceveva una telefonata da un numero di telefono mobile e interloquiva con un sedicente operatore dell'intermediario il quale lo informava che la sua carta era stata bloccata a seguito di un'operazione illecita proveniente da Lugano; durante la telefonata, il sedicente operatore dimostrava di conoscere una serie di dati del ricorrente quali nome, cognome, residenza, numero di telefono, data e natura di transazioni recenti realmente effettuate dal ricorrente, dati che venivano riferiti dal sedicente operatore dell'intermediario e confermati dal ricorrente; riceveva un sms con cui gli veniva richiesto di disconoscere l'operazione sospetta e una chiamata durante la quale, al fine di procedere al disconoscimento, gli venivano richiesti il cvv della carta e di effettuare il passaggio del conto corrente dal tipo standard al tipo smart; il sedicente operatore chiedeva di disinstallare l'app e reinstallarla per riattivare la carta e di cancellare tutti i messaggi provenienti dall'intermediario; terminata la telefonata, si rendeva conto di essere rimasto vittima di una truffa e procedeva a sporgere querela e a presentare reclamo; l'intermediario resistente procedeva al rimborso di alcune operazioni per l'importo di 1.000,00 euro, ma respingeva l'ulteriore richiesta di rimborso per 7.200,00 euro; non ha ricevuto alcun messaggio "*Alert*", né alcun codice OTP; le operazioni contestate non sono state autorizzate tramite autenticazione forte.

Pertanto si rivolge a questo Arbitro chiedendo il rimborso della somma pari a 7.200,00 euro, corrispondente all'importo delle operazioni disconosciute.

Costituendosi del procedimento, l'intermediario evidenzia che: in seguito al reclamo, ha rimborsato due transazioni per il valore complessivo di 1.000,00 euro in quanto solo tali operazioni non risultavano essere autenticate; non risulta allegata al ricorso alcuna evidenza del sms con cui veniva richiesto al ricorrente di disconoscere l'operazione contestata; durante la telefonata è stato chiesto al ricorrente: i) di attivare tramite *ebanking* l'opzione premium ***smart; ii) di richiedere una carta aggiuntiva virtuale, strumento incluso nei vantaggi connessi all'opzione premium, iii) di confermare una serie di transazioni al fine di mettere in sicurezza sulla nuova carta le somme disponibili; il ricorrente ha dato seguito alle richieste del truffatore, come ha ammesso nella live-chat con il servizio clienti; le transazioni sono state autorizzate dal cliente stesso tramite SCA; il ricorrente versa in colpa grave in quanto ha assecondato le richieste che gli venivano rivolte dai truffatori; il ricorrente ha ricevuto una notifica push per ciascuna delle operazioni da autorizzare e le notifiche push ricevute indicavano chiaramente le operazioni che sarebbero state autorizzate; il dispositivo da cui è stata autorizzata l'operazione è riconducibile al ricorrente in quanto lo user id associato al mobile token non è mai stato variato dopo la prima associazione, avvenuta in data 26/05/2022; il ricorrente non ha mai denunciato il furto o lo smarrimento del proprio smartphone; le operazioni di pagamento non sono state disposte attraverso alcuna intrusione all'interno del conto corrente del ricorrente; il frodatore - già in possesso dei dati della carta di debito - predisponeva autonomamente le operazioni e induceva il ricorrente ad autorizzarle dall'area riservata del suo *eBanking*; le operazioni contestate sono state direttamente autorizzate dal ricorrente e pertanto non trova applicazione la disciplina di cui al D.lgs 11/2010.

Conclude, pertanto, chiedendo il rigetto del ricorso.

In sede di repliche le parti insistono nelle rispettive posizioni.

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.

A fronte del disconoscimento delle operazioni di pagamento da parte dell'utente, incombe sul prestatore di servizi di pagamento l'onere di provare che l'operazione è stata autenticata, correttamente registrata e contabilizzata ai sensi dell'art. 10, comma 1, del D. lgs. 11/2010, che così statuisce: "Qualora l'utilizzatore di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, 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".

Con riguardo alla modalità di autenticazione delle operazioni, l'art. 10-bis del medesimo D. lgs. n. 11/2010 prevede: "Conformemente all'articolo 98 della direttiva (UE) 2015/2366 e alle relative norme tecniche di regolamentazione adottate dalla Commissione europea, i prestatori di servizi di pagamento applicano l'autenticazione forte del cliente quando l'utente: a) accede al suo conto di pagamento on-line; b) dispone un'operazione di pagamento elettronico; c) effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi".

L'art. 1, lettera q-bis del medesimo decreto chiarisce, conformemente alla suddetta direttiva, che la c.d. autenticazione forte consiste in "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".

Sul punto, è intervenuta l'EBA con la "Opinion" del 21 giugno 2019 (richiamata espressamente dal Regolamento UE/2018/389 del 27/11/2017) con cui ha precisato, ai fini dell'implementazione del suddetto Regolamento, quali elementi costituiscano o meno, allo stato attuale della tecnologia, fattori di autenticazione forte all'interno delle categorie della conoscenza, del possesso e dell'inerenza.

Così brevemente riassunto il quadro normativo, occorre verificare se nella specie l'intermediario abbia fornito elementi in sostegno della legittimità delle operazioni contestate.

Il ricorrente disconosce cinque transazioni online per complessive 7.200,00 euro disposte in data 5/10/2022 dalle ore 12:43 alle ore 12:52, corrispondente a quanto richiesto in restituzione.

A tali operazioni si aggiungono altre due operazioni online per complessive 1.000,00 euro già rimborsate dall'intermediario successivamente alla presentazione del reclamo in quanto non dotate di autenticazione forte.

L'intermediario ha dedotto che le operazioni contestate sono state effettuate dal dispositivo del ricorrente associato all'home banking fin dal 26/05/2022.

L'intermediario ritiene che le evidenze dallo stesso prodotte dimostrerebbero che il dispositivo associato all'home banking è sempre stato quello del ricorrente.

In particolare eccepisce che le operazioni contestate sono state direttamente autorizzate dal ricorrente e pertanto non troverebbe applicazione la disciplina di cui al D.lgs. n. 11/2010; ciò, a dire dell'intermediario, si desumerebbe dalla circostanza che il dispositivo associato all'home banking è sempre stato il medesimo e che il ricorrente non ha mai denunciato il furto o lo smarrimento del medesimo.

In effetti alcune di dette operazioni sarebbero state effettuate integralmente dal ricorrente e altre autorizzate dal ricorrente ma dopo essere state predisposte dai truffatori.

Il Collegio, in aderenza al proprio orientamento, ritiene al riguardo che debba applicarsi la disciplina prevista dal D. lgs n. 10/2011, in casi di operazioni disposte dal truffatore e autorizzate dal ricorrente (v. Collegio di Bologna, decisione n. 2265/2023).

L'intermediario descrive i passaggi attraverso i quali si sono realizzate le operazioni fraudolente, producendo la relativa documentazione.

A riprova dell'accesso all'app, l'intermediario fornisce evidenza corredata da relativo

glossario.

Si osserva che nella colonna “process” compare la dicitura “MFA OSC”, che stando al glossario denoterebbe (genericamente) l’utilizzo di un secondo fattore di autenticazione.

Va tuttavia evidenziato che nella colonna “device token” compare la stessa stringa riportata in altro allegato prodotto e pertanto l’accesso parrebbe essere stato effettuato dal device del ricorrente.

Per quanto riguarda l’attivazione dell’opzione smart e della carta virtuale, parte resistente produce ulteriore evidenza.

Tuttavia da tale documento non si evince quale ulteriore fattore di autenticazione sia stato utilizzato, oltre all’elemento di possesso.

Anche con riferimento all’attivazione dell’opzione smart e della carta virtuale, va evidenziato che nella colonna “*device token*” compare la stessa stringa riportata nell’allegato sopra indicato e che pertanto l’accesso parrebbe essere stato effettuato dal *device* del ricorrente.

Con riguardo all’esecuzione delle operazioni di pagamento, l’intermediario produce evidenze relative alle notifiche push inviate al ricorrente per le operazioni contestate nonchè i log relativi all’inoltro delle suddette notifiche push,

L’intermediario produce poi, per ciascuna delle operazioni contestate, una tabella, fornendo la spiegazione di tali evidenze.

Tuttavia non risulta quali stringhe dimostrerebbero l’utilizzo del fattore di inerenza.

Pertanto nel caso di specie la documentazione fornita dall’intermediario non consente di ritenere sufficientemente protettivi per il cliente i presidi di sicurezza predisposti, in quanto non risulta che le operazioni contestate siano state autenticate mediante la combinazione di almeno due dei tre elementi che caratterizzano la c.d. “autenticazione forte”.

In particolare, il Collegio ritiene che l’intermediario non ha fornito evidenze informatiche o contabili certe che, nel caso concreto, i presidi di sicurezza, conformi ai parametri SCA, siano stati applicati alle operazioni disconosciute.

Secondo l’orientamento dei Collegi ABF (v. *ex multis* Collegio di Bologna, decisione n. 597/2022 e n. 18571/2021), l’intermediario deve fornire la prova di aver adottato una procedura di autenticazione forte tanto nella fase di installazione dell’app e accesso all’home banking quanto nel momento dell’esecuzione delle operazioni.

Tanto premesso, il Collegio ritiene che, nel caso di specie, l’intermediario non abbia fornito la prova della regolarità formale delle operazioni, sotto il profilo della “autenticazione forte del cliente”, ai sensi della richiamata disciplina.

Al riguardo, mette conto evidenziare la “Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2” del 21/06/2019, nella quale l’Autorità Bancaria Europea ha preso in considerazione specifici esempi di soluzioni tecniche e chiarito quali elementi possono considerarsi conformi a ciascuna delle tre categorie (inerenza, possesso e conoscenza), che rilevano ai fini della sussistenza di una autenticazione forte.

In base al quadro normativo sopra delineato, così come corredato dagli interventi dell’EBA, non può che confermarsi che spetta all’intermediario la prova dell’intervenuta autenticazione forte delle operazioni di pagamento.

In merito alla prova della corretta autenticazione ed esecuzione delle operazioni di

pagamento si osserva che i Collegi territoriali ABF hanno condiviso l'orientamento per cui nel caso in cui l'intermediario non abbia assolto all'onere probatorio sull'autenticazione delle operazioni di pagamento contestate dal cliente, di cui all'art. 10, comma 1 del D.lgs. 11/2010, [...] il ricorso venga accolto, posto che la mancanza anche parziale della prova di autenticazione è risolutiva 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 della colpa grave dell'utente.

Secondo l'orientamento consolidato dei Collegi ABF in caso di mancata produzione di documentazione idonea a dimostrare la corretta e regolare autenticazione delle transazioni contestate, l'intermediario è tenuto al rimborso integrale delle somme, senza applicazione della franchigia (cfr. Collegio di Milano, decisione n. 20530/20; Collegio di Bologna n. 18713/21; Collegio di Torino n. 3464/2018).

Alla luce di tali considerazioni, che assorbono, altresì, ogni valutazione sul contegno della ricorrente nella dinamica della frode, merita accoglimento la domanda proposta con conseguente diritto alla restituzione della somma di 7.200,00 euro.

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 7.200,00 (settemiladuecento/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
MARCELLO MARINARI