COLLEGIO DI BOLOGNA

composto dai signori:

(BO) MARINARI	Presidente
(BO) BERTI ARNOALDI VELI	Membro designato dalla Banca d'Italia
(BO) LOMBARDI	Membro designato dalla Banca d'Italia
(BO) PASQUARIELLO	Membro di designazione rappresentativa degli intermediari
(BO) PETRELLI	Membro di designazione rappresentativa dei clienti

Relatore PATRIZIA PETRELLI

Seduta del 08/11/2022

FATTO

Con ricorso depositato in data 20 maggio 2022 parte ricorrente riferisce che: in data 7.4.2022 riceveva un SMS proveniente da numero riconducibile al servizio clienti dell'intermediario; il messaggio l'avvisava di un dispositivo sconosciuto collegato al suo conto corrente; il messaggio conteneva un link, da dove si accedeva alla pagina web presumibilmente dell'intermediario, ove si invitava a prenotare una telefonata da un operatore; riceveva la telefonata prenotata dallo stesso numero dell'intermediario di cui all'SMS, nella quale veniva riferito che occorreva installare una nuova App e disinstallare quella originaria dell'intermediario; successivamente riceveva gli SMS alert relativi all'avvenuta effettuazione di due bonifici rispettivamente di 9.500,00 euro e 49.550,00 euro che riusciva tempestivamente a bloccare telefonando alla banca; non riusciva però a bloccare un bonifico di 21.301,00 euro, in relazione al quale non era pervenuto alcun SMS alert; l'intermediario è responsabile della sottrazione dei fondi, in quanto la ricorrente non ha fornito alcun codice di sicurezza agli ignoti frodatori e non è stato ricevuto l'SMS alert.

Pertanto si rivolge a questo Arbitro chiedendo il rimborso della somma pari a 21.301,00

euro corrispondente all'importo dell'operazione disconosciuta.

Costituendosi del procedimento l'intermediario evidenzia che le operazioni sono state regolarmente autenticate ed autorizzate nelle modalità prevista dai propri sistemi di sicurezza, con utilizzo della password statica di accesso al sito istituzionale ed attivazione dell'App installata sul cellulare certificato della ricorrente, conformemente agli attuali standard tecnologici per i pagamenti a distanza; il funzionamento del sistema di autenticazione dell'intermediario prevede per l'accesso l'accreditamento mediante l'inserimento del numero cliente, del PIN e dell'OTP che si attiva internamente all'App scaricata sul dispositivo abilitato del cliente ed entra in funzione con l'intervento dell'utente, che inserisce il PIN o il touchID o il faceID in una notifica che gli compare sul dispositivo; una volta effettuato l'accesso, per le operazioni dispositive l'autenticazione avviene con il riconoscimento dell'OTP generato come al punto precedente; il cliente può attivare il sistema contemporaneamente su fino a due dispositivi; alle ore 11:09 del 7/4/2022 è stato attivato il Mobile token su un nuovo dispositivo, come da SMS inviato all'utenza della ricorrente, che evidentemente ha ignorato; per l'*enrollment* di un nuovo dispositivo sono necessari tra l'altro il codice titolare, il PIN ed il codice di attivazione inviato via SMS sull'utenza abilitata; la ricorrente afferma di aver digitato su un link truffaldino e, anche se non lo ammette espressamente, è verosimile che abbia comunicato il PIN ed il codice di attivazione ricevuto via SMS; la ricorrente è inoltre colpevole di aver installato un'App estranea alla banca sul proprio cellulare su indicazione dei malviventi; la ricorrente, nonostante l'SMS relativo all'*enrollment* di un nuovo dispositivo, ha chiamato la banca solo il giorno successivo, per cui è stato possibile bloccare solo i bonifici richiesti nel giorno, ma non quello effettuato il giorno precedente; la ricorrente è inadempiente rispetto agli obblighi di prudente custodia delle credenziali di accesso e utilizzo del proprio Home Banking; il bonifico controverso è stato correttamente autenticato, registrato e contabilizzato ai sensi del Dlgs 11/10 e nessuna anomalia o malfunzionamento dei sistemi è rilevabile; la ricorrente è stata vittima di un tipico fenomeno di *phishing*;

Pertanto conclude chiedendo il rigetto del ricorso.

In sede di repliche parte ricorrente si richiama a quanto già esposto, così come l'intermediario si richiama alle proprie controdeduzioni ed insiste nelle proprie richieste.

DIRITTO

L'operazione contestata è stata posta 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.

L'operazione disconosciuta e di cui si chiede il rimborso consiste in un bonifico ordinario dell'importo di 21.301,00richiesto alle ore 11:14 del 7/4/2022 tramite Home Banking.

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 l'operazione contestata sia stata autenticata mediante la combinazione di almeno due dei tre elementi che caratterizzano la c.d. "autenticazione forte".

Per l'autenticazione dell'operazione di pagamento contestata l'intermediario afferma di ricorrere ad una tecnologia multifattoriale.

Nel caso di specie l'intermediario afferma che è stato attivato il Mobile Token in data 7.4.2022 alle ore 11:09 mediante inserimento di Pin e utilizzando l'OTP ricevuto via SMS, da indirizzo IP 5.91.187.143

L'intermediario descrive il processo di attivazione del mobile token precisando che sono necessari i seguenti passaggi: scaricare l'app che si trova su Play Store e App Store; aprire l'app; inserire il Numero Cliente e PIN (che conosce soltanto il cliente); attivare token (secondo la procedura guidata); scegliere un nickname; digitare il codice di attivazione (inviato al cliente tramite SMS).

In particolare l'intermediario non fornisce la documentazione relativa alla fase dell'attivazione del mobile Token sul device del truffatore.

Di tale attivazione l'Istituto offre solo un'evidenza meramente descrittiva.

Tutto quanto considerato, questo Collegio evidenzia che non constano agli atti ulteriori tracciature informatiche attestanti le modalità con cui è avvenuta l'istallazione dell'app.

Secondo l'orientamento dei Collegi ABF (cfr. Collegio di Coordinamento, decisione n. 21285/21 nonché *ex multis* Collegio di Bologna, decisioni 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.

Da quanto sopra esposto consegue che l'intermediario non ha fornito evidenze informatiche o contabili certe che, nel caso concreto, simili presidi di sicurezza, conformi ai parametri SCA, siano stati applicati all'operazione disconosciuta.

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 della transazione contestata, 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 del ricorrente nella dinamica della frode, merita accoglimento la domanda proposta con conseguente diritto alla restituzione della somma complessiva di 21.301,00 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 21.301,00 (ventunomilatrecentouno/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