COLLEGIO DI BOLOGNA

composto dai signori:

(BO) TENELLA SILLANI	Presidente
(BO) VELLA	Membro designato dalla Banca d'Italia
(BO) LEMME	Membro designato dalla Banca d'Italia
(BO) IELASI	Membro di designazione rappresentativa degli intermediari
(BO) PETRELLI	Membro di designazione rappresentativa dei clienti

Relatore FRANCESCO VELLA

Seduta del 25/02/2025

FATTO

Il ricorrente, premesso di essere titolare di conto corrente acceso presso la resistente, come di seguito ricostruisce i fatti accaduti.

In data 08.01.2024 riceveva una chiamata sul suo cellulare da parte del numero 800**, che verificava appartenere alla sua banca online. Tuttavia un falso operatore bancario, a conoscenza di tutti i suoi dati, gli riferiva che vi erano alcuni tentativi di accesso al suo home banking e un tentativo di bonifico per €10.000,00. Lo induceva quindi a comunicare il codice ricevuto via sms al dichiarato fine di bloccare un bonifico estero, asseritamente falso. Dopo circa un'ora di conversazione telefonica, la chiamata si interrompeva. Subito dopo, controllando l'home banking, notava l'esecuzione proprio di un bonifico di € 10.000,00 in favore di un soggetto sconosciuto; notava inoltre che erano state tentate altre operazioni su siti esteri tramite la sua carta, non andate a buon fine. Realizzava di essere stato vittima di una truffa e provvedeva a bloccare le carte di pagamento. Lamenta che la banca non ha stornato l'operazione, contestata solo pochi minuti dopo il perfezionamento, e non lo ha informato sui rischi del vishing. Eccepisce inoltre di non aver sottoscritto alcun contratto di internet banking. Conclude che la resistente ha consentito l'operazione senza l'utilizzo di due fattori forti poiché ha fornito solo l'otp e non gli altri codici di accesso, evidentemente già in possesso dei malviventi. Precisa di avere, il 09.01.2024, sporto denuncia e successivamente inoltrato reclamo alla resistente, ricevendo riscontro negativo.

Parte ricorrente chiede il rimborso di € 10.000,00.

L'Intermediario resistente precisa in primo luogo che tutte le operazioni disconosciute sono state correttamente autorizzate mediante l'utilizzo di credenziali statiche e dinamiche in possesso esclusivo del cliente, posto che per poter eseguire l'accesso all'area riservata (da sito o da app) è necessario inserire le credenziali statiche (username e password); da app inoltre è possibile accedere col meccanismo di sblocco biometrico delle smartphone, che deve essere attivato previo accesso all'area riservata e inserimento di apposita otp. Sul punto, osserva che ai sensi dell'art. 10 del Regolamento Delegato UE 2018/389 è richiesta l'autenticazione forte la prima volta che il cliente accede all'area, oppure successivamente, qualora siano trascorsi più di 180 giorni dall'ultima volta che il cliente ha avuto accesso con SCA; in caso di accesso senza autenticazione forte, l'accesso è limitato alle informazioni sul saldo del conto e sulle operazioni di pagamento eseguite negli ultimi 90 giorni. Il bonifico inserito dopo il login, viene confermato mediante opt ricevuta sul cellulare. In questo caso l'accesso all'area riservata rappresenta il primo fattore (fattore di conoscenza) e la OTP il secondo fattore (fattore di possesso) ai fini del rispetto dell'autenticazione forte.

Nel caso di specie l'accesso all'area riservata è avvenuto alle 18:04:13 dall'abituale dispositivo del ricorrente mediante riconoscimento biometrico, precedentemente attivato in data 15.10.2023; successivamente, tra le 18:04 e le 18:06, sono stati registrati dal medesimo indirizzo IP la generazione di un CVV dinamico della carta e due consultazioni del pin della carta con autenticazione forte (riconoscimento biometrico e autorizzazione mediante token precedentemente attivato in data 15.10.2023). Il giorno della frode il ricorrente operava quindi personalmente nella propria area personale e condivideva i propri dati bancari con terzi sconosciuti. Solo alle 18:07 si è registrato un accesso da IP differente, con il quale veniva avviata la procedura di reset della password. Tuttavia, alle 18:07:34 il cliente eseguiva una nuova consultazione del pin della carta, di conseguenza l'accesso da IP differente con username e password e il bonifico delle 18:09 facevano attivare un blocco automatico dell'area personale grazie al motore antifrode. Nonostante ciò, il ricorrente alle 18:10 effettuava un nuovo accesso così comportando lo sblocco del conto posto dal motore antifrode; in quel momento permetteva nuovamente un cambio password al truffatore e alle 18:14 veniva eseguito il bonifico di € 10.000,00 nel rispetto del sistema di autenticazione forte.

Precisa ancora che l'otp ricevuta dal cliente e comunicata al truffatore era all'interno di un messaggio dal testo chiaro "xxx***: Per eseguire il bonifico di 10.000 EUR al conto di destinazione IT***, usa il codice 4**"; sono state effettuate diverse generazioni di CVV dinamici per l'esecuzione di pagamenti online, che tuttavia venivano bloccati; il precedente accesso da area personale con username, password e otp ricevuta tramite sms era avvenuto in data 06.10.2023, di conseguenza non ha applicato l'autenticazione forte all'accesso avvenuto il giorno della frode; le due procedure di cambio password autorizzate tramite otp rappresentano nuovi accessi con autenticazione forte a doppio fattore.

Conclude che il ricorrente è stato vittima di vishing e con colpa grave ha dato seguito alla telefonata del sedicente operatore, posto che è ormai fatto notorio che i "numero verde" sono abilitati sono a ricevere e non a effettuare chiamate e tale circostanza avrebbe dovuto insospettire il cliente che, con una media diligenza, avrebbe potuto porre fine alla telefonata.

Non si tratta dunque di una truffa sofisticata ed è evidente la colpa grave del ricorrente, che ha continuato la telefonata per oltre un'ora e ha fornito tutti i codici OTP nonostante il

testo degli sms fosse molto chiaro.

Parte resistente chiede il rigetto del ricorso.

DIRITTO

Con il presente ricorso il ricorrente chiede la restituzione dell'importo di un bonifico eseguito in data 8.01.2024, tramite home banking, per un importo di € 10.00,00, in quanto operazione da lui non autorizzata.

Il Collegio precisa in primo luogo che l'operazione contestata è disciplinata dal d.lgs. 27 gennaio 2010, n. 11, modificato a seguito dell'entrata in vigore (il 13/01/2018) del d.lgs. 15 dicembre 2017, n. 218, di recepimento della direttiva (UE) 2015/2366 (c.d. PSD2) relativa ai servizi di pagamento nel mercato interno, nonché adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta.

L'art. 12 del d. lgs. n. 11/2010 regola il regime della responsabilità a fronte dell'utilizzo non autorizzato di strumenti e servizi di pagamento. La disposizione, con un evidente favor nei confronti dell'utilizzatore, opera uno spostamento della responsabilità in capo al prestatore dei servizi di pagamento in caso di utilizzo fraudolento, estendendola a tutte le ipotesi di violazione degli obblighi di custodia e sicurezza non caratterizzate da frode, dolo o colpa grave. Ne consegue che, nel caso in esame, al fine di escludere la responsabilità della parte ricorrente, è necessario escludere che il suo comportamento possa configurarsi quale colpa grave. Sul punto deve essere richiamato l'art. 7, comma 3 del d. lgs. n. 11/2010, in base al quale l'utente "adotta tutte le ragionevoli misure idonee a proteggere le credenziali di sicurezza personalizzate".

Tuttavia, ai sensi del 1° comma dell'art. 10 del d. lgs. n. 11/2010, nel caso di un'operazione di pagamento disconosciuta, il prestatore del servizio è tenuto a "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".

Deve ancora richiamarsi l'art. 10 bis, comma 1, del d. lgs. n. 11/2010, il quale, recependo l'art. 98 della direttiva UE 2015/2399, sancisce l'obbligo per i prestatori di servizi di pagamento di applicare "l'autenticazione forte del cliente" nei casi in cui questi acceda al proprio conto di pagamento on line, effettui un'operazione o "qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi".

L'operazione contestata, in base alla documentazione prodotta ed alla ricostruzione effettuata dalle parti, è stata possibile attraverso diversi passaggi.

L'intermediario descrive i passaggi autorizzativi nel seguente modo e li correda di relativa documentazione unita alla legenda esplicativa: per l'accesso all'area riservata, ai sensi dell'art. 10 del Regolamento Delegato (UE) 2018/839, è sempre richiesta l'autenticazione forte mediante OTP, trasmessa via SMS all'utenza mobile indicata dal cliente in fase di apertura del rapporto e validata dalla banca, nei casi di (a) primo accesso e (b) qualora siano trascorsi più di 90 giorni dall'ultima volta che il cliente ha avuto accesso al conto corrente mediante autenticazione forte. Quindi, nella prima sessione di login è avvenuta la procedura di reset della password e successivamente è stato effettuato un nuovo login con nuovo reset password a seguito dell'intervenuto blocco ad opera dell'intermediario.

Per la disposizione del bonifico, è richiesto l'inserimento di un otp inviato al device del ricorrente.

Dalla documentazione in atti emerge dunque che il primo accesso nel giorno della frode (08.01.2024) è stato effettuato dal ricorrente alle 18:04, dal suo abituale device e mediante solo riconoscimento biometrico; in tale occasione è stato generato un cvv dinamico e sono state effettuate due consultazioni del pin della carta; successivamente, è avvenuto il primo collegamento (18:07) di accesso all'area riservata tramite username e password personali da una città differente, con successivo reset della password tramite inserimento di username, due cifre del PIN della carta di debito e OTP inviata via SMS. Poiché è stato effettuato un nuovo accesso alle 18:07:3, in cui è consultato il pin della carta, è avvenuto un blocco automatico da parte dell'intermediario tramite motore antifrode. In seguito il ricorrente ha effettuato un ulteriore accesso all'area riservata con riconoscimento biometrico e ha così sbloccato il conto. A seguito di nuovo reset della password, è stato effettuato un nuovo accesso con inserimento di username e password scelta dal truffatore e senza il secondo fattore di autenticazione ai sensi dell'esenzione di cui all'art.10 del Regolamento delegato. Alle 18:14 è stato eseguito il bonifico disconosciuto di € 10.000,00 mediante otp inviato con sms all'utenza mobile del ricorrente (333**16) che li ha comunicati al truffatore.

Dai log prodotti, si evince l'utilizzo del fattore di conoscenza (i.e. la password), come risulta dal valore "Autentication con usuario y password personales" in corrispondenza della voce "Medio de autentificacion". In merito al secondo fattore di autenticazione, l'intermediario riferisce di essersi avvalso dell'esenzione dalla SCA prevista dall'art. 10 Reg. UE 2018/389 e quindi di non aver richiesto l'autenticazione forte mediante OTP, trasmessa via SMS all'utenza mobile indicata dal cliente in fase di apertura del rapporto.

Il Collegio rileva che secondo l'"Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2" del 21 giugno 2019, un'app o un web browser possono costituire una prova di possesso, a condizione che includano un processo di associazione del dispositivo che garantisca una connessione unica tra l'app del PSU, browser o chiave e il dispositivo. Ciò può avvenire, ad esempio, tramite crittografia hardware, web-browser e registrazione di dispositivi mobili o chiavi memorizzate nell'area sicura di un dispositivo. Al contrario, un'app o un web browser che non garantisce una connessione unica con un dispositivo non costituisce un elemento di possesso conforme. Inoltre, in merito alle esenzioni SCA previste dal Reg. Delegato 389/2018, l'EBA ha chiarito che, qualora l'intermediario decida di non adottare l'autenticazione forte, applicando un'esenzione dalla SCA normativamente prevista, nel caso in cui le operazioni siano state disconosciute dal cliente, resta ferma la sua responsabilità (fatta salva la frode dell'utilizzatore) (cfr. EBA Q&A 2018-4042).

Ciò posto, precisato inoltre che, come da orientamento già espresso, l'art. 10 del Regolamento Delegato dispone "sì l'esenzione per la SCA, ma solo ed esclusivamente per l'accesso al conto a fini informativi, non certo anche per quell'accesso che avvenga al fine dell'esecuzione di disposizioni di pagamento" (Cfr. Collegio di Bologna, decisione 9591/2024 ed in tal senso, implicitamente, Collegio di Bari, decisione n. 6380/2024), non avendo parte resistente assolto all'onere della prova su di essa gravante della corretta autenticazione a doppio fattore di tutti passaggi necessari al compimento della truffa, come previsto dai richiamati artt. 10 e 10 bis d. lgs. n. 11/2010, questa è tenuta al rimborso dell'intera somma fraudolentemente sottratta.

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 10.000,00 (diecimila/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
CHIARA TENELLA SILLANI