COLLEGIO DI BOLOGNA

composto dai signori:

(BO) MARINARI	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) CAPILLI	Membro di designazione rappresentativa dei clienti

Relatore FRANCESCO VELLA

Seduta del 08/10/2024

FATTO

In merito ai fatti accaduti, nel caso in esame dal ricorso e dalla denuncia in atti emerge che il 06/02/2024 il ricorrente ha ricevuto una chiamata da un numero apparentemente riconducibile alla banca e, su richiesta del sedicente operatore, ha comunicato il codice fiscale. Terminate le verifiche si è collegato alla home banking e ha notato due operazioni di € 1,00 ed € 2.850,00.

Disconosciute le operazioni senza esito, si rivolge all'ABF al quale chiede di riconoscere il suo diritto al rimborso di € 2.850,00.

Parte resistente in via preliminare illustra che, in generale, l'accesso al conto di pagamento avviene mediante inserimento di username e password, unitamente al codice OTP in caso di primo accesso e qualora siano trascorsi più di 180 giorni dall'ultimo accesso); in caso di accesso senza autenticazione forte, l'accesso del cliente è limitato alle seguenti informazioni: saldo del conto e operazioni di pagamento eseguite negli ultimi 90 giorni.

Dichiara quindi che, nel caso in esame, le operazioni sono state effettuate mediante un sistema di autenticazione forte, posto che il primo accesso al conto corrente è avvenuto mediante modifica della password e la password è stata modificata inserendo il nome

utente, due cifre del pin della carta (che può essere visualizzato solo all'interno dell'area riservata) scelte randomicamente dal sistema, e di una OTP inviata sul numero di cellulare del cliente univocamente associato all'area riservata.

Precisa che, se il cliente non ricorda il proprio nome utente, può inserire il suo codice fiscale sul sito web della banca oppure in app per ricevere lo username via SMS al telefono univocamente associato al conto corrente. Infatti, nel caso di specie il ricorrente ammette di avere comunicato il proprio codice fiscale al terzo, necessario a generare l'invio via SMS dello username di accesso all'area riservata. A conferma di quanto esposto, il ricorrente ha ricevuto il proprio username via SMS al proprio numero di telefono alle ore 18:52:43.

Successivamente alla modifica della password, i terzi accedevano all'area riservata e provvedevano anzitutto a visualizzare il PIN della carta di debito mediante inserimento di specifica OTP inviata al numero di telefono del ricorrente. Inoltre, i truffatori aumentavano il limite massimo giornaliero di spesa con carta all'importo massimo consentito a sistema (ossia 3.000,00 Euro), mediante inserimento di OTP inviata al numero validato dal ricorrente.

Per quanto riguarda l'operazione di pagamento, dichiara che è stata disposta con carta con le seguenti credenziali: a) inserimento nel POS virtuale utilizzato per l'esecuzione dell'operazione delle credenziali statiche (PAN e data di scadenza) della Carta, consultabili esclusivamente all'interno dell'area riservata della banca accessibile secondo le modalità sopra illustrate; b) inserimento del CVV della carta (come primo fattore di autenticazione). A tale fine, il CVV della carta non è stampato sulla carta come ordinariamente avviene, ma è generabile esclusivamente nell'area riservata previo accesso e inserimento di una OTP inviata all'utenza mobile validata dal cliente. Il CVV è inoltre dinamico, variando numerazione dopo pochi minuti dalla visualizzazione al fine di ridurre ulteriormente il rischio di sua sottrazione; c) conferma dell'operazione all'interno dell'area riservata mediante inserimento di una ulteriore OTP inviata via SMS al numero di telefono validato del cliente, quale secondo fattore di autenticazione.

Precisa ancora che ha apposto un blocco cautelativo all'accesso all'area riservata del ricorrente, superabile esclusivamente mediante cambio della password che i truffatori hanno nuovamente modificato.

Argomenta quindi che il ricorrente è incorso in colpa grave nella custodia delle credenziali di sicurezza, tenuto anche conto della mole dei contatti intercorsi con i terzi malfattori e dei codici condivisi dal ricorrente con questi ultimi, osservando che la banca mette a disposizione dei propri clienti numerosi contenuti in materia di sicurezza informatica. In particolare, il 4.1.2024 il ricorrente ha ricevuto un'apposita e-mail volta ad informare i clienti di una importante iniziativa posta in essere dalla stessa al fine di prevenire le frodi perpetrate mediante tecniche di spoofing. Nello specifico, per assicurare ai propri clienti di avere sempre la certezza di essere in contatto telefonicamente con la Banca, simultaneamente all'avvio della telefonata invia sempre al destinatario della stessa un avviso di conferma mediante il canale "i miei messaggi" accessibile esclusivamente nell'App del cliente previa autenticazione.

Chiede il rigetto del ricorso.

DIRITTO

La controversia verte sulla questione relativa alla responsabilità in relazione ad una operazione di pagamento fraudolenta.

Il Collegio precisa 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".

Richiamate le norme, il Collegio precisa che il ricorrente chiede il rimborso di un'operazione di pagamento on line effettuata in data 6/02/2024 con carta di € 2.850,00. È contestata anche una prima operazione pari a € 1,00, che è stata rimborsata dall'intermediario.

I passaggi rilevanti ai fini della valutazione di corretta autenticazione sono: 1) Accesso all'home banking mediante modifica della password di accesso, ove la modalità di autenticazione dichiarata dalla resistente è elemento di conoscenza, 2 cifre del codice pin, elemento di possesso, codice OTP inviato al device del ricorrente; 2) Accesso all'home banking tramite password; 3) Visualizzazione poi, tramite codice OTP inviato al device del ricorrente; 4) aumento del plafond con identica modalità; infine 5) operazione eseguita con carta, tramite OTP inviato al device del ricorrente (elemento di possesso) e CVV dinamico.

Dall'analisi della documentazione in atti il Collegio osserva che il processo di autenticazione richiesto per la modifica della password di accesso all'home banking (fase n.1), per come descritto da parte resistente, può ritenrsi fondato su due fattori di autenticazione indipendenti, posto che secondo *l'Opinion of the European Banking Authority on the elements of strong customer authentication* under PSD2" del 21 giugno

2019, il Pin rappresenta un elemento di conoscenza, mentre il codice OTP inviato tramite sms rientra nella categoria "possesso". Quanto all'accesso all'home banking (fase n. 2) effettuato a seguito della modifica della password, tale accesso, come affermato dall'intermediario, è avvenuto con username e password, tramite app. L'intermediario nulla riferisce in merito al secondo fattore di autenticazione utilizzato per l'accesso ma afferma di aver applicato un meccanismo di autenticazione forte, aggiungendo, che, conformemente alla normativa in materia, si avvale dell'esenzione di cui all'art. 10 del regolamento delegato UE 2018/389.

Il Collegio sul punto richiama ancora *l'Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2* del 21 giugno 2019, ove è stabilito che 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 sarebbe un elemento di possesso conforme. Nel caso di specie l'intermediario non si sofferma sul processo di enrollment dell'app su altro device, affermando genericamente che la password di accesso possa essere modificata da app o dal sito internet. Dalla documentazione emerge inoltre un cambio di dispositivo che parrebbe essersi perfezionato dopo aver avviato la procedura di modifica della password e aver effettuato l'accesso con la password reimpostata.

Inoltre, il Collegio osserva, in merito alle esenzioni SCA previste dal Reg. Delegato 389/2018, che 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).

A seguito dell'accesso all'home banking risultano poi compiute una serie di attività funzionali all'autenticazione delle operazioni dispositive (i.e. visualizzazione pin, aumento del plafond, generazione del cvv dinamico) e emerge altresì che ciascuna di tali attività è stata perfezionata mediante inserimento di un codice OTP nell'ambito di accessi all'home banking avvenuti con username e password.

In ordine all'autenticazione dell'accesso all'home banking vale quanto già sopra osservato.

Il Collegio non ritiene pertanto, in conclusione, richiamato quanto osservato in relazione all'autenticazione dell'accesso all'home banking, che parte resistente abbia adempiuto, da un lato, all'onere su di essa gravante di corretta e completa prova della SCA nella fase di accesso all'Home banking, e, in ogni caso, rileva che, oltre a quanto appena sopra richiamato in merito alla responsabilità in caso di esenzione, 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" (Collegio di Bologna, decisione n. 9591/2024), come nel caso in esame.

Il Collegio ritiene pertanto che gravi su parte resistente la responsabilità per l'operazione fraudolenta, essendo la prima fase di autenticazione prodromica e necessaria al fine dell'esecuzione della stessa, fase in relazione alla quale non risulta adottata una modalità di autenticazione idonea ad escluderla.

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 2.850,00 (duemilaottocentocinquanta/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