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

Il ricorrente, premesso di essere titolare di un conto corrente aperto di recente presso l'intermediario convenuto. Come di seguito ricostruisce i fati accaduti.

In data 10/04/2024, riceveva sul proprio numero di cellulare un SMS con l'invito a "contattare la centrale per certificare il dispositivo" e il giorno successivo, 11/04/2024, chiamava il numero riportato sul messaggio e, su indicazione di un presunto operatore qualificatosi come addetto di una centrale di sicurezza interbancaria nazionale operante per conto di Banca d'Italia, scaricava un'applicazione denominata "Sicurezza Banca", ricevuta tramite SMS.

Accedeva poi all'App dell'home banking, senza comunicare le credenziali all'interlocutore, e constatava che era in corso un aggiornamento dell'App. Nello stesso momento, riceveva un sms contenente il codice OTP per confermare un pagamento con carta di € 1.956,81 e non inseriva tale codice, ma verificava subito che sul conto risultavano effettuati due addebiti da lui non autorizzati: uno di € 0,10 e l'altro di € 1.956,81.

Chiudeva immediatamente la conversazione telefonica e contattava il servizio clienti dell'intermediario convenuto che provvedeva a bloccare immediatamente la carta di pagamento.

Poiché a seguito di disconoscimento dei due addebiti, la convenuta riaccreditava l'importo di € 0,10 ma non rimborsava il pagamento con carta di € 1.956,81, il ricorrente si rivolge all'ABF, al quale chiede di riconoscere il suo diritto al rimborso dell'operazione fraudolenta.

Parte resistente dichiara in primo luogo che l'operazione disconosciuta è stata correttamente autorizzata mediante l'utilizzo delle credenziali statiche e dinamiche in possesso del ricorrente con autenticazione forte a due fattori e registrata e contabilizzata senza aver subito le conseguenze di alcun malfunzionamento delle procedure necessarie per la sua esecuzione.

In generale, osserva che per l'accesso all'area riservata, ai sensi dell'art. 10 del Regolamento Delegato (UE) 2018/839, è 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 180 giorni dall'ultima volta che il cliente ha avuto accesso al conto corrente mediante autenticazione forte; ove non venga effettuata l'autenticazione forte, l'accesso del cliente è limitato alle seguenti informazioni: saldo del conto corrente; operazioni di pagamento eseguite negli ultimi 90 giorni.

Nel caso in esame, precisa che tutti gli accessi all'area riservata del ricorrente sono stati effettuati da indirizzi IP e dispositivi già in passato ordinariamente utilizzati dal ricorrente medesimo e che venivano tentate ulteriori due operazioni che venivano bloccate dai sistemi della banca. Dichiara inoltre che di tutte le operazioni disposte, tanto di quella eseguita, quanto di quelle bloccate, la banca informava il ricorrente in tempo reale mediante push notification.

Conclude sostenendo che la violazione da parte del ricorrente dei propri obblighi ai sensi dell'art. 7 del D.Lgs. 11/2020 è connotata da colpa grave, poiché l'sms e la chiamata ricevuta dal ricorrente non erano in alcun modo riconducibili alla banca e pertanto il ricorrente ha consentito a terzi di entrare in possesso delle credenziali e dei codici necessari, tra l'altro, a operare con la banca.

Parte resistente chiede il rigetto del ricorso.

Nelle repliche il ricorrente osserva che il sistema antifrode della banca ha bloccato un primo pagamento di € 2.896,71 ed un ulteriore pagamento di € 1.029,88 effettuato successivamente a quello oggetto del presente ricorso, che pertanto poteva essere bloccato dalla banca.

Argomenta ancora che la App fraudolenta installata ha carpito gli OTP, sovrapponendosi allo schermo del cellulare del ricorrente, impedendone il controllo, senza nessun inserimento manuale da parte del ricorrente-truffato durante la sessione e che le push notification di fatto non erano visibili, posto che la App fraudolenta occupava tutto lo schermo dello smartphone impedendone la visualizzazione.

Lamenta infine che gli operatori della banca, contattati dopo pochi minuti, non hanno bloccato il pagamento prima che si contabilizzasse e che la banca non ha ritenuto di poter tamponare in nessun modo la perdita.

Nelle controrepliche la resistente precisa che la banca assume nei confronti del cliente l'obbligo di eseguire le operazioni di pagamento disposte secondo le modalità e le tempistiche previste dalla normativa di riferimento, pertanto un'operazione di pagamento può essere bloccata solamente per ragioni eccezionali, fondate sul motivato sospetto che il pagamento possa non essere stato autorizzato dal titolare dello strumento, e le

operazioni di cui è causa non presentavano, sotto il profilo dell'accesso all'area riservata e della loro autorizzazione, alcun elemento di sospetto. Infatti le operazioni non eseguite venivano bloccate in ragione del fatto che le stesse venivano effettuate a brevissima distanza l'una dall'altra, pattern identificato dalla banca come potenzialmente sospetto, criterio che non può portare al blocco indefinito dell'operatività dello strumento in assenza di alcuna anomalia con riferimento al dispositivo e indirizzo IP utilizzati per la connessione. È proprio per questo, argomenta, che il terzo pagamento disposto a breve distanza veniva autorizzato: avendo il ricorrente assunto un obbligo contrattuale di diligente custodia delle proprie credenziali, è ragionevole ritenere che il terzo tentativo consecutivo di pagamento eseguito a distanza di breve tempo dagli altri (che comporterebbe la condivisione di una mole di codici dispositivi particolarmente rilevante con i terzi, e dunque la violazione con evidente colpa grave di tale obbligazione) sia imputabile al legittimo titolare dello strumento di pagamento.

Dichiara infine che nessun rilievo assume la circostanza che il ricorrente avesse installato sul proprio smartphone un'applicazione malevola che peraltro impediva al medesimo di prendere visione delle notifiche in App inviate dalla Banca.

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 11/04/2024 con la carta di debito associata al conto corrente di € 1.956,81.

L'intermediario descrive così i passaggi autorizzativi. 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; ove non venga effettuata l'autenticazione forte, l'accesso del cliente è limitato alle seguenti informazioni: saldo del conto corrente; operazioni di pagamento eseguite negli ultimi 90 giorni. Precisa che per la disposizione dell'operazione di pagamento con carta, è richiesto l'inserimento delle credenziali statiche (PAN e data di scadenza) della carta, consultabili esclusivamente all'interno dell'area riservata, nonché del CVV della carta, che non è stampato sulla stessa come ordinariamente avviene, ma è generabile esclusivamente nell'area riservata previo (a) accesso alla medesima con le modalità sopra descritte e (b) inserimento di una OTP inviata all'utenza mobile validata dal cliente. Precisa ancora che il CVV è dinamico, variando numerazione dopo pochi minuti dalla visualizzazione al fine di ridurre ulteriormente il rischio di sua sottrazione (primo fattore di autenticazione) e l'operazione viene poi confermata all'interno dell'area riservata, previo accesso con le modalità, mediante inserimento di una ulteriore OTP inviata via SMS all'utenza mobile validata dal cliente (secondo fattore di autenticazione).

Nel caso di specie, l'intermediario riepiloga l'attività registrata dalla banca e trasmette documentazione da cui emerge in primo luogo che tutti gli accessi all'area riservata del ricorrente sono stati effettuati da indirizzo IP e dispositivo già in passato ordinariamente utilizzati dal ricorrente medesimo.

Il primo accesso all'area riservata dell'11/04/2024 è stato registrato alle ore 12:25:59, con inserimento di username e password conosciute esclusivamente dal ricorrente (colonna "Medio de autentificacion"); l'accesso non ha richiesto l'inserimento anche di una OTP quale secondo fattore di autenticazione, in quanto il ricorrente aveva eseguito l'accesso all'area riservata mediante strong customer authentication meno di 90 giorni prima di tale accesso, in data 27/03/2024 (in atti).

Emerge quindi che alle ore 12:57:24, veniva in primo luogo generato il CVV dinamico della carta mediante inserimento, all'interno dell'area riservata del ricorrente, di OTP inviata con SMS al cellulare indicato dal ricorrente in denuncia e alle ore 12:58:30, veniva aumentato il limite massimo di esecuzione dei pagamenti online con Carta ad Euro 3.000,00 mediante conferma dell'operazione con secondo fattore di autenticazione a mezzo OTP inviata via SMS al cellulare indicato dal ricorrente in denuncia.

Era quindi tentata l'esecuzione di un primo pagamento con carta di Euro 2.986,71, mediante (a) inserimento di PAN, data di scadenza e CVV precedentemente generato della Carta all'interno del POS virtuale utilizzato e (b) conferma mediante OTP inviata via SMS al ricorrente (l'allegato a cui l'intermediario fa riferimento nelle controdeduzioni non risulta peraltro trasmesso); tale operazione non veniva tuttavia eseguita; alle ore 13:09:00, veniva nuovamente generato il CVV dinamico con le medesime modalità di cui sopra.

Emerge ancora che veniva quindi tentata l'esecuzione di un nuovo pagamento con carta, sempre di Euro 2.986,71, mediante (a) inserimento di PAN, data di scadenza e CVV

precedentemente generato della Carta all'interno del POS virtuale utilizzato e (b) conferma mediante OTP inviata via SMS al ricorrente (cfr. all. 8 alle controdeduzioni); l'operazione veniva tuttavia bloccata dai sistemi antifrode della Banca, in considerazione del tentativo a breve distanza dal precedente; nella medesima sessione di validità del CVV, alle ore 13:11, veniva disposto il pagamento con carta di Euro 1.956,81, oggetto del presente ricorso, mediante (a) inserimento di PAN, data di scadenza e CVV precedentemente generato della carta all'interno del POS virtuale utilizzato e (b) conferma mediante OTP inviata via SMS al cellulare indicato dal ricorrente in denuncia. Al riguardo, l'intermediario trasmette anche il registro di conferma dell'operazione, in lingua spagnola prodotto da processor utilizzato dalla banca per l'esecuzione dei pagamenti con carta, precisando che tale documento attesta l'autenticazione dell'operazione oggetto del presente ricorso mediante SCA con utilizzo dei due fattori menzionati (CVV dinamico e OTP inviata via SMS al ricorrente), senza fornire ulteriori precisazioni né legenda. Da ultimo emerge la tentata esecuzione di un'ultima operazione con carta di € 1.029,88 con le medesime modalità di cui alle precedenti (cfr, l'SMS recante l'OTP dell'operazione, allegato 12); anche questo tentativo di pagamento veniva bloccato dai sistemi della banca.

Ciò posto, il Collegio osserva innanzitutto che il processo di autenticazione richiesto per l'accesso all'area riservata è avvenuto con username e password. Dal log prodotto 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. Anche l'accesso all'home banking è avvenuto da app installata sul device del ricorrente.

Il Collegio sul punto richiama *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 sull'app come fattore di autenticazione e riferisce che il secondo elemento per la SCA sarebbe l'inoltro dell'OTP al device del cliente.

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).

Il Collegio non ritiene pertanto, in conclusione, che parte resistente abbia adempiuto, da un lato, all'onere su di essa gravante di corretta e completa prova della SCA nella fase di login, 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 non possa che gravare su parte resistente la responsabilità per l'operazione fraudolenta, essendo la prima fase di autenticazione prodromica e necessaria al fine dell'esecuzione della stessa.

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 1.957,00 (millenovecentocinquantasette/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