COLLEGIO DI NAPOLI

composto dai signori:

(NA) CARRIERO	Presidente
(NA) CAGGIANO	Membro designato dalla Banca d'Italia
(NA) LIACE	Membro designato dalla Banca d'Italia
(NA) RUGGIERO	Membro di designazione rappresentativa degli intermediari
(NA) PALMIERI	Membro di designazione rappresentativa dei clienti

Relatore ILARIA AMELIA CAGGIANO

Seduta del 03/10/2023

FATTO

Il ricorrente lamenta nel ricorso che in data 22.11.2022 riscontrava l'esecuzione di operazioni anomale da lui non autorizzate sul proprio conto corrente, con conseguente sottrazione di tutto il capitale ivi depositato; resosi conto dell'ammanco, denunciava l'accaduto alla Polizia Postale e al servizio clienti dell'intermediario, che rifiutava di restituire le somme sottratte pari ad € 18.200,00.
Assumendo che l'intera responsabilità dell'accaduto sia imputabile all'intermediario/prestatore dei servizi di pagamento, anche per mancata diligente custodia dei propri dati personali di tipo finanziario, chiede, pertanto, la restituzione di tutte le somme sottratte per € 18.200,00.
L'intermediario si oppone alle richieste del ricorrente, evidenziando che:
- dalle verifiche effettuate risulta la legittima esecuzione e sostanziale regolarità delle operazioni contestate e l'adeguatezza dei presidi di sicurezza informatica di cui dispone;
- il ricorrente non ha descritto dettagliatamente le modalità della frode subita né la dinamica, limitandosi ad affermare di non aver autorizzato le operazioni oggetto di contestazione, delle quali si sarebbe avveduto solamente a frode conclusa;
- tale ricostruzione non coincide con le risultanze informatiche versate in atti; infatti dall'analisi della documentazione allegata risulta evidente che il ricorrente ha autorizzato le singole transazioni nel pieno rispetto della normativa in materia nonché in applicazione del sistema di autenticazione multifattoriale; egli sarebbe, dunque, rimasto vittima di una

tipologia di frode di tipo “social hacking ”, che consiste nell’impartire telefonicamente o tramite altro canale comunicativo istruzioni manipolative al titolare dello strumento di pagamento, lasciando che sia questi ad autenticare le singole transazioni;
- il ricorrente ha omesso di riferire circostanze rilevanti: non ha riferito che in data 22.11.2022 aveva dapprima effettuato una serie di accessi al proprio conto corrente dalla app installata sul device personale associato al conto con sistema operativo Android e device token, per poi autorizzare in app, verosimilmente sulla scorta delle istruzioni impartite da soggetti terzi, le n. 6 operazioni di bonifico oggetto di contestazione; gli accessi al conto sono avvenuti tramite autenticazione forte multifattoriale, con inserimento dell’ID biometrico (elemento di inerenza) e contestuale utilizzo dell’app installata sul dispositivo associato in via esclusiva al conto del ricorrente (elemento di possesso);
- il comportamento del ricorrente appare connotato da colpa grave;
- in riferimento al generale fenomeno del phishing ed alle sue possibili declinazioni, da tempo ha intrapreso una capillare serie di campagne informative finalizzate a rendere edotta la propria clientela.
L’intermediario precisa che:
- è una banca interamente digitale, che opera esclusivamente da remoto con la propria clientela;
- adotta sistemi informatici che rispettano i più alti standards di sicurezza, al fine di assicurare il rispetto dei requisiti regolamentari imposti alle banche a livello comunitario e nazionale e di garantire ai propri clienti la migliore esperienza e la massima tutela rispetto a possibili intromissioni fraudolente da parte di soggetti terzi non autorizzati, predisponendo un sistema di autenticazione forte sia per l’accesso all’ home-banking - tramite la propria applicazione mobile oppure tramite la Web-App - sia per l’autorizzazione delle operazioni dispositive;
- non si è verificato alcun “data breach”, posto che il ricorrente ha sempre mantenuto - nel corso della frode - il pieno ed esclusivo controllo dell’app installata sul proprio dispositivo mobile personale associato al conto; tale circostanza è avvalorata dal fatto che il dispositivo mobile che ha effettuato gli accessi al conto in data 22.11.2022, contestualmente alla disposizione ed autorizzazione degli ordini di pagamento oggetto di ricorso, risulta essere il device token associato allo UserID esclusivamente riferibile al ricorrente ed in uso fin dalla data di prima associazione avvenuta il giorno 7.7.2021; il ricorrente, inoltre, non ha mai denunciato lo smarrimento o il furto del proprio smartphone;
- il ricorrente, utilizzando una media diligenza, avrebbe dovuto provvedere autonomamente al tempestivo blocco del proprio strumento di pagamento e a contattare la Banca; invece, egli ha autorizzato le n. 6 operazioni di pagamento oggetto di controversia durante un arco temporale che andava dalle ore 20:13 UTC+1 (esecuzione della prima transazione) alle ore 20:32 UTC+1 (esecuzione dell’ultima transazione), assicurando così il perfezionamento della frode stessa;
- al caso di specie deve essere applicato quanto previsto dall’art. 12 co. 4 del d. lgs. 11/2010, dovendo il ricorrente sopportare la perdita derivante dalle operazioni di pagamento per l’importo complessivo pari ad € 18.200,00.
L’intermediario chiede, pertanto, al Collegio di rigettare il ricorso.
Il ricorrente ha replicato alle controdeduzioni, evidenziando di non poter riferire i dettagli della truffa subita perché avvenuta a sua insaputa, a differenza della banca che avrebbe immediatamente rilevato che vi era stato un accesso anomalo sul suo c/c.
L’intermediario ha depositato controrepliche, osservando - tra l’altro - che il ricorrente afferma per la prima volta in sede di repliche alle controdeduzioni che i truffatori sarebbero riusciti da remoto a prendere possesso del suo cellulare, autorizzando dunque a sua insaputa le diverse operazioni contestate.

DIRITTO

Oggetto del ricorso è la richiesta di rimborso integrale di n. 6 operazioni di pagamento (bonifici istantanei), eseguiti on line con l'utilizzo di credenziali a lui riferibili in data 22.11.2022, per un importo complessivo di € 18.200,00.
Le operazioni contestate rientrano pienamente nell'ambito applicativo 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), entrato in vigore il 13.01.2018, che è la normativa regolante la materia, la quale va ad integrare le norme generali in tema di adempimento delle obbligazioni e responsabilità, di diligenza del mandatario (art. 1710 c.c.) e della banca nell' "esecuzione degli incarichi" (art. 1852 c.c.).
La disciplina speciale regola gli obblighi e le responsabilità gravanti sul prestatore e sull'utente dei servizi di pagamento, nel seguente modo:
a) sul prestatore incombono gli obblighi, riconducibili all'organizzazione dell'impresa (bancaria), di predisporre misure e sistemi di sicurezza che non consentano l'accesso da parte di terzi ai dispositivi personali dell'utente, che assicurino la disponibilità di mezzi per consentire a quest'ultimo di comunicare senza indugio evenienze di usi non autorizzati o di sottrazione; ulteriori obblighi di impedire l'uso degli strumenti di pagamento successivamente a tali comunicazioni (art. 8). Per l'inadempimento di tali obblighi e per la mancata predisposizione di sistemi di autenticazione forte (che è una delle più significative novità introdotte dalla suddetta normativa per qualsiasi azione tramite canali a distanza, tra cui i pagamenti online, art. 10-bis), il prestatore è responsabile, in via aggravata, fatta salva l'ipotesi del comportamento fraudolento dell'utente (art. 8, co. 2, 2bis, in correlazione con art. 12, co. 1 e 2). Sul punto, il Regolamento Delegato (UE) 2018/389 individua come requisiti ai fini della SCA due o più elementi che siano classificati nelle categorie della conoscenza, del possesso e dell'inerenza, purché indipendenti tra loro, nonché la presenza di un collegamento dinamico, e la Opinion del 21 giugno 2019 dell'EBA, quale atto di soft law, individua esempi specifici come paramento di valutazione degli elementi sopra indicati;
b) all'utente s'impone l'adozione di misure idonee di protezione delle credenziali e si ribadisce l'utilizzo dello strumento di pagamento in conformità con i termini, esplicitati nel contratto quadro, nonchè la tempestiva denuncia di furto, smarrimento, distruzione o altro uso non autorizzato dello strumento (art. 7). Egli è responsabile per comportamento fraudolento ovvero per doloso o gravemente colposo inadempimento degli obblighi previsti (art. 12, co. 4).
Il sistema di responsabilità appena descritto, ispirato al principio del rischio d'impresa e all'allocazione dei costi principalmente sull'impresa bancaria (recte sulla molteplicità degli utenti, "essendo quest'ultimo in grado di parcellizzare, distribuendolo sulla moltitudine dei clienti, il rischio dell'impiego fraudolento di carte di credito o di strumenti di pagamento") (sul punto v. ABF, Collegio di Coordinamento, nn. 3947/2014 e 3498/2012) è assistito da uno speciale regime probatorio che, a fronte del mero disconoscimento delle operazioni di pagamento da parte dell'utente, onera il prestatore di:
i) provare che l'operazione è stata autenticata, correttamente registrata e contabilizzata e che la sua patologia non si deve a malfunzionamenti delle procedure esecutive o ad altri inconvenienti del sistema (art. 10, d.lgs. 11/2010 e Coll. Coord. 3947/2014). Nell'ambito di tali oneri, per orientamento condiviso tra i Collegi e indirizzo del Collegio di Coordinamento, vi è la prova di aver fornito il servizio di sms alert o assimilabili da cui l'intermediario può essere esonerato solo dimostrando l'esplicito rifiuto dell'utente ad avvalersene. In ogni caso, gli effetti della mancata adozione del servizio di alert devono

essere valutati alla stregua delle circostanze di fatto del caso concreto (Coll. Coord., n. 24366/2019);
ii) provare la riconducibilità dell'operazione all'utente che la disconosca ovvero la frode o l'inadempimento doloso o gravemente colposo dell'utente stesso, nonostante l'apparentemente corretta autenticazione dell'operazione di pagamento, (art. 8, co. 1, 2; Collegio di Coordinamento, con decc. n. 22745 del 2019 e 3947/2014). In particolare, il Collegio di coordinamento dell'ABF, con decisione n. 22745/2019, ha chiarito: "La previsione di cui all'art. 10, comma 2, del d.lgs. n. 11/2010 in ordine all'onere posto a carico del PSP della prova della frode, del dolo o della colpa grave dell'utilizzatore, va interpretato nel senso che la produzione documentale volta a provare l''autenticazione' e la formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere probatorio, essendo necessario che l'intermediario provveda specificamente a indicare una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente".
L'onere della prova della genuinità della transazione, ovvero della frode, dolo o colpa grave dell'utente ricade quindi sul prestatore del servizio e può ovviamente essere fornita pure per mezzo di presunzioni gravi, precise e concordanti, secondo quanto dispone l'art. 2729 c.c., di un comportamento fraudolento, doloso o gravemente colpevole dell'utente (ex multis cfr. Collegio Napoli, dec. 1091/2018). La stessa Corte di Cassazione, a tale specifico riguardo, ritiene che sia ammissibile la prova indiziaria della sussistenza della colpa grave (cfr. Cass. n. 654/2010).
Nel caso in esame, ai fini della decisione, dirimente è il fatto che l'intermediario non ha fornito piena prova della autenticazione delle operazioni contestate che sia riconducibile alla cliente ai sensi e per gli effetti dell'art. 10 e 12 del D. Lgs. 11/2010 (e successive modifiche).
In particolare, l'intermediario produce evidenze informatiche relative alla fase di accesso al conto da parte del ricorrente nella giornata del 22.11.2022, con doppio fattore di autenticazione (biometria e possesso del device, in cui risulta installata l'app) da cui risulta che - sempre in data 22.11.2022 - a partire dalle ore 8:33 PM (UTC – ora locale 21:33), sono stati registrati numerosi tentativi di accesso al conto del ricorrente da altro device (nuovo ID device_token registrato).
Sulle singole operazioni contestate, dalla produzione documentale, si evince che: le prime tre operazioni di bonifico – eseguite rispettivamente alle ore 19:13 UTC/20:13 ora locale, 19:21 UTC/20:21 ora locale, 19:22 UTC/20:22 ora locale sono state autorizzate a seguito del login effettuato dal ricorrente alle ore 19:02 UTC/20:02 ora locale; le altre tre operazioni - rispettivamente delle ore 19:28 UTC/20:28 ora locale, 19:30 UTC/20:30 ora locale, 19:32 UTC/20:32 ora locale - sono state effettuate a seguito del login avvenuto alle ore 19:25 UTC - 20:25 ora locale.
L'intermediario produce, altresì, evidenza informatica delle seguenti attività: 1. notifiche push inviate per l'autorizzazione delle singole operazioni, 2. autorizzazione delle operazioni, che risulta avvenuta da un device token associato al conto corrente del ricorrente in data 7.7.2021 e dissociato in data 22.11.2022 alle ore 21:54 (UTC), dopo l'esecuzione delle operazioni contestate.
L'autorizzazione risulta avvenuta tramite l'app installata sul dispositivo associato al conto corrente, mediante autenticazione a due fattor costituiti dalla digitazione del codice PIN di conferma (creato dal ricorrente in data 7.7.2021 in fase di apertura conto) e dalla convalida dell'operazione con notifica push generata in app.
Tuttavia, questo Collegio osserva che non è riportata nella produzione documentale alcuna indicazione del device al quale le notifiche push sono state inviate, né, peraltro,

risulta indicato il testo delle suddette notifiche, che l'intermediario nelle sue controdeduzioni solo riporta in via descrittiva, non producendo alcuna evidenza.
In altri termini, sebbene l'operazione risulti esser stata autorizzata mediante invio di notifica push all'App del cliente (fattore di possesso) e confermata mediante digitazione di codice PIN (fattore di conoscenza), e quindi astrattamente conforme alle prescrizioni normative in materia di SCA, nel caso di specie non risulta un processo di autorizzazione interamente riconducibile al device del ricorrente, che ben potrebbe essere avvenuta per mano di un truffatore (che avrebbe installato la app sul proprio dispositivo e ivi ricevuto la push), né sono state provate le modalità della fase di installazione e di configurazione dispositiva dell'app sul dispositivo. Tale mancanza di allegazioni in merito non consente di ritenere assolto l'onere probatorio gravante sull'intermediario di aver predisposto misure e sistemi di sicurezza che non consentano l'accesso da parte di terzi ai dispositivi personali dell'utente (i) e che l'operazione sia riconducibile all'utente (ii).
Ciò conduce all'accoglimento del ricorso, esimendo dalla disamina dei profili di eventuale colpa grave dell'utilizzatore dello strumento di pagamento.
Giova ricordare che, 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 va accolto integralmente, 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 (ex multis cfr. Collegio di Napoli decisione n. 23331/2021; Collegio di Milano decisione n. 23546/2021).
In virtù di quanto sopra esposto, il Collegio accoglie il ricorso e dichiara l'intermediario tenuto al rimborso, in favore della parte ricorrente, della somma di € 18.200,00.

P.Q.M.

In accoglimento del ricorso, il Collegio accerta il diritto del ricorrente alla restituzione dell'importo di € 18.200,00.
Il Collegio dispone inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di € 200,00 quale contributo alle spese della procedura e al ricorrente la somma di € 20,00 quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
GIUSEPPE LEONARDO CARRIERO