Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

# COLLEGIO DI BOLOGNA

composto dai signori:

| | |
|---|---|
| (BO) MARINARI | Presidente |
| (BO) MARTINO | Membro designato dalla Banca d'Italia |
| (BO) TRENTO | Membro designato dalla Banca d'Italia |
| (BO) SOLDATI | Membro di designazione rappresentativa degli intermediari |
| (BO) PETRAZZINI | Membro di designazione rappresentativa dei clienti |

Relatore NICOLA SOLDATI

Seduta del 21/12/2021

Esame del ricorso n. 1149941/2021 del 03/08/2021

proposto da BONUCCI SIMONA

nei confronti di 7601 - POSTE ITALIANE S.P.A.

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

## COLLEGIO DI BOLOGNA

composto dai signori:

| | |
|---|---|
| (BO) MARINARI | Presidente |
| (BO) MARTINO | Membro designato dalla Banca d'Italia |
| (BO) TRENTO | Membro designato dalla Banca d'Italia |
| (BO) SOLDATI | Membro di designazione rappresentativa degli intermediari |
| (BO) PETRAZZINI | Membro di designazione rappresentativa dei clienti |

Relatore NICOLA SOLDATI

Seduta del 21/12/2021

## FATTO

Il ricorrente riferisce di essere stato vittima, in data 16.05.2021, di un caso di *vishing*, essendo state effettuate dal suo conto n. 4 accrediti su carte prepagate per l'importo complessivo di € 6.974,46 (nel dettaglio: € 2.971,00; € 2.973,00; € 990,00; € 37,46); accedendo al suo *home banking*, si accorgeva che l'applicazione risultava bloccata, pertanto provvedeva a chiamare il numero verde dell'intermediario convenuto e l'operatore gli riferiva che sarebbe stato ricontattato per ricevere istruzioni; il giorno successivo, un sedicente operatore della banca, tramite il numero verde "ufficiale" dell'intermediario convenuto, telefonava al coniuge del ricorrente, che aveva in uso i codici del conto, e lo invitava a leggergli i numeri che gli arrivavano con sms (testualmente, lo invitava "*a compiere determinate operazioni, nello specifico allo stesso venivano mandati sms con delle numerazioni, poi, una volta richiamato, l'operatore gli chiedeva di rileggerli...non digitando però mai, lo stesso, il codice Pin di accesso, né tantomeno un OTP*"); nel frattempo, al ricorrente arrivavano messaggi di avvenuta transazione dei suddetti prelievi e, pertanto, provvedeva al blocco della carta bancomat e della carta di credito; accertata l'avvenuta esecuzione delle operazioni fraudolente, sporgeva querela presso l'autorità competente ed inoltrava il disconoscimento delle suddette operazioni; con pec del 3.6.2021, chiedeva infruttuosamente alla convenuta di conoscere i beneficiari degli accrediti, oltre all'orario e al luogo delle operazioni, al fine di procedere con

l'identificazione dei soggetti titolari delle carte prepagate; la telefonata del sedicente operatore è pervenuta dal numero verde "*ufficiale*" della banca, questo comporta una responsabilità oggettiva della convenuta e l'assenza di colpa dei ricorrenti; risulta inoltre evidente l'assenza della cosiddetta "*autenticazione forte*", in quanto il solo codice OTP non è sufficiente a garantire la sicurezza on line, essendo necessario un secondo elemento.
La parte ricorrente chiede all'ABF di condannare l'intermediario al rimborso integrale delle operazioni da questi negate, per l'importo complessivo di Euro 6.974,446 oltre 200,00 euro di spese legali.

Costituitosi ritualmente l'intermediario precisa ed eccepisce che: a) il ricorrente è titolare di un conto a cui è associata una carta di debito; b) le operazioni contestate sono tre operazioni di ricarica *on line*, di € 2.971,00, € 2.973,00 ed € 990,00, nonché un'operazione di pagamento pos di € 37,46, disposte in data 16 e 17 maggio 2021; c) le verifiche effettuate hanno accertato la legittima esecuzione e sostanziale regolarità delle contestate operazioni; d) per quanto riguarda le operazioni di ricarica, il ricorrente si è correttamente autenticato sulla piattaforma con le proprie credenziali e le transazioni sono state eseguite con sistema dinamico di autenticazione; e) ciò in quanto l'esecuzione delle stesse ha necessitato l'utilizzo del codice ***.ID in App; f) il funzionamento del ***.ID prevede che la transazione disposta da canale home banking venga firmata mediante certificato presente sul *Back-End*; la transazione firmata viene sottoposta a controllo da parte del *framework* Identità Digitale; in caso di esito positivo, la transazione firmata genera una notifica *push* che invita il cliente ad attivare l'App, la quale verifica la firma sulla transazione apposta dal canale, mostra i dati transazione all'utente e chiede il PIN per l'autorizzazione; viene quindi generata una OTP contenente ID Transazione, Chiave randomica e Chiave Simmetrica statica univoca; g) le operazioni in disamina sono state effettuate da App, per la cui installazione e configurazione dispositiva degli strumenti di pagamento è necessario conoscere: le credenziali di accesso ai servizi di *internet banking*, i dati della carta utilizzata per effettuare i pagamenti online (ossia PAN, CVV2 e data di scadenza) e la password dinamica "*usa e getta*" inviata sul numero di cellulare rilasciato dal cliente all'intermediario, necessaria per impostare il "codice ***.id" per autorizzare le successive disposizioni di pagamento effettuate da App; h) la responsabilità della frode è imputabile esclusivamente al cliente, il quale ha comunicato tutti i codici sopra specificati, causando di fatto la violazione del sistema di autenticazione informatica c.d. "*a due fattori*"; i) il comportamento gravemente colposo del ricorrente ha favorito l'indebito utilizzatore, anche consentendogli di adottare un comportamento del tutto analogo all'utente in buona fede, il quale di solito accede ai servizi online in prima battuta grazie al pronto uso delle credenziali, inserisce correttamente i dati del dispositivo da utilizzare perché a portata di mano e conosce per diretta verifica l'entità della somma fruibile per l'eventuale acquisto; l) le evidenze informatiche attestano la certificazione del numero di cellulare del cliente (lo stesso presente in denuncia), il quale risulta essere regolarmente abilitato al sistema autorizzativo funzionante mediante invio con sms della password dinamica; m) al truffatore risultava indispensabile la ricezione delle OTP, necessarie ai fini dell'"*onboarding*" della carta e della configurazione del ***.Id all'interno dell'App sul proprio *device*; n)le successive transazioni di ricarica, disconosciute da parte ricorrente, sono state infatti disposte tramite inserimento del codice ***.Id in App; o) relativamente alla restante operazione di pagamento da € 37,46, le evidenze informatiche certificano che al momento della materiale esecuzione della stessa i sistemi informativi non hanno rilevato alcuna anomalia o irregolarità, essendo stata disposta dietro diretta ed immediata autenticazione da parte della legittima titolare; p) la transazione in questione è un pagamento POS regolarmente eseguito con lettura del *microchip* della carta e digitazione corretta del

codice PIN; q) detta operazione è avvenuta presso un esercizio commerciale sito presso la città di residenza del ricorrente, dove controparte dichiara di essersi recato più volte; r) la cliente non dichiara di aver mai smarrito la carta, ragion per cui tale operazione deve essere stata necessariamente eseguita dal cliente stesso; s) la ricorrente ha provveduto al blocco della carta in questione solo in data 20/05/2021, ovvero quattro giorni dopo l'inizio delle transazioni in questione; t) un servizio di *alert* è attivo di default all'interno dell'App; u) il negligente comportamento della ricorrente ha dato modo al frodatore di completare la certificazione del ***.Id sul proprio *device*, per poi porre in essere le transazioni per cui è controversia; v) la presente frode è riconducibile alla tipologia di *phishing* definita "classica" nella Decisione del Collegio di Coordinamento 3498/2012; x)) in merito a tale forma di *phishing* l'intermediario ormai da tempo sta rendendo edotta la propria clientela; y) la titolare della carta ha tenuto un comportamento gravemente colposo, al quale è esclusivamente imputabile la compromissione dello strumento finanziario in suo possesso.
Alla luce di quanto sopra l'intermediario richiede di respingere il ricorso e in subordine in caso di accoglimento chiede l'applicazione della franchigia.

**DIRITTO**

Il Collegio rileva che le operazioni contestate sono state poste 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.

Parte ricorrente disconosce tre operazioni di ricarica on line di € 2.971,00, € 2.973,00 ed € 990,00, nonché un'operazione di pagamento POS di € 37,46 disposte in data in data 16 e 17 maggio 2021. Agli importi sopra indicati si aggiungono € 3,00 a titolo di commissioni, richiesti nella domanda di ricorso.
Dalla documentazione prodotta dalle parti, in particolare dalla denuncia, si evince che la truffa sarebbe stata attuata con una chiamata telefonica da parte di una persona rivelatasi essere un finto funzionario.
Dalla ricostruzione effettuata dall'intermediario (cfr. *infra*) risulterebbe che le tre operazioni di ricarica disconosciute sono state effettuate da *App* con l'"*onboarding*" della carta e la generazione di un nuovo "*codice […]ID*", mentre l'operazione di € 37,46 sarebbe un pagamento POS eseguito con lettura del microchip della carta e digitazione corretta del codice PIN.

L'art. 10-*bis*, comma 1, del suddetto d.lgs., come modificato, statuisce che i prestatori di servizi di pagamento applichino l'autenticazione forte (SCA) del cliente qualora l'utente:
a) acceda al suo conto di pagamento online;
b) disponga un'operazione di pagamento elettronico;
c) effettui qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi.

Il Collegio osserva innanzitutto che, in allegato alle controdeduzioni, l'intermediario deposita una "scheda tecnica" che descrive in ottica SCA il processo di autenticazione di una transazione generata da *Web* e autorizzata in *App* tramite il *codice[…] ID.*
Del pari, il Collegio osserva che le più recenti decisioni dei Collegi ABF (cfr. Collegio di Bologna, n. 14124/2020 e Collegio di Roma, n. 19067/2020, *infra* riportate tra i "Precedenti ABF"), ritengono il sistema di autenticazione mediante "codice […] ID" compatibile con i

criteri previsti per l'autenticazione forte, "*posto che il codice statico scelto dall'utente integra il fattore di conoscenza, in relazione all'ulteriore fattore del possesso, le "Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2" del 21 giugno 2019 riconoscono come "compliant with SCA" l'utilizzo di un App collegata a un dispositivo*".

Tanto premesso, il Collegio evidenzia che occorre valutare se, nel caso di specie, la documentazione prodotta dall'intermediario sia idonea a dimostrare la corretta autenticazione dell'operazione contestata.
A tal fine, per quanto riguarda le tre operazioni di ricarica, l'intermediario ha depositato evidenza informatica relativa alle operazioni disconosciute che riporta la dicitura "*transazione securizzazione con codice ***.ID in App B****"; evidenza attestante la certificazione del numero di cellulare del cliente (lo stesso presente in denuncia), il quale risulta essere regolarmente abilitato al sistema autorizzativo funzionante mediante invio con sms della password dinamica; tracciatura dell'SMS di configurazione del codice ***.ID, senza indicazione del testo/oggetto, inviato al numero di cellulare di parte ricorrente alle ore 19:12, poco prima della prima operazione, avvenuta alle ore 20:05.
Non constano agli atti ulteriori tracciature informatiche attestanti le modalità con cui è avvenuta l'installazione dell'App su un diverso dispositivo e la generazione del nuovo "codice […] ID" né *log* concernenti l'autenticazione delle tre operazioni fraudolente tramite inserimento del predetto codice.
Alla luce di quanto sopra e in mancanza di tale produzione il ricorso deve essere accolto *in parte qua*, oltre ad euro 1,00 per spese di ciascuna commissione.

Per quanto riguarda, invece, l'operazione di pagamento di € 37,46, l'intermediario ha depositato le evidenze informatiche dell'operazione evidenziando anche che detta operazione è avvenuta presso un esercizio commerciale sito presso la città di residenza del ricorrente, dove controparte dichiara nel verbale della denuncia di essersi recato più volte. Ne consegue il ricorso in merito a tale operazione non può trovare accoglimento.

La domanda di rimborso delle spese legali deve essere rigettata in forza del consolidato orientamento dei Collegi ABF.

Da ultimo, il Collegio rileva che l'intermediario in caso accoglimento del ricorso ha richiesto l'applicazione della franchigia che, nel caso di specie, deve trovare applicazione.

**PER QUESTI MOTIVI**

**Il Collegio – in parziale accoglimento del ricorso – dichiara l'intermediario tenuto in favore della parte ricorrente alla restituzione dell'importo complessivo di euro 6.886,00 (seimilaottocentottantasei/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