Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI NAPOLI

composto dai signori:

(NA) CARRIERO	Presidente
(NA) SANTAGATA DE CASTRO	Membro designato dalla Banca d'Italia
(NA) CAGGIANO	Membro designato dalla Banca d'Italia
(NA) SILVESTRI	Membro di designazione rappresentativa degli intermediari
(NA) PALMIERI	Membro di designazione rappresentativa dei clienti

Relatore GIANMARIA PALMIERI

Seduta del 09/03/2021

FATTO

La ricorrente che è intestataria con il consorte, aderente al ricorso, di un conto corrente in essere presso la banca convenuta, riferisce di aver ricevuto, il 29 settembre 2020, una telefonata da parte di un sedicente operatore della Banca, che le ha chiesto di disinstallare l'applicazione dell'intermediario, per aggiornamenti in corso.
Successivamente, il 3 ottobre, lo stesso operatore le ha chiesto, sempre via telefono, di procedere alla installazione della applicazione. Tuttavia, durante tale processo, sul suo *smartphone* le è apparso l'avviso di un prelievo di € 2.000,00, a seguito del quale l'operatore ha interrotto la telefonata.
Accortasi dell'anomalia, la ricorrente, contattata la banca, ha scoperto di essere stata truffata. Ha quindi bloccato immediatamente la carta e si è recata presso uno sportello ATM, ove ha scoperto che le erano stati sottratti € 5.000,00 tramite nr. 3 prelievi e ha sporto denuncia dinnanzi le competenti autorità.
Insoddisfatta della prodromica interlocuzione con l'intermediario si rivolge all'Arbitro precisando di non aver comunicato all'operatore le password né altri dati. Evidenzia altresì che quest'ultimo si è mostrato *"tecnico e padrone della materia"*, qualificandosi come dipendente della banca e dando precise direttive, ingenerando quindi un legittimo affidamento.
Richiamata la normativa di riferimento - ai sensi della quale il disconoscimento da parte del cliente dell'operazione fraudolenta implica l'inversione dell'onere probatorio, sicché è

l'istituto, nella sua qualità di prestatore di servizi di pagamento, a dover dimostrare la riconducibilità dell'operazione contestata al proprio correntista (Cass. Civ. Sent. n. 9158/2018) - chiede all'Arbitro di condannare l'intermediario alla somma prelevata fraudolentemente, pari a € 5.000,00, oltre alle spese di assistenza difensiva.
Costituitosi, l'intermediario rappresenta che la ricorrente medesima ha confermato di aver ricevuto almeno due telefonate da un finto operatore della Banca che, con l'inganno, ha fatto sì che lei gli comunicasse i codici per abilitare un altro dispositivo. Sul punto, precisa che per l'accesso ai servizi online della banca è necessario l'inserimento di due password statiche (codice del titolare e codice Pin) e una password dinamica (codice OTP).
Al riguardo, evidenzia di aver inviato al numero di cellulare della ricorrente un sms contenente il codice per l'attivazione del servizio, con espresso avvertimento di usare tale codice solo all'interno dell'App mobile; l'invio di tale messaggio consente al cliente di venire a conoscenza dell'avvio della procedura finalizzata alla generazione di codici dispositivi, il quale ha così la possibilità di impedirne l'esecuzione.
Nel caso di specie, la ricorrente ha comunicato il codice al truffatore, così abilitando lo *smartphone* in possesso del truffatore a generare OTP virtuali in sostituzione del suo dispositivo. Di tale abilitazione è stata data comunicazione alla ricorrente tramite invio di un *sms alert,* con specifica indicazione del dispositivo da cui il servizio opera.
Una volta attivato il servizio, il malfattore ha potuto autorizzare le operazioni di prelievo *cardless,* confermate con la creazione di codice dinamico OTP, come evidenziano le tracciature delle suddette operazioni.
Pertanto l'intermediario ritenendo che la ricorrente abbia fornito le credenziali necessaria al truffatore per attivare il servizio sullo *smartphone* di quest'ultimo, lamenta una violazione da parte della ricorrente dell'obbligo di custodire con diligenza i propri codici.
Chiarisce poi che sebbene la ricorrente asserisca di esser stata contattata dal numero verde dell'intermediario, da tale numero non possono essere effettuate telefonate, trattandosi di un servizio abilitato alla sola ricezione in entrata di telefonate. Tale circostanza avrebbe da subito dovuto allarmare la ricorrente, così come la modifica delle domande di sicurezza, per la quale ella è stata prontamente informata.
D'altronde dalle tracciature si rilevano le disposizioni impartite dal *My Key* della Cliente che hanno portato in data 2 e 3 ottobre ai prelievi *cardless* disconosciuti che sono avvenuti con la corretta digitazione dei codici OTS tramessi via sms al cellulare della ricorrente che, evidentemente, ha dettato a voce al *phisher* al telefono il relativo codice univoco necessario per finalizzare le singole operazioni di prelievo.
Tale conclusione viene confermata proprio dalle dichiarazioni in denuncia della ricorrente che ammette di essere stata contattata il 29.09.2020 alle ore 15:13 e la mattina del 3.10.2020.
Ciò posto, ritiene perfettamente applicabile alla fattispecie quanto sostenuto dal Collegio di Coordinamento (decisione n. 22745/2019) in tema di ripartizione dell'onere probatorio, laddove si stabilisce che *"…in merito alla colpa grave dell'utente, il Collegio [può] comunque affermarne l'accertamento se palesemente emergente dalle dichiarazioni rese dal ricorrente in sede di denuncia all'autorità giudiziaria e/o nel ricorso".* Sul punto, richiama altresì delle recenti decisioni dei Collegio ABF (tra cui la decisione n. 14760/20 del Collegio di Bologna; la n. 15139/2020 del Collegio di Roma) ove esaminando casi analoghi a quello oggetto di ricorso i Collegi hanno reputato provata la colpa grave dei ricorrenti.
In merito alla richiesta di rimborso delle spese di lite ricorda l'ormai consolidato orientamento dei Collegi che ha escluso la ripetibilità delle spese legali per la mancanza della prova di aver effettivamente sostenuto gli oneri di cui si intende richiedere il ristoro e

per la non complessità della materia, che rende il ricorso all'assistenza professionale dell'avvocato una scelta autonoma del ricorrente.
In conclusione, ribadisce la correttezza delle determinazioni assunte in precedenza in ordine alla richiesta di rimborso della ricorrente, non potendo ricadere sull'intermediario le conseguenze di operazioni fraudolente determinatesi per comportamenti poco prudenti della clientela.
Chiede pertanto al Collegio di non accogliere il ricorso o di riconoscere tra le parti l'esistenza di un concorso di colpa ai sensi dell'art. 1227 c.c.

DIRITTO

La domanda della ricorrente è relativa all'accertamento del proprio diritto ad ottenere dall' intermediario il rimborso di somme sottrattegli da ignoti mediante l'utilizzo fraudolento delle proprie credenziali di utilizzo del conto corrente *online* di cui la stessa è titolare presso lo stesso intermediario.
La materia, come noto, è regolata, oltre che dalle norme generali in tema di adempimento delle obbligazioni e sulla diligenza del mandatario (art. 1710 c.c.) e della banca nell' "esecuzione degli incarichi" (art. 1852 c.c.), dal d. lgs. n. 11/2010 il quale – al fine di favorire il corretto uso di strumenti di pagamenti diversi dal contante – impone una serie di obblighi tanto in capo all'utilizzatore, quanto in capo all'emittente.
In particolare, l'art. 7 impone che il primo utilizzi siffatti strumenti, conformemente alle prescrizioni contrattuali, in modo diligente, adottando misure idonee a garantire la sicurezza dei dispositivi personalizzati che ne consentono l'utilizzo. Inoltre, l'art. 9 stabilisce l'obbligo da parte dell'utilizzatore avvedutosi di un'operazione fraudolenta di darne tempestivo avviso al prestatore dei servizi, mentre l'art. 12, comma 2, esonera da responsabilità, salvo il caso in cui abbia agito fraudolentemente, l'utilizzatore di uno strumento di pagamento, smarrito, sottratto o utilizzato indebitamente, nel caso in cui il prestatore di servizi di pagamento non abbia assicurato la piena fruibilità di strumenti atti consentire all'utilizzatore di comunicare senza indugio allo stesso prestatore l'utilizzo indebito dello strumento di pagamento.
Corrispondentemente, l'art. 8 impone a quest'ultimo di predisporre sistemi di sicurezza che non consentano l'accesso da parte di terzi ai dispositivi personali dell'utilizzatore e di impedire l'uso degli strumenti di pagamento successivamente alla comunicazione ricevuta dal cliente ai sensi del citato art. 9.
La normativa stabilisce la responsabilità dell'intermediario ove quest'ultimo non abbia predisposto un sistema di autenticazione forte. Tale tipologia di autenticazione viene declinata nell'art. 1, lettere q) e q-bis), del d. lgs. ("Definizioni") ove si definisce per "autenticazione": "la procedura che consente al prestatore di servizi di pagamento di verificare l'identità di un utente di servizi di pagamento o la validità dell'uso di uno specifico strumento di pagamento, incluse le relative credenziali di sicurezza personalizzate fornite dal prestatore (lettera q)"; per "autenticazione forte del cliente": "un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione (lettera qbis)". La predetta definizione di autenticazione forte è ribadita dagli Orientamenti finali sulla sicurezza via internet emanati dall'EBA.

L'evidente disparità di posizioni che le norme suddette comportano nei rapporti fra fornitore ed utente dei servizi di pagamento trova una giustificazione di natura sia sociale, sia commerciale, riconducibile al rischio, ossia all'idea secondo la quale è ragionevole far gravare i rischi statisticamente prevedibili legati ad attività oggettivamente "pericolose" che interessano una vasta platea di consumatori o di utenti, sull'impresa in quanto quest'ultima è in grado di distribuire su una moltitudine di utenti il rischio dell'impiego fraudolento di carte di credito, di strumenti di pagamento, di conti correnti *online*, evitando che gravi direttamente ed esclusivamente sul singolo pagatore (sul punto v. ABF, Collegio di Coordinamento, nn. 6168/2013 e 3498/2012; recentemente, Collegio di Napoli, n. 1091/2018 e 10188/2018).
Peraltro, la concreta applicazione del principio non può prescindere da un'esatta delimitazione delle rispettive sfere di responsabilità del prestatore e dell'utilizzatore del servizio di pagamento.
Occorre, infatti, verificare, da una parte, se il fornitore abbia adottato tutti i migliori accorgimenti della tecnica per scongiurare tali impieghi fraudolenti, dall'altra, se l'eventuale negligenza del titolare dello strumento di pagamento sia tale da ricadere o meno nella nozione di colpa grave al cui ricorrere il summenzionato art. 12 d. lgs. n. 11/2010, esclude ogni responsabilità dell'intermediario.
Al fine di bilanciare le diverse posizioni, ed in ragione del rischio d'impresa riconosciuto in capo al prestatore dei servizi di pagamento, la normativa de qua prevede, come si è detto, una diversa distribuzione degli oneri probatori, in caso di furto o smarrimento degli strumenti di pagamento, con l'obiettivo di attribuire la responsabilità degli utilizzi fraudolenti all'impresa, nel caso in cui essi non siano stati cagionati da dolo o colpa grave del cliente.
Come si è visto, la controversia in esame concerne nr. 3 prelievi ATM cardless di un importo complessivo di € 5.000,00 che la ricorrente afferma essere stati fraudolentemente eseguiti da terzi tra il 2 e il 3 ottobre 2020.
Dalla documentazione acclusa agli atti sembra emergere con chiarezza che la ricorrente è stata vittima di un episodio di *vishing*, originato in particolare da due telefonate ricevute il 29 settembre e il 3 ottobre apparentemente provenienti dall'intermediario.
Nel corso della prima telefonata il sedicente operatore della banca le avrebbe chiesto di disinstallare l'applicazione dell'intermediario, per aggiornamenti in corso. Successivamente, il 3 ottobre, lo stesso operatore le avrebbe chiesto di procedere alla installazione della applicazione mobile. Riguardo a tale telefonata, la stessa ricorrente riferisce che sul suo smartphone le è apparso l'avviso di un prelievo di € 2.000,00, a seguito del quale l'operatore ha interrotto la comunicazione.
Dalle tracciature prodotte dall'intermediario si rilevano le disposizioni impartite dal My Key della Cliente che hanno portato in data 2 e 3 ottobre ai prelievi *cardless* disconosciuti, che sono avvenuti con la corretta digitazione dei codici OTS tramessi via sms al cellulare della ricorrente. Sotto questo profilo, il Collegio ritiene pertanto che siano stati addotti elementi di fatto circa le modalità esecutive dell'operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente, secondo quanto indicato nella decisione del Coll. di Coordinamento n. 22745/2019. Il Collegio reputa dunque che l'istante è rimasta vittima di una colpevole credulità: colpevole in quanto ella è stata portata a comunicare le proprie credenziali di autenticazione al di fuori del circuito operativo dell'intermediario e tanto più colpevole si rivela quell'atto di ingenuità, quanto più si consideri che tali forme di "accalappiamento" possono dirsi ormai note al pur non espertissimo navigatore di Internet (cfr. Collegio di Coordinamento, n. 3498/2012). Onde, l'intrusione non autorizzata nel sistema appare ascrivibile anche a colpa grave del cliente, con conseguente utilizzo abusivo delle sue credenziali di accesso.

Tuttavia, dalla stessa documentazione agli atti emerge pure che il sistema di sicurezza predisposto dall'intermediario ed utilizzato nella vicenda in esame ha contemplato l'utilizzo dell'OTS (One Time SMS). Un siffatto presidio di sicurezza informatica, alla luce della vigente normativa e dell'orientamento condiviso dei Collegi territoriali ABF (Coll. Napoli, 306/2021; Coll. Bari n. 1686/2021; Coll. Torino, n. 23256/2020) non risulta adeguato: si tratta infatti di una password dinamica supplementare inviata sullo stesso canale già adoperato per l'invio di quella di base, sicché, compromesso potenzialmente quel canale, il suo riutilizzo non assicura alcuna protezione rafforzata.
Invero, un punto cruciale nella definizione dei sistemi di sicurezza è costituito dall'indipendenza dei diversi fattori; anche gli RTS dell'EBA stabiliscono che gli elementi dell'autenticazione forte devono essere indipendenti fra loro, in modo tale che la violazione di uno di essi non comprometta l'affidabilità degli altri (cfr. in particolare l'art. 9 del Regolamento delegato n. 2018/389).
Pertanto, anche in capo alla convenuta rinviene il Collegio profili di responsabilità. Per quanto esposto, la gradazione delle rispettive responsabilità al 50% è quella ritenuta equa nel caso di specie dal Collegio.
Merita accoglimento anche la richiesta della ricorrente del rimborso delle spese legali: è, infatti, orientamento di questo Collegio (cfr. ABF Napoli, 3498/2012) che, là dove sia dimostrato che la parte ricorrente si sia avvalsa, nell'intero snodo procedimentale che va dal reclamo al ricorso, dell'ausilio di un difensore sopportandone il relativo costo, quest'ultimo possa e debba prendersi in considerazione quale componente del più ampio pregiudizio patito dalla parte ricorrente, che questo Collegio determina equitativamente in euro 200,00.

P.Q.M.

In parziale accoglimento del ricorso, il Collegio dichiara l'intermediario tenuto al risarcimento del danno per l'importo di € 2.500,00 oltre interessi legali dalla data del reclamo.
Il Collegio dispone altresì il ristoro delle spese di assistenza difensiva nella misura equitativamente determinata in € 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