Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) TINA	Membro designato dalla Banca d'Italia
(MI) PEDERZOLI	Membro designato dalla Banca d'Italia
(MI) DALMARTELLO	Membro di designazione rappresentativa degli intermediari
(MI) DI NELLA	Membro di designazione rappresentativa dei clienti

Relatore ANDREA DALMARTELLO

Seduta del 18/01/2022

Esame del ricorso n. 1140265 del 30/07/2021

proposto da

nei confronti di 3475 - ING BANK N.V.

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) TINA	Membro designato dalla Banca d'Italia
(MI) PEDERZOLI	Membro designato dalla Banca d'Italia
(MI) DALMARTELLO	Membro di designazione rappresentativa degli intermediari
(MI) DI NELLA	Membro di designazione rappresentativa dei clienti

Relatore ANDREA DALMARTELLO

Seduta del 18/01/2022

FATTO

Il ricorrente afferma che:
- il 19.04.21 ha effettuato un bonifico per €15.000, che tuttavia il 21.04.21 non risultava ancora pervenuto alla banca beneficiaria.
- alle 11.43 di tal giorno ha ricevuto un sms dall'intermediario con cui veniva segnalato il blocco del suo conto corrente e, per procedere alla riattivazione dello stesso, lo si invitava a cliccare sul link presente nel messaggio.
- poiché il messaggio proveniva dal medesimo numero con cui solitamente giungevano le comunicazioni dell'intermediario, il ricorrente ha cliccato sul link.
- si era, così, aperta una schermata del tutto uguale a quella della banca, sicché vi inseriva il proprio codice cliente.
- alle 14.23 è stato contattato telefonicamente, con l'utenza 347***427 da un soggetto che si è qualificato come operatore della banca e lo ha informato che il suo conto corrente era stato bloccato a seguito di bonifici sospetti, sicché il bonifico del 19 aprile era stato annullato.
- su richiesta dell'operatore, il ricorrente ha provveduto a rimuovere l'applicazione della banca.
- il 21 e il 23 aprile il ricorrente ha ricevuto alcuni sms dall'intermediario con cui si comunicava l'esecuzione di bonifici.
- il 23.04.21 il sedicente operatore ha contattato più volte il cliente tramite whatsapp e

telefonicamente gli ha spiegato che tali sms ed e-mail venivano inviati automaticamente dal sistema ma non essendo bonifici autorizzati sarebbero stati respinti.
- il 26 aprile ha ricevuto ulteriori 21 e-mail di richieste di bonifici. Immediatamente il sedicente operatore ha contattato nuovamente il cliente e tali chiamate risultavano provenienti dal numero telefonico ***789, riconducibile al servizio clienti della banca.
- su richiesta del cliente, l'operatore ha inviato tramite whatsapp la contabile relativa al bonifico di € 15.000 comunicando che dal giorno successivo il conto sarebbe tornato operativo.
- il 27/28 aprile il finto operatore ha rassicurato di nuovo il cliente, per poi interrompere le comunicazioni.
- il 29 aprile il ricorrente ha contattato il servizio clienti ed ha scoperto che il conto risultava completamente svuotato "e con poste a debito".
- il giorno seguente il cliente ha bloccato il conto ed ha scoperto che erano stati eseguiti 24 bonifici non autorizzati per complessivi € 33.563,26 ed ha presentato denuncia.
Pertanto, il ricorrente il rimborso dell'importo pari a € 33.563,26, oltre interessi dal giorno della domanda e spese legali.
L'intermediario, nelle controdeduzioni, ha puntualizzato che:
- dalla prospettazione dei fatti offerta dal cliente è evidente che, senza la inconsapevole quanto colpevole collaborazione del cliente, nessuna frode avrebbe potuto essere compiuta;
- la banca ha adottato un sistema di autenticazione forte di accesso all'Area Riservata e di autorizzazione delle disposizioni di pagamento, nel rispetto delle previsioni normative.
- in particolare, per poter accedere all'area riservata, occorre inserire "inizialmente" in due sessioni separate prima il codice cliente e la data di nascita poi il codice segreto PIN (modificabile dal cliente). In seguito, il cliente deve autorizzare l'accesso mediante il servizio Token, che genera tramite App del codice token mediante l'utilizzo del codice numerico di sei cifre (c.d. smart code) impostato dal cliente o, in alternativa e a scelta del cliente, tramite uso di impronta digitale o altri dati biometrici;
- a questo punto, il cliente visualizza sul proprio dispositivo una notifica push per finalizzare l'accesso;
- ciascuna operazione è stata effettuata tramite autenticazione forte, quando ormai il frodatore era in possesso di tutte le credenziali necessarie. Dopo avere effettuato l'accesso all'area riservata del cliente, il frodatore ha impartito le disposizioni contestate e ha proceduto alla relativa autorizzazione con doppio fattore.
- dai log risulta la corretta esecuzione di ciascun bonifico intervenuto dunque senza anomalie tecniche, nonché l'invio da parte della Banca di appositi alert.
- quanto al contegno del cliente, dalle evidenze in possesso della Banca deve ritenersi che il contatto con il truffatore sia avvenuto, come indicato peraltro nel ricorso, prima dell'esecuzione dell'operazione e che vi sia stata una cooperazione colpevole tra il cliente e il truffatore
- risulta infatti che alle 14.27 del 21 aprile 2021, sia stata richiesta l'attivazione del Token, necessario per impartire la disposizione di bonifico, su un altro dispositivo, mentre la prima disposizione di bonifico è stata impartita alle ore 14.32.
- per richiedere l'attivazione del Token su un nuovo dispositivo è indispensabile disporre anche del vecchio supporto. Il cambio di dispositivo token avviene infatti tramite Strong Customer Authentication.
- occorre a tal fine accedere tramite app sul nuovo dispositivo con l'inserimento di Codice Cliente, data di nascita e Codice PIN. L'APP richiede se si vuole attivare il Token su un nuovo dispositivo e viene inviato un sms OTP sul recapito telefonico registrato sull'anagrafica, di cui l'app richiede l'inserimento unitamente alla domanda di sicurezza.

Detti dati sono stati necessariamente forniti dal cliente.
- il cliente avrebbe dovuto dubitare dell'autenticità delle comunicazioni, considerato che il link indicato nel sms civetta non ha nulla a che vedere con gli indirizzi istituzionali della banca; inoltre: i) l'utenza 347***427 non i riferibile all'istituto; ii) le comunicazioni via whatsapp risultavano anomale e persino incongruenti rispetto alle prospettazioni del frodatore; iii) la rimozione dell'APP e del token può essere avvenuta solo comunicando al truffatore le proprie credenziali e l'OTP; iv) ha ricevuto vari sms ed e-mail alert, che tuttavia ha ignorato, così come il codice per modificare il device su cui era attivato il token.
- non rileva, e non risulta peraltro provato, che il truffatore il 26.4.21 abbia contattato il cliente da un numero riferibile alla banca, dato che la truffa era già stata perfezionata.
Di conseguenza, l'intermediario chiede il rigetto delle pretese avversarie.
Nel replicare alle controdeduzioni, la parte ricorrente contesta le allegazioni avversarie, rimarcando l'assenza di idonea documentazione a supporto di esse. Insiste inoltre sulla particolare sofisticatezza della truffa subita. Nelle controrepliche, l'intermediario ha in sostanza insistito sulle proprie difese già illustrate nelle controdeduzioni.

DIRITTO

Le operazioni contestate sono disciplinate 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. Devono in particolare essere richiamati gli artt. 7, 10 e 12 del citato decreto: disposizioni che, con l'obiettivo dichiarato di tutelare l'utente, allocano in via tendenziale sull'intermediario il rischio di utilizzazione fraudolenta degli strumenti di pagamento. Più precisamente, l'art. 12 d. lgs. n. 11/2010 regola il regime della responsabilità dell'intermediario per l'utilizzo non autorizzato dall'utente di strumenti e servizi di pagamento. La disposizione ascrive la responsabilità in capo al prestatore dei servizi di pagamento in tutte le ipotesi di uso non autorizzato, a meno che non vi sia evidenza della frode dell'utente ovvero del dolo o della colpa grave di quest'ultimo nell'adempiere gli obblighi di cui all'art. 7 (ossia, gli obblighi di custodia e di corretta utilizzazione dello strumento di pagamento). In coerenza con la segnalata finalità di tutela dell'utente, l'art. 10 alloca sull'intermediario l'onere di 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*", precisando, al secondo comma, che "*l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utilizzatore medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'articolo 7*", gravando sull'intermediario "*la prova della frode, del dolo o della colpa grave dell'utente*". Da questo complesso di disposizioni si ricava, come chiarito dal Collegio di Coordinamento (dec. n. 22745/2019), che, per un verso, è onere dell'utente il solo disconoscimento dell'operazione di pagamento non autorizzata, mentre, per non incorrere nella responsabilità di cui all'art. 12 va tenuto conto del principio interpretativo secondo il quale "*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".

Venendo ai fatti oggetto del ricorso, il ricorrente disconosce ventiquattro operazioni di pagamento, eseguite tra il 21 e il 26 aprile 2021. Si tratta in particolare di tre bonifici pari a € 5.000,00 ciascuno, eseguiti il 21 e il 23.4 e di 21 bonifici di € 922,25 ciascuno, tutti eseguiti il 26.4.

Occorre, anzitutto, prendere in considerazione la documentazione prodotta dall'intermediario relativa all'autenticazione dell'operazione.

Il sistema di autenticazione delle operazioni di pagamento adottato dall'intermediario è conforme a quanto richiede l'art. 10 *bis* del d.lgs. n. 11/2010, in base al quale "*i prestatori di servizi di pagamento applicano l'autenticazione forte del cliente*". L'autenticazione forte consiste in "*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*" (art. 1, comma 1, lett. q-bis, d.lgs. n. 11/2010).

Più precisamente, con riferimento ai bonifici, il sistema dell'intermediario richiede, per accedere all'area riservata, l'inserimento, in sessioni separate sul sito della banca, del codice cliente, della data di nascita e di un codice PIN statico (elementi di conoscenza). Successivamente, il cliente, al fine di autorizzare le operazioni di pagamento, deve attivare il *token*, mediante la *app* accoppiata al proprio *device* (elemento di possesso), che richiede l'inserimento di un ulteriore codice *token* (elemento di conoscenza) o, se tecnologicamente possibile, dei dati biometrici (elemento di inerenza). Si osserva altresì che le operazioni sono state precedute dall'*enrollement* della *app* su un nuovo dispositivo, per effettuare il quale è necessario inserire codice cliente, data di nascita, pin statico e codice OTS che l'intermediario invia al *device* precedentemente certificato dal cliente.

A dimostrazione della corretta autenticazione delle operazioni contestate, l'intermediario resistente ha prodotto evidenza del *log*, ossia della tracciatura informatica relativa sia all'accesso al sito di *home banking*, sia all'*enrollment* della *app* su nuovo *device*, che al primo bonifico di € 5.000,00.

Il Collegio ritiene che non possa costituire una valida dimostrazione della concreta applicazione della SCA l'affermazione dell'intermediario, in virtù della quale le operazioni successive alla prima sarebbero state autorizzate allo stesso modo. Incombendo sull'intermediario un preciso onere probatorio, questi è chiamato ad assolverlo con precisione e completezza, senza che possa costituire un valido sostituto della documentazione informatica un generico riferimento alla somiglianza di essa per tutte le operazioni oggetto di ricorso.

In assenza della dimostrazione della corretta autenticazione forte (artt. 10, 10-*bis* e 12, comma 2-*bis*, d.lgs. n. 11/2010) e salva la dimostrazione dell'agire fraudolento del pagatore (nel caso di specie assente), il rischio di operazioni di pagamento disconosciute da quest'ultimo, a seguito di smarrimento o furto dello strumento di pagamento, deve essere integralmente sopportato dal prestatore del servizio di pagamento.

Pertanto, devono essere rimborsati, ai sensi del citato art. 12, comma 2-*bis,* i due bonifici eseguiti in data 23.4 per complessivi € 10.000,00 e le restanti 21 operazioni del 26.4 per complessivi € 28.563,00.

In relazione alla prima operazione del 21.4 occorre ricordare che, come sottolineato dal Collegio di Coordinamento (dec. n. 22745/2019), "*la semplice produzione in giudizio del "log informatico" relativo all'operazione contestata non è sufficiente perché possa considerarsi assolto l'onere probatorio posto a carico dell'intermediario ai sensi del comma*

2 della norma, richiedendosi che il PSP alleghi specifiche deduzioni su fatti e circostanze riguardanti la fase esecutiva dell'operazione stessa in modo da consentire al Collegio di accertare l'eventuale responsabilità dell'utente nel compimento dell'operazione contestata". Nel caso di specie, il Collegio rileva la sussistenza di tali circostanze riguardanti la fase esecutiva delle due operazioni in discorso.

Risulta sempre dalle scarne spiegazioni dei *log* fornite dall'intermediario, confermate dagli sms ricevuti dal ricorrente agli atti, che il pagamento sia stato correttamente eseguito a seguito di *enrollment* della app sul *device* dei malfattori, mediante comunicazione a questi ultimi dei codici necessari e, in particolare, dell'OTP ricevuto dal ricorrente sul proprio cellulare.

Benché la nota esplicativa versata in atti non risulti particolarmente chiara, si evince da essa l'inserimento dei fattori di autenticazione sia per l'accesso al sito, che per l'esecuzione dell'operazione.

È inoltre confermato dalla denuncia e dai fatti allegati al ricorso che il ricorrente abbia comunicato all'operatore i codici necessari per effettuare l'*enrollment* del dispositivo sul nuovo *device* e per autorizzare le operazioni correttamente autenticate con SCA.

Queste circostanze sono idonee a comprovare la colpa grave del ricorrente, tale da escludere che l'intermediario sia tenuto *ex* art. 12, comma 3, d.lgs. n. 11/2010 a restituire gli importi oggetto dell'operazione disconosciuta in discorso (ferma restando l'obbligo di restituire gli importi sopra indicati ex art. 12, comma 2-*bis*).

Né è idonea a escludere la concreta dimostrazione della colpa grave del ricorrente la particolare insidiosità della truffa perpetrata ai suoi danni, in altri casi pure ritenuta, anche da questo Arbitro, tale da neutralizzare la grave negligenza del comportamento del cliente che abbia comunicato a terzi le proprie credenziali (v. ad es. Coll. Torino, decc. nn. 11712/2021; 10044/2021). Anzitutto, occorre considerare che, lo sms ricevuto conteneva un *link* non riferibile all'intermediario e la successiva telefonata non proveniva da un'utenza telefonica che potesse apparire ufficiale. Inoltre, il ricorrente ha ricevuto un sms contenente il codice OTP necessario per installare la app sul nuovo device e ne ha ignorato gli avvertimenti.

Di conseguenza, alla luce delle precedenti considerazioni, il ricorso può trovare accoglimento solo parziale. Sono altresì dovuti gli interessi dal reclamo al saldo.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 28.563,00, oltre interessi dal reclamo al saldo.

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 alla parte ricorrente la somma di € 20,00, quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
FLAVIO LAPERTOSA