Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI ROMA

composto dai signori:

(RM) GRECO	Presidente
(RM) PAGLIETTI	Membro designato dalla Banca d'Italia
(RM) ACCETTELLA	Membro designato dalla Banca d'Italia
(RM) GULLO	Membro di designazione rappresentativa degli intermediari
(RM) CESARO	Membro di designazione rappresentativa dei clienti

Relatore VINCENZO MARIA CESARO

Seduta del 20/12/2019

FATTO

Nel ricorso, depositato in data 29.08.2019, l'istante chiede la restituzione della somma di euro 34.676,82 (oltre "alla refusione delle anticipazioni"), corrispondente all'importo di due bonifici disconosciuti, eseguiti fraudolentemente da terzi non autorizzati, in seguito a clonazione della sua Sim card.
In particolare, il ricorrente deduce che, dopo avere invano tentato di connettersi all'home banking dal proprio portatile, ha scoperto, soltanto in data 1° giugno 2019, che l'accesso al conto risultava bloccato a partire dal 15 maggio 2019 a seguito di una frode realizzata a suo danno da parte di terzi che avevano effettuato n. 2 bonifici fraudolenti verso l'estero per un importo complessivo di euro 34.676,82. Le operazioni in questione sarebbero state ordinate tramite un cellulare "utilizzando l'applicazione mobile della banca o comunque il browser di un dispositivo cellulare" con utilizzo di password dinamiche fornite dalla resistente tramite sms.
Rilevato che nella propria scheda cliente risultava inserito, quale numero di telefono principale, un'utenza sconosciuta e appreso che, in considerazione della natura sospetta delle operazioni, l'intermediario avrebbe tentato, senza successo, di bloccarle e di contattare il ricorrente al numero di cellulare, per informarlo, l'istante ha ricollegato l'accadimento al fatto che, lo stesso giorno in cui risultano effettuate le operazioni

fraudolente, si era verificata una disattivazione della propria utenza telefonica, la cui corretta funzionalità era stata ripristinata solo il giorno dopo.
Contattato il gestore telefonico quest'ultimo confermava che, in data 15 maggio 2019 alle ore 13:10, la Sim in uso al ricorrente veniva sostituita con causale "sostituzione furto/smarrimento" e il relativo numero migrava su altra Sim card.
Ritenendo, quindi, di essere stato vittima di una frode, il ricorrente sporgeva denuncia alle forze dell'ordine e presentava formale reclamo riscontrato negativamente dall'intermediario.
Parte attrice censura la condotta della resistente che avrebbe omesso di considerare quali indici sintomatici di un'attività truffaldina: i) l'inserimento di un numero telefonico diverso; l'accesso al portale home banking per la prima volta tramite un'applicazione mobile o un browser diverso dal computer fino a quel momento utilizzato dal ricorrente; ii) l'attivazione del servizio di OTP tramite sms in luogo dell'utilizzo del token fisico; iii) la disposizione di due bonifici di importo rilevante a fronte di un'attività storica del conto del tutto ordinaria - aggravata dal fatto che i predetti indici si manifestavano nell'arco di poche ore.
L'istante rileva, inoltre, che il blocco non è stato comunicato né sul numero di rete fissa, né tramite mail.
Nelle controdeduzioni l'intermediario rileva di avere adottato un sistema di autenticazione "a due fattori", che richiede l'inserimento delle credenziali di accesso per effettuare il login (numero cliente + Pin) e necessita del Pin e dell'OTP per disporre le singole operazioni.
Esso è pacificamente riconosciuto come sistema "forte" dai Collegi Abf (cfr. decisione n. 5565/2019), e deve presumersi, non rilevandosi anomalie di sistema, che ci sia stata una negligenza del cliente nella custodia delle credenziali necessarie ad utilizzare i servizi di pagamento. Allega a riprova copia dei Log riferiti alla giornata del 15 maggio 2019 dai quali si ricava il corretto inserimento di "Login name" e password necessari per l'autorizzazione delle disposizioni.
La banca allega, altresì, evidenza attestante la consegna, il giorno 15 maggio 2019 tra le ore 13:30 e le ore 14:17, al numero del ricorrente di n. 2 messaggi relativi all'attivazione del mobile token, con il quale sono stati generati i codici OTP necessari per autorizzare i bonifici, e n. 2 messaggi relativi all'inserimento di bonifici, precisando che opportunamente il motore antifrode, avendo intercettato le due operazioni di importo rilevante e ravvicinate nel tempo, ha innescato il blocco delle credenziali di accesso del ricorrente.
Nelle repliche, parte ricorrente afferma che il sistema di autenticazione forte avrebbe dovuto essere attivo non solo per le singole operazioni dispositive ma anche per accedere all'area riservata del cliente laddove invece, al momento dei fatti, per accedere all'area clienti era sufficiente inserire il nome utente e la password acquisendo così tutte le informazioni relative alla posizione del ricorrente, il che – secondo parte attrice – avrebbe consentito ai criminali di farsi scaricare dal Call center della resistente l'App che ha generato la one time password procedendo ai due bonifici e consumando, quindi, la truffa.
Nelle controrepliche, la resistente richiama quanto affermato in sede di controdeduzioni e ribadisce che solo il comportamento incauto del cliente, che ha permesso a terzi di conoscere le proprie credenziali di accesso al sito e all'App, ha consentito il perpetrarsi della frode, affermando inoltre che quanto indicato nelle repliche circa le modalità con cui l'App sarebbe stata scaricata non corrisponde al vero poiché l'App è scaricata in autonomia dal cliente riconosciuto in base alle credenziali riservate di cui solo lui è in possesso senza alcun intervento del Call center o della banca in generale.

DIRITTO

Le operazioni contestate sono state effettuate sotto la vigenza del d.lgs. 11/2010, così come modificato dal d.lgs. 218/2017, che ha recepito la nuova Direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015 (c.d. PSD 2). L'art. 12 del D.Lgs. n. 11 del 2010, così come successivamente modificato dal D.Lgs. n. 218/2017 ("Responsabilità del pagatore per l'utilizzo non autorizzato di strumenti o servizi di pagamento"), prevede che: "2-bis. Salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente. Il beneficiario o il prestatore di servizi di pagamento del beneficiario rimborsano il danno finanziario causato al prestatore di servizi di pagamento del pagatore se non accettano l'autenticazione forte del cliente. […] 4. Qualora abbia agito in modo fraudolento o non abbia adempiuto ad uno o più obblighi di cui all'articolo 7, con dolo o colpa grave, l'utente sopporta tutte le perdite derivanti da operazioni di pagamento non autorizzate".

La nuova normativa stabilisce, pertanto, 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 q-bis)". Tale definizione di autenticazione forte è ribadita dagli Orientamenti finali sulla sicurezza via internet emanati dall'EBA.

Già alla luce della previgente formulazione dell'art. 12 si era ritenuto che, trattandosi di un fatto impeditivo dell'esercizio del diritto risarcitorio da parte del ricorrente, l'onere di provare la colpa grave (o addirittura il dolo) di quest'ultima gravasse sull'intermediario resistente, ai sensi dell'art. 2697, 2° comma, c.c. Tale soluzione è stata espressamente affermata dal Collegio di Coordinamento di questo Arbitro nella decisione n. 5304 del 17 ottobre 2013. Secondo la giurisprudenza di legittimità, la colpa grave è costituita da una "straordinaria e inescusabile" imprudenza, negligenza o imperizia, la quale presuppone che sia stata violata non solo la diligenza ordinaria del buon padre di famiglia di cui all'art. 1176, 1° comma, c.c., ma anche "quel grado minimo ed elementare di diligenza generalmente osservato da tutti" (Cass., 3 maggio 2011, n. 913; Cass., 19 novembre 2001, n. 14456). Questo Arbitro si è costantemente richiamato a tale orientamento giurisprudenziale, com'è stato ribadito dalla già richiamata decisione del Collegio di Coordinamento n. 5304 nonché dalla decisione n. 6168 del 2013.

L'onere di provare la colpa grave (o addirittura il dolo) della parte ricorrente da parte dell'intermediario resistente è esplicitamente affermato dal disposto dell'art. 10, 2° comma, del D.lgs. n. 11 del 2010, così come modificato dal D.Lgs. n. 218/2017, il quale statuisce che "quando l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento eseguita, l'utilizzazione di uno strumento di pagamento registrato dal prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utente 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'art. 7. È onere del prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, fornire la prova della frode, del dolo o della colpa grave dell'utente".

Il Collegio di Coordinamento, con la decisione n. 8553 del 28 marzo 2019, nell'esaminare la specifica questione della portata del comma 2-ter dell'art 12, introdotto dal D.Lgs. n. 218/2017, ha affermato più in generale che "il d.lgs. 15 dicembre 2017, n. 218 non modifica il regime della responsabilità né quello probatorio precedentemente applicati" osservando che "… resta invariato il principio secondo cui la responsabilità dell'utente non sussiste, salvo che nelle ipotesi in cui si accerti che egli abbia 'agito in modo fraudolento o non abbia adempiuto a uno o più degli obblighi di cui all'art. 7, con dolo o colpa grave' (art. 12, comma 3)".

Richiamata la disciplina applicabile, il Collegio ritiene il presente ricorso fondato atteso che l'intermediario non ha fornito adeguata prova della colpa grave di parte ricorrente.

Nel caso di specie, il ricorrente risulta vittima della truffa denominata sim swap fraud, la quale consiste in un furto di identità tramite captazione dei dati di accesso relativi al conto home banking e conseguente sostituzione/contraffazione della sim card telefonica. La frode ha avuto, dunque, luogo mediante un intervento sul numero di cellulare sul quale si fonda il sistema di autenticazione delle operazioni tramite home banking. La sostituzione della sim card consente di fatto un aggiramento del sistema di autenticazione a doppio fattore, poiché il cd. codice OTP (one time password) viene ricevuto da chi ha fraudolentemente carpito l'identità telefonica, ottenendo una nuova sim, attiva e funzionante.

Dalle circostanze dedotte non può certo ravvisarsi una colpa grave del cliente per la captazione degli OTP.

Per quanto riguarda le credenziali statiche di accesso (codice cliente e password) non si è ricostruito come potessero essere conosciute da persone diverse dal titolare, ma come è noto le tecniche di acquisizione dei codici identificativi personali sono sempre più sofisticate e tali da rendere possibile l'acquisizione di tali dati da parte di terzi a prescindere da qualsiasi forma di negligenza del titolare, potendo essere carpiti dagli archivi delle banche, come pure dalle reti telematiche sulle quali transitano i flussi di informazioni (cfr. in questo senso Collegio di Roma, n. 8144/2014 e n. 82/2012 e Collegio di Milano n. 7440/2019).

Non può pertanto escludersi - né, da tale punto di vista, le affermazioni dell'intermediario appaiono dotate del necessario grado di fondatezza ai fini dell'assolvimento dell'onere della prova ex art. 2697 c.c. - che le credenziali statiche della carta siano state acquisite dal terzo frodatore con modalità indipendenti da profili di colpa grave a carico del ricorrente (cfr. art. 10, comma 2, D.Lgs. n. 11 del 2010).

PER QUESTI MOTIVI

Il Collegio, in accoglimento del ricorso, dispone che l'intermediario corrisponda alla parte ricorrente la somma di euro 34.676,82.

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
FERNANDO GRECO