COLLEGIO DI NAPOLI

composto dai signori:

(NA) CARRIERO	Presidente
(NA) CONTE	Membro designato dalla Banca d'Italia
(NA) PATRONI GRIFFI	Membro designato dalla Banca d'Italia
(NA) RISPOLI FARINA	Membro designato da Associazione rappresentativa degli intermediari
(NA) BARENGHI	Membro designato da Associazione rappresentativa dei clienti

Relatore RISPOLI FARINA MARILENA

Nella seduta del 25/02/2014 dopo aver esaminato:

- il ricorso e la documentazione allegata
- le controdeduzioni dell'intermediario e la relativa documentazione
- la relazione della Segreteria tecnica

FATTO

In data 23/5/2013, i ricorrenti, titolari presso la banca resistente di un conto corrente con annesso servizio di *home banking*, venivano contattati da un responsabile della filiale di riferimento che riferiva loro di una disposizione sospetta impartita *on line*, cui era stata data comunque esecuzione. Si trattava di un bonifico per € 2.479,76 effettuato in favore di uno sconosciuto, intestatario di un conto di moneta elettronica in essere presso un IMEL.
L'operazione fraudolenta veniva denunciata alla competente Autorità di polizia già nella giornata del 24/5/2013: richiesto pure il rimborso dell'importo sottratto, la banca comunicava l'11 luglio 2013 di non potere accogliere l'istanza, soggiungendo di ritenere che "non siano stati adeguatamente custoditi i dispositivi di identificazione".
In sede di ricorso, i ricorrenti dichiarano di avere sempre custodito – impedendone l'accesso a terzi – i dispositivi di identificazione per l'accesso al canale internet; che non è imputabile loro alcuna colpa grave o mancanza di diligenza; che verosimilmente "chi ha effettuato l'operazione fraudolenta ha utilizzato sistemi informatici sofisticati, entrando illegalmente e provvisoriamente nel conto corrente dei ricorrenti"; che viceversa risultava gravemente colposa la condotta della banca, la quale aveva avuto immediata

consapevolezza della "abnormità" dell'operazione e, ciò nondimeno, vi aveva dato esecuzione.
La banca resistente ha innanzitutto precisato di potere fornire solo considerazioni di carattere induttivo sui fatti denunciati, posto che il ricorrente – anche in sede di denuncia - non aveva inteso fornire alcun elemento volto a chiarire la dinamica della truffa subita. In tal senso, soggiunge la scrivente, assume rilievo il fatto che il ricorrente "per l'operatività su internet poteva disporre [recte: disponeva] del token – un congegno in grado di generare mutevoli password monouso dalla durata limitata a poche decine di secondi e privo di ogni collegamento al WEB – che, pertanto, aggiungendosi alla password nota solo all'utente, forma un sistema di autenticazione a due fattori, tale da garantire in sé margini di sicurezza invalicabili se non con una collaborazione da parte del titolare che, sebbene non consapevole, quasi mai si presenta scevra da colpa grave".
Proprio la circostanza che i ricorrenti non forniscano alcun elemento utile a ricostruire le modalità attraverso le quali i malfattori siano venuti in possesso delle credenziali di accesso, costituisce "una indiretta ma chiara prova dell'inescusabile leggerezza commessa dal cliente nel favorire la truffa subita". D'altra parte, nella valutazione dei fatti, non può non considerarsi anche la qualità del ricorrente principale, professore ordinario presso un'università di Napoli, in virtù della quale è certo esigibile un maggiore grado di diligenza nel trattamento e custodia dei dispositivi di sicurezza e nell'uso del canale internet.
Con riferimento, infine, alla condotta della banca, censurata dal ricorrente, la scrivente ha sottolineato che, nell'attuale sistemi dei pagamenti, il bonifico è il mezzo di gran lunga più utilizzato, "con la conseguenza che -atteso l'eccezionale numero di operazioni effettuate ogni giorno dalla clientela – la pretesa che ciascuna di esse sia sottoposta ad immediata valutazione con un gestione personalizzata sembra essere soltanto una forzatura pretestuosa". Tanto premesso, l'ufficio preposto si è attivato contattando il cliente e provando anche – inutilmente – a recuperare l'importo della disposizione presso l'intermediario del beneficiario.
La ricorrente ha chiesto all'Arbitro la restituzione di € 2.479,73, l'importo del bonifico fraudolentemente effettuato.
La resistente sulla base delle considerazioni esposte ha chiesto al Collegio di respingere il ricorso ovvero di limitare la responsabilità della banca al ritardo nell'apposizione del blocco.

DIRITTO

Il collegio deve decidere in merito al mancato rimborso, da parte della banca di un bonifico effettuato on line sul conto del ricorrente, che ha disconosciuto l'operazione.
Deve rilevarsi che il ricorrente ha appreso dell'avvenuta esecuzione dell'operazione dagli stessi responsabili della banca, che lo hanno contattato a fronte di un'operazione sospetta impartita on line sul conto del cliente, a favore di un soggetto a lui sconosciuto, intestatario di un conto di moneta elettronica in essere presso un Imel.
All'operazione la banca ha dato comunque esecuzione, attivandosi poi senza successo per il recupero della somma. Ammette anche di aver proceduto con ritardo al blocco nell'operatività del conto, ma ritiene che, in presenza di rafforzati presidi di sicurezza, sia onere del cliente chiarire la dinamica dell'operazione e la eventuale configurarsi di una truffa.

Il ricorrente afferma di contro di aver sempre custodito con diligenza i dispositivi di sicurezza, impedendone l'accesso a terzi, e ipotizza che terzi estranei si siano inseriti nell'operatività del conto attraverso sofisticati sistemi informatici.
Il Collegio rileva che non è da escludere – in considerazione dell'adozione del *token* e in mancanza di ulteriori elementi di fatto – che il ricorrente sia rimasto vittima di una frode informatica, probabilmente effettuata tramite l'installazione inconsapevole sul proprio PC di *malware* in grado di catturare le credenziali per l'accesso al conto *on line*, ma non ritiene che sia il cliente a dovere chiarire se e di che tipo di frode si tratti.
In relazione a casi analoghi, in cui pure la banca adottava un sistema di autenticazione a due fattori con un generatore OTP, si segnalano alcun precedenti, in particolare la decisione n.822/ 2014 del collegio di Milano nonché l'arresto del Collegio di coordinamento n.3498 del 2012 i quali hanno assunto deliberati di accoglimento delle richieste di rimborso dei clienti per operazioni non autorizzate.
Va allora ricordato che precedentemente, secondo il Collegio di Milano, la pressoché totale invulnerabilità del sistema a "due fattori" garantita dai sistemi OTP appariva tale da fondare la presunzione di una colpa grave in capo al cliente, precisamente consistente nel non aver custodito con la dovuta diligenza il dispositivo in questione (cfr., fra le moltissime, Collegio Milano, decc. nn.2103/2012, 2658/2011, 462/2012). Siffatto orientamento riposa sull'assunto per il quale, allo stato attuale dell'evoluzione delle tecnologia, l'autenticazione a due fattori con metodo OTP risulterebbe la più sicura possibile sicché diviene giocoforza concludere che, ove tale sistema risulti adottato, l'intrusione non si sia resa possibile se non attraverso la cooperazione, pur involontaria, del cliente, traducentesi nella mancata custodia dei codici e dei dispositivi di autenticazione ovvero nell'ingenua trasmissione degli stessi a terzi.
Detto orientamento è stato, in tempi recenti (cfr. dec. 1583/2012), non pienamente condiviso da questo Collegio, il quale, pur ammettendo la spiccata capacità protettiva del sistema OTP, ha escluso l'automatismo deduttivo cui si ispira invece il pensiero del Collegio milanese, per concludere che l'impiego dell'OTP non vale di per sé a lasciar irreversibilmente presumere una negligenza comportamentale del cliente, bensì a indurre l'Arbitro ad una valutazione più rigorosa della sua condotta. Il Collegio di Roma ha, a sua volta, ripreso la lettura del Collegio di Napoli ponendo una speciale enfasi sul principio di diritto ricavabile dalle anzidette norme del d. lgs. cit. La ripartizione dell'onere probatorio, per come delineata nell'impianto normativo, non consentirebbe, secondo l'Arbitro romano, di pervenire all'automatismo affermato dal Collegio di Milano, dovendosi al contrario apprezzare, oltre al meccanismo offerto, anche l'intero sistema di controlli approntato dall'intermediario, e potendosi con ciò concludere che la cattura dei codici ad opera di terzi non autorizzati ben possa avvenire in presenza di un pur diligente comportamento da parte del Cliente (Cfr. Collegio Roma, decc. nn.2264/2012, 2660/2012, 1910/2012). In particolare, in un caso nel quale il sistema di sicurezza approntato dall'intermediario contemplava un'autenticazione mediante l'uso di un lettore di *smartcard*, non azionabile dunque in difetto della carta, mentre il cliente aveva "abboccato" ad un contestuale *phishing* operato da terzi mediante la proiezione di una finestra a comparsa (c.d. *pop-up*) che richiedeva l'inserimento delle credenziali (OTP comprese), il Collegio romano è giunto ad affermare una colpa concorrente dell'intermediario desumendola dalla accertata ripetitività di simili intrusioni, come tali testimoni di una inadeguatezza o lacunosità dei presidi di sicurezza predisposti.
Questo progressivo spostamento del metro valutativo nella direzione di una più ampia ed efficace protezione del cliente si spiega, secondo la recente decisione del collegio di coordinamento, alla luce della parallela evoluzione dei metodi di aggressione informatica, la cui sofisticazione induce a porre in discussione non già il più generale principio di

ragionevole esigibilità delle contromisure di sicurezza da predisporsi a cura degli intermediari, quanto ad affermarlo secondo un nuovo stile ma di giudizio aggiornato all'evoluzione del fenomeno criminale e alla sua nuova capacità offensiva.
Nella decisione citata il Collegio di coordinamento ha stabilito essere di tutta evidenza che la ricorrente, immune nella specie da qualsivoglia colpa grave, non sia tenuta a sopportare le conseguenze dell'accaduto. Dal che consegue l'obbligo per la resistente di ristorare il danno patito dalla ricorrente calcolato in misura pari all'ammontare dell'operazione disconosciuta …"
Venendo al caso in esame il Collegio deve rilevare che la materia dei prelievi fraudolenti costituisce oggetto della recente disciplina sui sistemi di pagamento, introdotta dalla direttiva europea sui servizi di pagamento e recepita nell'ordinamento interno con il dlgs.n.11del 2010.
Il decreto riafferma un importante principio, contenuto nell' art.59 della Direttiva e poi traslato nel dlgs n.11del 2010 di attuazione della stessa,per il quale (Art. 10,comma 2.) "Quando l'utilizzatore di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento eseguita, 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*".*Pertanto, ai fini di escludere la propria responsabilità per i danni derivanti dall'uso non autorizzato dello strumento di pagamento, la banca non può simpliciter affermare, come ha fatto, che essendo stata l'operazione compiuta adoperando i codici del cliente, e constando un sistema di protezione rafforzato, si debba presumere che i sistemi di sicurezza non siano stati diligentemente custoditi dal cliente.
Come più volte ha ribadito questo collegio, la nuova disciplina prevede una sorta di inversione dell'onere della prova a carico del prestatore del servizio di pagamento che deve *dimostrare i*l dolo o la colpa grave del cliente nell'utilizzo dello strumento di pagamento, con particolare riguardo alla violazione degli obblighi di custodia sanciti all'art.7 del decreto.
Il Collegio di Coordinamento, nella decisione su citata, ha ricordato che il principio di distribuzione del rischio, nel regime dei servizi di pagamento appare decisamente squilibrato *a* favore dell'utilizzatore del servizio di pagamento. Tale assetto, ha ribadito il Collegio "si spiega in considerazione dell'incomparabilmente maggior capacità economica dell'intermediario di sostenere il rischio connesso all'impiego di strumenti la cui sicurezza assoluta non è stata sin qui raggiunta (e probabilmente non verrà mai raggiunta dato l'inarrestabile evolversi della tecnologia civile e la naturale "rincorsa" della tecnologia criminale nella stessa direzione), grazie ad una redistribuzione dei relativi costi sull'intero pubblico dell'utenza. Principio che il Collegio di Coordinamento ha ritenuto di pienamente condividere, soggiungendo che l'addossamento del rischio all'intermediario (il cui estremo confine si colloca all'altezza della colpa grave dell'utente) appare viepiù giustificato dalla forte e incessante promozione all'uso di tali strumenti posta in essere dal mondo bancario, in ciò aiutato anche da un sistema legislativo che sempre più ne impone l'adozione (si ponga mente soltanto all'obbligo per le imprese e i professionisti di operare i pagamenti tributari on line e non più allo sportello). Siffatta promozione e siffatta imposizione, sulla cui opportunità o Collegio di coordinamento non ha inteso esprimersi," " comporta obiettivamente un sensibile beneficio economico per gli stessi intermediari consentendo loro significativi ed evidenti risparmi rispetto ad una tradizionale operatività di sportello."
"Un tale beneficio deve dunque trovare, come trova, nel dettato normativo, un correlato *pendant* proprio nel trasferimento, in capo allo stesso intermediario che gode di quel beneficio, altresì del rischio portato dall'impiego dello strumentario tecnologico da cui

quello stesso beneficio deriva (con i soli estremi limiti, beninteso, della frode del dolo o della colpa grave ascrivibile all'utilizzatore)".

Pertanto ,per quanto riguarda il caso in esame, il Collegio ribadisce che, in assenza di elementi circonstanziali probatori addotti dalla banca, atti a dimostrare la colpa grave (nell'accezione più volte ribadita da questo collegio) del cliente nell'utilizzazione dello strumento di pagamento, la banca è tenuta al rimborso dell'operazione fraudolenta, ai sensi dell'art.11 del lgs.n.11 del 2010, che stabilisce l'obbligo "immediato" di rimborso dell'importo dell'operazione non autorizzata. Mette conto ricordare che è qualificabile come colpa grave quella "straordinaria ed inescusabile imprudenza e negligenza", caratterizzata non solo dall'omissione della diligenza media del buon padre di famiglia, ma anche da "quel grado minimo di diligenza osservato da tutti" (Cass. 13 ottobre 2009, n. 21679; Cass. 18 maggio 2009, n. 11459; Cass. 19 novembre 2001, n. 14456; il concetto di colpa grave elaborato dalla giurisprudenza di legittimità è stato più volte fatto proprio da questo Collegio: si veda, tra le tante, la decisione n. 514 del 17 febbraio 2012).

P.Q.M.

Il Collegio, in accoglimento del ricorso, dichiara l'intermediario tenuto alla restituzione dell'importo di € 2.479,76. 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