COLLEGIO DI MILANO– DECISIONEN. 16026/2019 – PRES. LAPERTOSA – EST.DI NELLA

Strumenti di pagamento – *Home banking* – Operazioni fraudolente– Sistema di autenticazione a due fattori – colpa grave - presunzione (d.lgs. n. 11/2010, artt. 7 – 8 –10 - 10 bis - 12)

Ove la banca abbia adottato un sistema di autenticazione a due fattori con metodo OTP, è presumibile che l'operazione fraudolenta sia stata resa possibile da un comportamento gravemente colposo del cliente nella custodia dei codici di accesso e dei dispositivi connessi, in assenza di ulteriori indici di anomalia dell'operazione. (FP)

FATTO

La parte ricorrente espone, allega e chiede nel ricorso quanto segue.
- Il 09/08/2017, leggendo la posta elettronica, si accorgeva di un bonifico per € 12.000,00 disposto sulle coordinate bancarie *** a favore di un terzo.
- Si recava presso la competente filiale dell'intermediario, chiedendo il disconoscimento in toto del bonifico effettuato e chiedendo spiegazioni circa il mancato avviso di tale operazione tramite sms, chiamata o altro strumento, tenuto conto anche dell'importo esoso rispetto alle operazioni ordinariamente effettuate, che si aggiravano intorno a € 400.
- In data 16/08/2017 sporgeva denuncia dei fatti.
- Ha inoltrato diversi reclami all'intermediario, rispettivamente in data 16/08/2017, 03/11/2017, 05/02/2018 e 20/09/2018, ricevendo sempre risposte negative. L'intermediario non riscontrava anomalie nell'esecuzione del bonifico in quanto l'operazione è stata correttamente autenticata, registrata e contabilizzata, essendo stata effettuata tramite home banking e autorizzazione previo l'inserimento di 1) codice cliente, 2) codice segreto Pin, 3) codice della carta dei codici operativi.
- Parte ricorrente chiede il rimborso dell'importo di € 12.000,00, maggiorato degli interessi maturati, in quanto non è stato avvisato dall'intermediario.

Nelle controdeduzioni l'intermediario espone, allega e chiede quanto segue.
- In data 08/08/2017, previa autenticazione della parte ricorrente tramite corretto inserimento del codice cliente, della data di nascita e del codice Pin di accesso all'area riservata, veniva eseguita un'operazione di giroconto dal conto al conto corrente, per un importo pari a € 11.000,00. Tale operazione veniva prontamente notificata alla ricorrente tramite messaggio di posta elettronica.
- In data 09/08/2017, alle ore 17.55, veniva richiesta un'operazione di bonifico in uscita dal conto corrente, d'importo pari a € 12.000,00. Tale operazione veniva autenticata previo corretto inserimento di tre cifre random scelte dal sistema e riportate sulla carta dei codici operativi, nonché a seguito di corretta digitazione del codice di sicurezza OTP inviato sul recapito telefonico della ricorrente, e veniva pertanto eseguita e notificata in data 09/08/2017 tramite messaggio SMS Alert.
- Le operazioni sono state eseguite senza alcuna variazione dei recapiti e del codice Pin della ricorrente.
- Questa, in data 16/08/2017, chiedeva il disconoscimento dell'operazione di bonifico e la banca, a fini cautelativi, disponeva il blocco del Pin di accesso all'area riservata e dei codici operativi, oltre a chiedere alla banca controparte il blocco delle somme, che tuttavia non risultavano più disponibili.
- L'intermediario ha effettuato le opportune verifiche in merito all'accaduto e rilevava la regolare autenticazione della suddetta operazione e l'assenza di anomalie nell'esecuzione della stessa, pertanto riteneva di non procedere con il rimborso della somma disconosciuta.

- Ha attuato, al fine di scongiurare tentativi di frodi informatiche, una serie di misure volte a rafforzare il livello di sicurezza offerto ai propri clienti, più precisamente: - l'inserimento congiunto del codice cliente, della data di nascita e del codice di accesso Pin per accedere all'area riservata, - l'inserimento di una combinazione randomica di alcuni codici operativi presenti sulla carta dei codici operativi consegnati al cliente alla stipula del rapporto, - un codice di sicurezza dinamico (OTP) generato per ogni singola operazione, valido per pochi minuti e inviato tramite SMS al numero di cellulare del cliente.
- Ha altresì adottato ulteriori misure di sicurezza: il sito internet della banca utilizza infatti un protocollo EV-SSL, che garantisce, attraverso la crittografia dei dati, la sicurezza di tutte le transazioni effettuate e delle informazioni inserite; l'area "Accesso clienti", all'interno del suddetto sito internet, utilizza una tastiera numerica virtuale (denominata PinPad), sulla quale la posizione dei numeri cambia ad ogni accesso e il codice di accesso Pin non viene mai chiesto per esteso.
- Nel caso di specie risulta la regolare autenticazione dell'operazione, non rilevando alcun tipo di manomissione nel sistema informatico, oltre che il regolare invio del messaggio di SMS Alert relativo all'operazione inserita, pertanto la responsabilità dei fatti lamentati è ascrivibile al comportamento della ricorrente.
- Quanto al tempestivo blocco del conto, rileva che la ricorrente ha disconosciuto l'operazione tardivamente, in data 16/08/2017, nonostante ne fosse a conoscenza già in data 09/08/2017.
- Il 06/03/2018 perveniva convocazione ad incontro di mediazione, che si è concluso con il verbale del 09/05/2018 attestante il mancato accordo tra le parti.
- L'intermediario chiede in via principale di respingere il ricorso in quanto infondato; in via subordinata, di applicare la franchigia di € 150,00 secondo la normativa vigente al momento dei fatti; in via ulteriormente subordinata, di diminuire il danno risarcibile ai sensi dell'art. 1227 c.c.

DIRITTO

Nella presente vicenda occorre valutare alla luce del d.lgs. n. 11 del 2010 la condotta delle parti in relazione ai fatti dichiarati. Secondo quando denunciato il 16/08/2017 all'Autorità di Pubblica Sicurezza, il 09/08/2017, leggendo la posta elettronica parte ricorrente si accorgeva di un bonifico da lei non autorizzato dell'importo di € 12.000,00 disposto a favore di un terzo sconosciuto. Parte ricorrente dichiara che non ha mai consegnato ad altri le proprie credenziali di accesso al conto online.

Nella descrizione dei fatti la ricorrente non fa mai riferimento a circostanze riconducibili allo schema classico del phishing. Non sembrano neppure emergere elementi che richiamano le modalità più sofisticate di truffa, attuate attraverso un malware o altre forme di penetrazione nel sistema informatico (tipo man in the middle o man in the browser). La contestazione risulta in realtà limitata al fatto di non aver mai disposto il bonifico disconosciuto, di non aver mai perso o comunicato le proprie credenziali/password-OTP e di non aver ricevuto alcun SMS di "richiesta" e "conferma" del bonifico.

Ai fini della decisione, è innanzi tutto onere dell'intermediario provare che l'operazione sia stata autenticata, correttamente registrata e contabilizzata ex art. 10, D.Lgs. n. 11/2010: in caso di mancanza della prova l'intermediario sopporta, in ogni caso, integralmente le conseguenze delle operazioni disconosciute. Qualora venga fornita la suddetta prova, occorre valutare se alla parte ricorrente sia imputabile una condotta connotata da dolo o colpa grave in violazione agli obblighi sui di lei gravanti in forza dell'art. 7, essendo altrimenti il rischio di operazioni fraudolente a carico dell'intermediario ai sensi dell'art. 12 d.lgs. n. 11 del 2010. La prova dei fatti a carico dell'utilizzatore dello strumento di pagamento è posta sull'intermediario dall'art. 10 d.lgs. n. 11/2010. In proposito, va richiamato

l'orientamento assunto dal Collegio di Coordinamento con la decisione n. 3947/2014, secondo la quale è comunque richiesto un quid pluris rispetto alla semplice dotazione del microchip per dimostrare la colpa grave o il dolo del cliente, gravando altrimenti l'allocazione legislativa della responsabilità in capo all'intermediario.

Il Collegio costata che l'intermediario ha fornito la prova di autenticazione, corretta registrazione e contabilizzazione delle operazioni di pagamento ed ha descritto i profili delle operazioni fraudolente. In particolare, l'intermediario allega evidenze che provano: l'accesso all'area riservata della ricorrente mediante l'inserimento di codice cliente, data di nascita, codice PIN segreto; l'avvenuto inserimento della OTP; l'inserimento dei codici della "Carta codici operativi" previsti per una singola transazione-disposizione. Da quanto esposto, si evince che lo strumentario avanzato di sicurezza è stato individuato, almeno per quanto specificamente attiene al caso in esame (pagamenti disposti mediante sistemi di internet banking), nella messa a disposizione dei c.dd. token o one time password, vale a dire di congegni in grado di generare mutevoli password monouso che, aggiungendosi alla password fissa nota solo all'utente, concorrono a formare un sistema di autenticazione a "due fattori".

Parte ricorrente contesta di non aver mai ricevuto gli SMS di richiesta bonifico e della relativa conferma dell'avvenuta disposizione. L'intermediario allega però evidenza dell'invio dell'SMS contente il codice OTP all'utenza della ricorrente, che coincide con quella indicata sul modulo di ricorso oltre che nel contratto di conto corrente, nonché dell'SMS di conferma dell'avvenuta disposizione del bonifico (entrambi riportanti la data dell'8.08.2017).

Preliminarmente, il Collegio rileva che, ai sensi dell'art. 10-bis D.Lgs. n. 11/2010, come novellato dal D.Lgs. n. 218/2017, (cfr. art. 5, comma 6), "i prestatori di servizi di pagamento applicano l'autenticazione forte del cliente quando l'utente: a) accede al suo conto di pagamento on-line; b) dispone un'operazione di pagamento elettronico; c) effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi". L'art. 2, comma 1, lett. q-bis, del predetto testo normativo definisce l'"autenticazione forte del cliente" quale "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".

Posta questa premessa di carattere normativo, il Collegio di Milano, ispirandosi al principio di ragionevole esigibilità della prestazione calato nel pur peculiare ed asimmetrico rapporto fra cliente e intermediario, già prima dell'entrata in vigore delle disposizioni sopra illustrate ha costantemente affermato la responsabilità di quest'ultimo nel caso di mancata adozione dei più avanzati accorgimenti tecnici di prevenzione (cfr., fra le molte, Collegio di Milano, n. 111/2012, n. 113/2012), mentre l'ha esclusa in tutto o in parte là dove il cliente, pur debitamente informato (con adeguata evidenza e trasparenza) della disponibilità di siffatti strumentari di sicurezza, ometta di avvalersene (cfr. Collegio di Milano, n. 528/2012). Nel caso di specie, lo strumentario avanzato di sicurezza è stato individuato nella messa a disposizione dei c.dd. token o OTP (one time password), vale a dire congegni in grado di generare mutevoli password monouso che, aggiungendosi alla password fissa nota solo all'utente, concorrono a formare un sistema di autenticazione a "due fattori" (altri dice a "tre fattori" includendovi anche lo username, per quanto più "visibile" e catturabile), sistema come tale di difficile forzatura. Una volta che il sistema OTP sia stato chiaramente offerto al cliente e questi se ne sia avvalso, ne consegue che l'eventuale intrusione fraudolenta di un terzo soggetto debba ricadere nella pur ristretta area di

rischio che la legge pone a carico dell'utente. Secondo il Collegio di Milano, l'elevata sicurezza del sistema a "due fattori" garantita dai sistemi OTP appare tale da fondare la presunzione di una colpa grave in capo al cliente, precisamente consistente nel non aver custodito ed utilizzato con la dovuta diligenza il dispositivo in questione (cfr., fra le moltissime, Collegio di Milano, nn. 2103/2012, 2658/2011, 1462/2012). Siffatto orientamento riposa sull'assunto per il quale, allo stato attuale dello sviluppo tecnologico, 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 si sia resa possibile soltanto attraverso la cooperazione, pur involontaria, del cliente, traducentesi questo nella mancata custodia dei codici e dei dispositivi di autenticazione ovvero nell'ingenuo utilizzo e trasmissione degli stessi a terzi (Collegio di Milano, n. 9731/2017).

Nel caso specifico oggetto dell'odierno ricorso, l'intermediario ha allegato le evidenze relative all'autenticazione delle operazioni di bonifico a favore del beneficiario titolare di una carta di credito emessa dalla medesima banca oltre a tutta una serie di evidenze volta a dimostrare la corretta autenticazione e contabilizzazione delle operazioni disconosciute anche con riferimento ai livelli di sicurezza adottati.

Riguardo al livello di sicurezza del sistema dell'intermediario convenuto, si fa presente che risulta caratterizzato da misure di autenticazione a due fattori con password di tipo dinamico e che il sistema di riconoscimento e di autorizzazione all'accesso dei propri clienti alle loro rispettive aree riservate di home banking prevede l'inserimento di diversi codici. Ad avviso del Collegio, l'adozione di un sistema a "due fattori" induce a ritenere, in assenza di ulteriori indici di anomalia dell'operazione, da un lato, che la banca abbia assolto all'onere di provare l'adempimento degli obblighi su di essa gravanti ai sensi dell'art. 8 D.lgs. n. 11/2010 e, dall'altro lato, che il cliente si sia reso gravemente inadempiente all'obbligo di custodia degli strumenti e dei codici di accesso che consentono l'utilizzo del servizio on line e l'invio di ordini di bonifico a valere sul conto a lui intestato. Alla luce delle caratteristiche tecniche di sicurezza adottate dall'intermediario, sembra dunque lecito presumere che l'operazione fraudolenta di cui si discute sia stata resa possibile da un comportamento inadempiente della parte ricorrente, la quale ha omesso di adottare tutte le cautele necessarie a custodire i codici di accesso e i dispositivi connessi e ad utilizzarli in modo prudente.

Né varrebbe obiettare, in contrario, che così facendo si violerebbe il disposto dell'art. 10 D.Lgs. n. 11/2010, nella parte in cui esclude che l'utilizzo dello strumento di pagamento possa costituire di per sé prova della violazione degli obblighi (nella specie, di custodia) da parte del cliente; la lettera della disposizione non sembra infatti incompatibile con l'interpretazione qui accolta, in quanto l'espressione "non è di per sé necessariamente sufficiente a dimostrare" non esclude che, al ricorrere di determinate condizioni (particolare affidabilità tecnica dello strumento, assenza di ulteriori elementi di anomalia dell'ordine), tale idoneità possa invece sussistere ed essere apprezzata dal giudicante come prova (presuntiva) della violazione degli obblighi gravanti sul cliente.

In senso contrario non depone neppure la pronuncia del Collegio di Coordinamento n. 3498/2012. Con tale decisione, il Collegio ha certamente escluso un "automatismo" tra l'utilizzo di un sistema a due fattori da parte dell'intermediario e la sussistenza di una colpa grave imputabile al cliente, ben potendosi, infatti, verificare la "cattura dei codici" ad opera di terzi anche in presenza di un comportamento diligente da parte del cliente. Più in particolare, nella decisione sopra richiamata, il Collegio di Coordinamento ha escluso ogni responsabilità a carico del cliente in ragione dell'accertata aggressione informatica operata attraverso un malware particolarmente sofisticato, "capace di

sorprendere la buona fede anche di un pur normalmente attento fruitore del servizio" e tale, quindi, da escludere ogni sua colpa. Nulla di tutto questo è invece ravvisabile nel caso in esame, né la ricorrente lamenta, del resto, alcuna di quelle circostanze in fatto che, in altre occasioni, hanno indotto altri Collegi dell'ABF a individuare una colpa concorrente dell'intermediario (email di phishing, ecc.).

Pur escludendo una necessaria ed automatica corrispondenza biunivoca tra il sistema di sicurezza a due fattori adottato dall'intermediario ed una colpa grave della ricorrente nella custodia dei propri codici identificativi e del dispositivo OTP, da una valutazione delle circostanze di fatto come descritte dalle parti e dall'adozione di un sistema di sicurezza a due fattori approntati dall'intermediario - che, salvo il ricorrere di meccanismi informatici particolarmente sofisticati (nel caso in esame nemmeno allegati dalla ricorrente), consente di escludere accessi non autorizzati da parte di terzi - il Collegio ritiene, quindi, di poter presumere che l'operazione fraudolenta sia stata resa possibile da un comportamento gravemente colposo della ricorrente. Pertanto, il ricorso non può essere accolto.

P. Q. M.

Il Collegio non accoglie il ricorso.