COLLEGIO DI BOLOGNA - DECISIONE N. 8120/2017 - PRES. MARINARI – REL. LUCARELLI

Conto corrente bancario – Home banking – Operazioni non autorizzate – Rimborso – Violazione degli obblighi di diligenza nella custodia dello strumento di pagamento – Infondatezza (cod. civ., art. 1176)

TESTO:

FATTO

Titolare di conto corrente acceso presso l'intermediario resistente, la parte ricorrente, anche a mezzo della documentazione acclusa al ricorso, riferisce che in data 27.8.2016, erano state effettuate, a sua insaputa, due ricariche di una carta di credito prepagata dell'importo di euro 497,00 ciascuna - rispettivamente alle ore 08:58 ed alle ore 08:59- nonché - alle ore 08:56- un bonifico di euro 2.976,00 verso un conto corrente intestato ad un nominativo italiano. Nella denuncia-querela acclusa al ricorso, la ricorrente dichiara che nel mese di agosto 2016 aveva ricevuto sul suo cellulare un sms, apparentemente proveniente dalla convenuta, nel quale le veniva comunicato di accedere al conto on-line per modificarne le credenziali di accesso per ragioni di sicurezza; pertanto, aveva cliccato sul link presente nello sms e aveva seguito la procedura ivi richiesta, senza riscontrare, apparentemente, alcuna anomalia. In un secondo momento, si era accorta di non riuscire più ad accedere tramite internet al proprio conto corrente, e contestualmente di non potere più utilizzare il proprio telefono cellulare, come se fosse stato bloccato. Esposto reclamo all'intermediario per ottenere il rimborso delle somme corrispondenti alle operazioni disconosciute, riceve un riscontro negativo visto che l'intermediario aveva rilevato la legittimità delle transazioni disconosciute. Di conseguenza, effettua ricorso presso questo Arbitro, chiedendo il rimborso della somma complessiva di euro 3.970,00, pari all'importo delle tre operazioni disconosciute di cui sopra. Convenuto ritualmente, l'intermediario, nel confermare i fatti enunciati dalla ricorrente, fa presente che: x le operazioni disconosciute dalla ricorrente sono state effettuate mediante il servizio di home banking, utilizzando un canale di autenticazione on line "ID". **[*omissis*]** Il sistema di sicurezza ID dell'intermediario si attiva direttamente dall'apposita applicazione del cellulare. x il suddetto servizio è stato attivato dalla ricorrente in data 3.03.2016, abilitandovi il dispositivo X e fornendo l'utenza n. xxx/yyy quale "numero di telefono certificato"; x il giorno antecedente a quello in cui sono state effettuate le operazioni disconosciute è stato associato al numero di cellulare indicato dalla ricorrente (n. xxx/yyy) un nuovo dispositivo smartphone Y; i codici inviati dall'intermediario per abilitare il nuovo dispositivo Y, associato al numero di telefono n. xxx/yyy, sono stati inviati al numero di telefono certificato come appartenente alla ricorrente, ovvero il n. xxx/yyy; x le operazioni di pagamento disconosciute sono state effettuate in osservanza degli impegni contrattuali e apparentemente disposte da soggetto identificatosi come il legittimo titolare e mediante il corretto inserimento di tutti quei riconoscimenti informatici indispensabili per l'esecuzione di operazioni on line come quelle di specie; non avendo ricevuto da parte della ricorrente segnalazioni circa lo smarrimento o il furto dei codici personali e/o dello smartphone, l'intermediario era contrattualmente obbligato ad autorizzare le disposizioni di pagamento

disconosciute. In considerazione di quanto riportato, l'intermediario resistente chiede che il ricorso sia rigettato.

DIRITTO

ABF ha più volte affermato che nelle controversie relative ad un utilizzo fraudolento di strumenti di pagamento, occorre valutare, da un lato, la condotta dei clienti con riguardo agli obblighi di diligenza nella custodia dello strumento di pagamento e dei dispositivi collegati, dall'altro, la condotta dell'intermediario, il quale è chiamato ad adempiere al mandato secondo la diligenza professionale e qualificata dell'art. 1176, comma 2, c.c., attraverso l'adozione di misure di protezione adeguate rispetto agli standard esistenti, sotto il profilo dei presidi tecnici adottati. L'orientamento dei Collegi ABF è nel senso di ravvisare la colpa grave del cliente per imprudente navigazione qualora risulti che quest'ultimo abbia comunicato a terzi i dati associati ad uno strumento di pagamento in risposta ad una e-mail di phishing ovvero SMS. Sono ormai molteplici, infatti, le modalità attraverso le quali vengono perpetrate le frodi attraverso internet (invio di mail-civetta volte ad indurre i clienti a comunicare i propri dati personali, malware di reindirizzamento web, ecc.). In materia assumono particolare rilevanza le decisioni n. 3498/2012 e n. 1820/2013, con le quali il Collegio di coordinamento ha distinto le truffe realizzate mediante metodi ormai conosciuti alla clientela (le classiche email di phishing), dalle truffe più insidiose in cui maggiore è la difficoltà di avvedersi della situazione di apparenza generata dal malware. In particolare, il Collegio di Coordinamento con le suddette decisioni, ha distinto le ipotesi di "phishing tradizionale", caratterizzate dall'invio di un semplice messaggio telefonico o email con il quale si invita il cliente a digitare le proprie credenziali di accesso al conto, da quelle più insidiose consistenti in un "subdolo meccanismo di aggressione (che) ha luogo attraverso un sofisticato metodo di intrusione caratterizzato da un effetto sorpresa capace di spiazzare l'utilizzatore, grazie alla perfetta inserzione nell'ambiente informatico originale e nella correlata simulazione di un messaggio che a chiunque non potrebbe apparire che genuino". Tra le due fattispecie v'è una differenza tale da indurre a ritenere che solo nella seconda, consistente in una sofisticata intrusione nell'autentico sito della banca nel momento in cui l'utente vi accede per compiere un'operazione, debba escludersi la ravvisabilità di una colpa grave del cliente; laddove nel caso di phishing tradizionale, l'assenza di cautela dell'utente appare difficilmente scusabile, trattandosi in tal caso di fenomeno oramai diffusamente noto, che quanto meno qualunque utente dotato di normale avvedutezza e prudenza, come si ritiene siano quelli avvezzi all'uso del c.d. homebanking, deve essere in grado di individuare, non facendosi trarre in inganno. Nell'ipotesi del "phishing tradizionale", il cliente è, pertanto, vittima di una colpevole credulità: colpevole in quanto egli è portato 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. Il caso in esame costituisce una forma del phishing tradizionale, il c.d. smishing. Si tratta, infatti, di ipotesi caratterizzate non dall'invio di una email ma, piuttosto, di un SMS. Segnatamente, in tali casi l'utente è raggiunto da un SMS contenente la richiesta di cliccare su di un link e, quindi, di raggiungere una pagina web. L'utente, dopo aver cliccato sui link, approda in siti online artefatti che chiedono l'inserimento di dati personali, carpendo, in tal modo, le credenziali di utilizzo degli strumenti di pagamento Nel caso di specie, è la stessa ricorrente a dichiarare di aver ricevuto un SMS "apparentemente proveniente" dell'intermediario e di aver fornito tutti i propri dati per

l'abilitazione alle operazioni dispositive dal proprio conto on line. È fuori di dubbio, infatti, che la ricorrente abbia fornito le credenziali associate al conto per il funzionamento delle procedure di sicurezza, in risposta ad un anomalo messaggio telefonico, che sollecitava la digitazione all'interno di un sito internet al quale tale messaggio rinviava. La ricorrente non dichiara, né tantomeno fornisce evidenza, di aver verificato in via preventiva la genuinità e le veridicità di quanto richiesto, la provenienza del sms o se il link ricevuto fosse provvisto del protocollo di sicurezza HTTPS. Appare, pertanto, pacifico che l'operazione contestata sia scaturita da un fenomeno di smishing realizzato ai danni del cliente, avendo la stessa ricorrente fornito tutti i dati necessari per l'esecuzione dell'operazione oggi contestata. Ne consegue che la colpa grave della ricorrente risulta provata, essendo indubitabile che l'operazione abusiva contestata è stata resa possibile dal suo comportamento, avendo dato credito, nonostante la notorietà di tale pratica e la sua pericolosità, ad un SMS costituente un evidente caso di smishing. E tale comportamento denuncia una colpevole violazione degli obblighi di custodia dei dati identificativi e dispositivi del proprio conto. Tali circostanze, secondo il consolidato orientamento in materia (v., tra le altre, Collegio di coordinamento, decisione n. 3498/2012; Collegio di Milano, decisione n. 467/2014 e Collegio di Roma, n. 1699/2013), non possono che indurre a ribadire che al ricorrente è imputabile una violazione gravemente colpevole degli obblighi di custodia dei dati identificativi e dispositivi del conto on line, sicché la perdita subita non può che restare interamente a proprio carico (cfr. ex multis dec. n. 2177/2016), con la conseguenza che il ricorso non può trovare accoglimento.

P.Q.M.

Il Collegio non accoglie il ricorso.