COLLEGIO DI BOLOGNA

composto dai signori:

(BO) MARINARI	Presidente
(BO) MARTINO	Membro designato dalla Banca d'Italia
(BO) PAGNI	Membro designato dalla Banca d'Italia
(BO) SOLDATI	Membro di designazione rappresentativa degli intermediari
(BO) D ATRI	Membro di designazione rappresentativa dei clienti

Relatore MARCO MARTINO

Seduta del 23/07/2019

FATTO

Parte ricorrente riferisce che:

- è titolare di carta di debito rilasciata dall'intermediario resistente;
- in data 16.12.2018, alle ore 12:22, riceveva sulla propria utenza telefonica un sms di notifica dell'avvenuto pagamento di 2.500,00 euro in favore di un sito straniero, che disconosce;
- provvedeva subito al blocco della carta e in data 21.12.2018 sporgeva denuncia e presentava reclamo all'intermediario, riferendo di non avere subito lo spossessamento della carta e di esserne l'unica utilizzatrice;
- l'intermediario ha negato il rimborso, stornando l'importo di 2.500,00 euro inizialmente accreditato, affermando la regolarità della transazione, effettuata con tecnologia *"3DS Dinamico"*, che prevede l'utilizzo di una password usa e getta generata dai dispositivi in possesso del cliente, e la colpa grave del ricorrente per incauta custodia della carta e dei codici dispositivi, noti a lui solamente ;
- allega al ricorso un sms ricevuto il giorno della truffa alle ore 11:40, contenente un link ad una "notifica importante" contenuta nella sua bacheca;
- insiste nel rimborso e afferma la buona fede dell'utente.

Parte resistente eccepisce che:

- la transazione disconosciuta dal ricorrente risulta autenticata, correttamente registrata e contabilizzata, eseguita nei limiti del plafond, prima dell'apposizione del blocco, mediante utilizzo delle credenziali di commercio elettronico sicuro (tecnologia 3DS dinamico) con inserimento della password dispositiva OTP, generata dal *token* nella esclusiva disponibilità del ricorrente;
- parte ricorrente è stata vittima di una operazione di *phishing* tradizionale, come riconosciuto nel reclamo del 12.2.2019, in cui riferisce di avere cliccato sul link contenuto in un sms, apparentemente proveniente dall'intermediario, per "verificare" dei documenti; nella pagina di re-indirizzamento ha poi provveduto per ben due volte a inserire il codice richiesto;
- l'utente è incorsa in colpa grave nella custodia delle credenziali, in violazione degli obblighi imposti dall'art. 7, comma 2, D.Lgs 11/2010 e dalle condizioni contrattuali;
- l'intermediario da tempo promuove sul proprio sito una pagina informativa sui rischi connessi all'utilizzo degli strumenti di pagamento.

Parte ricorrente chiede il rimborso di Ero 2.500,00

Parte resistente chiede il rigetto del ricorso.

DIRITTO

Parte ricorrente disconosce un pagamento on line di 2.500,00 euro, eseguito il 16.12.2018 alle ore 12:22 con la carta di cui alla parte in fatto..

A sostegno della domanda allega la denuncia e il reclamo.

L'intermediario eccepisce la colpa grave del ricorrente per incauta custodia dei dispositivi personalizzati che consentono l'utilizzo dello strumento di pagamento, avendo dato seguito, con colpevole credulità, a una operazione di phishing classico. Sul punto, fa presente che sul proprio sito istituzionale è presente un'apposita sezione sicurezza contenente ogni informazione in tema di phishing.

L'art. 10, d.lgs. 11/2010 dispone che "è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata".

Nel dettaglio, l'intermediario afferma che il bonifico disconosciuto è stato disposto mediante corretto inserimento delle credenziali di accesso al sistema e digitazione della password dinamica OTP generata da un token in possesso esclusivo del ricorrente, in assenza di alcuna anomalia.

L'intermediario ha documentazione tecnica che evidenzia che il pagamento contestato è stato disposto con codice generato da token.

Sulla base della denuncia e delle ulteriori evidenze in atti, emerge che: parte ricorrente non ha perso il possesso dello strumento di pagamento e del token; nel giorno della frode ha risposto ad un sms di phishing apparentemente proveniente dall'intermediario, ricevuto alle ore 11:40, del seguente tenore:

- nella lettera di reclamo inviata all'intermediario, riconosce di avere cliccato sul link e di avere inserito un codice sul link di re-indirizzamento.

- dal log dell'operazione, sopra accluso, si ricava che la stessa è stata eseguita alle ore 12:22 del 16.12.2018.

Nel caso di specie non risultano integrati gli indicatori di anomalia di cui all'art. 8 del D.M. 112/07.

Per concorde affermazione delle parti, era attivo il servizio di avviso tramite sms per le transazioni disposte con la carta in contesa.

L'intermediario allega evidenza di un sms alert inviato in occasione del prelievo disconosciuto.

Molti dei tentativi di truffa posti in essere con modalità telematiche in materia di servizi di pagamento si svolgono secondo uno schema tipico e ampiamente noto, consistente nell'indurre il titolare dello strumento, a seconda dei casi tramite telefono, e-mail, Sms o altri strumenti di comunicazione, a comunicare e/o a inserire su dispositivi o piattaforme informatiche le proprie credenziali personalizzate, solitamente adducendo falsamente l'esistenza di tentativi di accesso abusivo o più genericamente l'opportunità di verificare o implementare caratteristiche di sicurezza (c.d. phishing che, se tradizionalmente prende le forme di una mail civetta, può tuttavia presentarsi anche mediante l'invio di sms (c.d. smishing) o l'effettuazione di chiamate vocali (c.d. vishing).

La diffusione del fenomeno è tale che i Collegi ABF ritengono che l'impiego di una media diligenza sia sufficiente a scongiurare il pericolo e ad impedire la truffa.

Nel caso sottoposto all'attenzione del Collegio, emerge come la fattispecie descritta dal ricorrente possa essere ricondotta, per espressa ricostruzione del medesimo, al ben noto fenomeno della truffa informatica denominata phishing. Tale fattispecie è stata esaminata, come noto, dalle 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.

Ne deriva che il ricorso non può essere accolto.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE

Firmato digitalmente da
MARCELLO MARINARI