Diritto Bancario

Bonifico non autorizzato, tecniche per carpire le credenziali di accesso e responsabilità della banca

di **Valerio Sangiovanni, Avvocato**

Tribunale di Grosseto, 16 maggio 2023, Giudice Frosini

Parole chiave

Conto corrente – *Home banking* – Bonifico non autorizzato – Credenziali di accesso – Colpa grave del cliente - Esclusione

Massima: "*Nel caso in cui il cliente della banca venga indotto a rivelare le credenziali di accesso al proprio home banking in conseguenza di plurime e sofisticate tecniche poste in essere dal malfattore per carpire i vari codici di accesso, non sussiste colpa grave del cliente, trattandosi di mezzi truffaldini non riconoscibili da un utente di media diligenza, con la conseguenza che la banca deve rimborsare al cliente l'importo sottratto dal terzo*".

Disposizioni applicate

Art. 12 d.lgs. 27 gennaio 2010, n. 11 (responsabilità del pagatore per l'utilizzo non autorizzato di strumenti o servizi di pagamento)

CASO

Due coniugi sono **titolari di un conto corrente**, che può essere movimentato anche per via elettronica mediante il c.d. *home banking*, come avviene ormai usualmente. La moglie riceve un messaggio sul telefono cellulare, apparentemente proveniente dalla banca presso cui i coniugi hanno il conto, con il quale viene resa edotta di movimentazioni anomale sul conto, unitamente a un *link* da utilizzare per procedere al blocco delle operazioni sospette. Poco dopo la stessa moglie riceve, sempre sul cellulare, una telefonata da un numero verde

apparentemente riconducibile alla banca, con il quale l'interlocutore le chiede di fornirgli il codice fiscale del coniuge, cointestatario del conto. La moglie mette in contatto l'interlocutore con il marito. Il malfattore telefona infine al marito e si fa inviare la tessera bancaria, al fine dichiarato (ma non corrispondente al vero) di bloccare una presunta operazione anomala.

All'esito di queste articolate condotte truffaldine, dal conto dei coniugi viene effettuato un bonifico *online* verso un terzo sconosciuto per l'importo di 7.665 euro. **I coniugi disconoscono l'operazione** nei confronti della banca e presentano denuncia penale. L'istituto di credito tuttavia si rifiuta di rimborsare l'importo sottratto, argomentando nel senso che non ci sarebbe alcuna responsabilità della banca per l'accaduto. I coniugi si rivolgono così al Tribunale di Grosseto.

SOLUZIONE

Il Tribunale di Grosseto dà applicazione al d.lgs. n. 11/2010, il quale stabilisce una **presunzione di colpa della banca**, che può essere vinta solo in caso di dolo o colpa grave del correntista. Nel caso di specie, ritiene il giudice grossetano che i fatti illustrati non possano essere ricondotti a colpa grave. Viene dunque affermata la responsabilità della banca che viene condannata a risarcire il danno patito dai correntisti, nella misura di 7.665 euro, ossia per l'importo della distrazione avvenuta con il bonifico non autorizzato.

QUESTIONI

Negli anni settanta, **i delinquenti rapinavano fisicamente le banche**, armi in pugno. Oggi le rapine in banca sono pressoché sparite: a parte il fatto che le filiali hanno poco danaro contante, gli ausili elettronici consentono con una certa facilità di scoprire gli autori. I sistemi di allarme sono più sofisticati, le porte delle filiali si bloccano, le casseforti si aprono solo a tempo, le telecamere sono ovunque, i telefonini sono tracciabili. I malfattori hanno allora cambiato la tecnica per sottrarre danaro: essi hanno imparato a usare le nuove tecnologie, in continua evoluzione. Ottenendo le credenziali di accesso ai conti, è possibile asportare danaro, producendo un effetto simile a quello della classica rapina in banca, peraltro senza rischiare la propria incolumità fisica.

Si tratta di quanto avvenuto nel caso oggetto dell'ordinanza del Tribunale di Grosseto. Dai fatti riportati nel provvedimento emerge che i delinquenti hanno usato **una pluralità di tecniche per carpire le credenziali** di accesso. Le principali tecniche esistenti sono le seguenti:

- *phishing*: un messaggio di posta elettronica invita a cliccare su di un *link*, che porta a una pagina creata dai malfattori (talvolta simile al sito della banca) dove il cliente digita le credenziali di accesso;
- *smishing*: un messaggio ricevuto sul telefono cellulare invita a cliccare su di un *link*, che porta a una pagina creata dai truffatori dove il cliente scrive le credenziali
- *vishing*: i malfattori telefonano al cliente della banca carpendogli – con le scuse più fantasiose - le credenziali di accesso e, in particolare, la *password* dispositiva;

- *spoofing*: i truffatori fanno apparire che il messaggio di posta elettronica oppure il messaggio di testo oppure la telefonata provenga dalla banca vera (ad esempio sul *display* appare la denominazione della banca): il mittente o telefonante appare essere la banca, mentre in realtà si tratta del malfattore, che si finge un funzionario dell'istituto di credito.

Phishing e *smishing* consentono ai malfattori di ottenere le credenziali di accesso statiche (tipicamente *user* e *password*). Il *vishing* viene invece più spesso usato per carpire la *password* dinamica, ossia il codice univoco che serve per la singola operazione dispositiva. Nel caso deciso dal Tribunale di Grosseto i coniugi sono stati vittime dell'utilizzo misto di più tecniche: alla fine i malfattori hanno ottenuto – in parte dalla moglie, in parte dal marito - tutte le credenziali di accesso e hanno fatto il bonifico a sé stessi. Non vi è certamente dolo dei clienti. La questione è se vi sia una loro colpa, e in particolare se la colpa possa considerarsi grave.

La questione della responsabilità nelle operazioni di *home banking* è disciplinata nel d.lgs. n. 11/2010. Rilevante è in particolare l'art. 12 di detto decreto. L'ordinanza del Tribunale di Grosseto contiene una piccola imprecisione, in quanto fa riferimento a una versione dell'art. 12 ormai non più in vigore: il d.lgs. n. 11/2010, attuativo di normativa comunitaria, è stato modificato a far tempo dal 13 gennaio 2018, ed è in vigore - da allora - una nuova versione. La versione attuale del comma 3 dell'art. 12 del d.lgs. n. 11/2010 prevede che "*salvo se abbia agito in modo fraudolento o non abbia adempiuto a uno o più degli obblighi di cui all'articolo 7,* ***con dolo o colpa grave****, il pagatore può sopportare, per un importo comunque non superiore a euro 50, la perdita relativa a operazioni di pagamento non autorizzate derivanti dall'utilizzo indebito dello strumento di pagamento conseguente al suo furto, smarrimento o appropriazione indebita*".

La modifica normativa non ha peraltro cambiato la sostanza della questione: in caso di dolo o colpa grave risponde il cliente; negli altri casi (colpa lieve o assenza di colpa del cliente) risponde la banca. Spetta al giudice di merito, di volta in volta, stabilire se vi sia colpa grave o meno. Il Tribunale di Grosseto esclude, nel caso di specie, la colpa grave dei coniugi: l'*sms* appariva provenire dalla banca e la telefonata appariva provenire dalla banca. Vero è che i coniugi hanno creduto al messaggio e alla telefonata. Tuttavia non possono considerarsi integrati – scrive il giudice grossetano – gli estremi della colpa grave, in quanto queste modalità di truffa - che usano una pluralità di tecniche sofisticate (*smishing*, *vishing* e *spoofing*) - **non sono riconoscibili per un utente di media diligenza**. In conclusione, il Tribunale di Grosseto condanna la banca a risarcire i correntisti.