Diritto Bancario

Telefonate sospette e vishing: responsabilità della banca e tutela del cliente contro le frodi informatiche

di **Valerio Sangiovanni, Avvocato**

Arbitro Bancario Finanziario, decisione n. 9549 dell'8 aprile 2021

Parole chiave

Sistemi di pagamento – Strumenti di pagamento – Carta di credito – Operazioni non autorizzate – Autenticazione forte – Sistema a un fattore - Vishing - Responsabilità della banca

Massima

Nel caso di movimenti su carta di credito non autorizzati dal cliente, laddove la banca consenta i movimenti sulla base di sole informazioni in possesso del cliente e senza prevedere l'utilizzo di un sistema di autenticazione forte, la banca risponde del danno patito dal cliente, consistente nelle somme che sono state fraudolentemente distratte dal terzo.

Disposizioni applicate

Art. 10 d.lgs. n. 11 del 27 gennaio 2010 (prova di autenticazione ed esecuzione delle operazioni di pagamento)

CASO

Una signora riceve una telefonata da una persona che si presenta come operatore di una banca. Il presunto operatore chiedeva conferma di un SMS che la signora aveva ricevuto poco prima, contenente l'indicazione di spese sospette e le chiede di seguire le sue indicazioni per bloccare tali operazioni. In particolare l'operatore informava la signora che le avrebbe mandato un SMS con i codici per il riconoscimento, chiedendole di comunicare tali codici.

Mentre era al telefono, le giungevano degli SMS alert da parte dell'intermediario che l'avvisavano che **erano state compiute due operazioni rispettivamente dell'importo di € 1.000 e di € 1.300**. Una volta terminata la telefonata, insospettiva, chiamava il numero verde dell'intermediario, dove l'operatore la informava di essere stata vittima di truffa.

SOLUZIONE

La signora vittima di truffa si rivolge all'Arbitro Bancario Finanziario (ABF) per ottenere il rimborso della somma di € 2.300 indebitamente sottratta. **L'Arbitro Bancario Finanziario accoglie il ricorso** e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 2.300, per non essersi la banca dotata di sistemi di sicurezza a elevato standard (autenticazione forte).

QUESTIONI

In passato, quando l'uso del contante era maggiormente diffuso, i criminali puntavano a rapine presso gli sportelli delle banche oppure a portavalori: si trattava di sottrarre fisicamente il danaro contante. Progressivamente queste modalità di rapina si sono ridotte d'importanza, poiché **le operazioni di pagamento vengono per lo più effettuate con mezzi elettronici**, mentre il contante in circolazione diminuisce. È invece cresciuto il rilievo delle operazioni volte a sottrarre danaro mediante frodi perpetrate sui canali elettronici di pagamento. La fantasia dei malfattori varia con il variare delle tecnologie. Particolarmente subdolo è il c.d. "vishing", oggetto della decisione dell'Arbitro Bancario Finanziario che si commenta qui brevemente. Si tratta di un meccanismo che consente ai criminali di carpire, mediante una telefonata (voice, da cui vishing), i codici necessari per movimentare il conto del malcapitato.

Nella maggior parte dei casi, il danaro sottratto non può essere recuperato dai malfattori, cosicché residua solo la possibilità di far valere la responsabilità della banca. A questo riguardo va osservato che la normativa italiana, di attuazione di quella comunitaria, prevede una forma di responsabilità della banca quasi oggettiva. Il testo di riferimento è il d.lgs. n. 11 del 27 gennaio 2010. Più precisamente l'art. 10 comma 2 di questo testo normativo prevede che: "quando l'utente 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'utente 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. **È onere del prestatore di servizi di pagamento ... fornire la prova** della frode, del dolo o della colpa grave dell'utente".

Il meccanismo previsto dal legislatore comunitario è basato sull'autorizzazione delle operazioni. Il cliente che non ha autorizzato un'operazione può limitarsi a disconoscere detta operazione. In questo caso, si inverte l'onere della prova e spetta alla banca dimostrare che vi è colpa o dolo del proprio cliente. **Si tratta di una prova difficile da rendere** e spesso le richieste di risarcimento rivolte dal cliente alla banca vengono accolte dall'Arbitro Bancario

Finanziario.

Nel caso in commento, la responsabilità della banca viene affermata per non essersi l'intermediario dotato di un sistema di autenticazione "forte". La disposizione di riferimento è l'art. 1 lett. q-bis d.lgs. n. 11 del 2010 secondo cui per "**autenticazione forte**" si intende: "un'autenticazione 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". L'elemento della conoscenza è tipicamente la password usata dal cliente. L'elemento del possesso consiste, ad esempio, nell'utilizzo di un telefono cellulare, che è in possesso fisico dell'utente. L'elemento dell'inerenza fa riferimento all'impronta digitale oppure al riconoscimento facciale. Ciò che in ogni caso emerge dalla definizione è che le banche devono dotarsi di sistemi di sicurezza doppia basati, alternativamente, su: conoscenza + possesso oppure conoscenza più inerenza oppure possesso + inerenza. Un sistema di sicurezza doppia è più difficilmente violabile dai malfattori e vale a escludere la responsabilità della banca.

Tornando all'esame della decisione n. 9549 del 2021 dell'Arbitro Bancario Finanziario, vennero poste in essere nel giro di due soli minuti due distinte transazioni online tramite carta di credito. Le operazioni furono autenticate mediante: **inserimento delle credenziali statiche + inserimento del codice dinamico OTP** (one time password). La banca in questione dunque, per evitare intrusioni di terzi, aveva dato al cliente un nome utente e una password "statica", cui si aggiungeva l'invio di una password "dinamica" per il compimento dell'operazione dispositiva. Questo sistema di difesa è solo apparentemente a due fattori: credenziali statiche + password dinamica "usa e getta". In realtà, secondo la decisione dell'ABF in commento, si tratta di un meccanismo con un unico livello di sicurezza (autenticazione c.d. "debole", non "forte"). Difatti tutto ciò che serve per effettuare l'operazione (inserimento codice utente + inserimento password statica + inserimento password dinamica) attiene alla sfera della "conoscenza" in capo al cliente.

Nel caso in esame i malfattori erano a conoscenza di nome utente e password del cliente della banca. Con uno stratagemma, ossia mediante telefonata, si fanno rivelare dal cliente la singola e specifica password generata una tantum dal sistema per movimentare la carta di credito. **I malviventi hanno potuto distrarre somme dalla carta del cliente senza avere il "possesso" di alcunché** (come potrebbe essere un telefono cellulare), bensì sulla base di mere informazioni di cui sono venuti in possesso. L'Arbitro Bancario Finanziario ritiene che la banca non disponga di sistemi di sicurezza a doppio fattore (autenticazione forte) e afferma la responsabilità dell'intermediario per le somme distratte, che dovranno essere rimborsate dalla banca al cliente.