Pagamenti fraudolenti tramite e-banking

Oggetto: **Abuso e truffa** Numero del caso: **2017/09**

> Il cliente era stato vittima di truffatori che erano riusciti ad intercettare i suoi dati di login al sistema e-banking e ad effettuare dei versamenti a beneficio di una ditta titolare di un conto presso una banca inglese. La banca era disposta a indennizzarlo unicamente per la metà dell'importo accreditato in tal modo. Il cliente riteneva l'offerta insufficiente. Anche nell'ambito della procedura di mediazione, la banca ha recisamente contestato qualsiasi obbligo di indennizzo, ma ha mantenuto l'offerta di versargli, a titolo di gesto di cortesia, un importo pari al 50% del danno. Su consiglio dell'Ombudsman, il cliente ha accettato l'offerta della banca.

Il cliente aveva ricevuto una telefonata da un interlocutore che si era presentato come ingegnere informatico alle dipendenze del suo fornitore di servizi Internet. Egli aveva detto che a seguito di un attacco informatico, nel sistema si era introdotto un malware che poteva influire sull'accesso ai sistemi di e-banking e che per eliminarlo, necessitava delle coordinate bancarie. Dopo avergli forniti i dati richiesti, il cliente aveva ricevuto l'istruzione di accedere ai siti web delle banche in questione dopo aver inserito un codice specifico. Una volta eseguita questa istruzione, il sito web spariva ogni volta per un breve istante dallo schermo, prima di riapparire nuovamente. L'interlocutore gli aveva infine detto che ora lui e i suoi collaboratori avrebbero potuto eliminare il malware. In seguito, il cliente si era connesso ai sistemi e-banking delle sue banche con la procedura d'accesso abituale, senza notare nulla di particolare. Alcuni giorni dopo, nel connettersi nuovamente con il sistema e-banking della banca, il cliente aveva constatato che era stato eseguito un pagamento, da lui non ordinato, a favore di un conto presso una banca inglese intestato a una ditta a lui sconosciuta. Ne aveva quindi immediatamente informato la banca, che gli aveva assicurato di intraprendere i passi necessari. Era infine emerso che al momento in cui la banca del cliente era stata informata della truffa, il denaro era già stato prelevato dal conto cliente della banca destinataria.

Secondo il cliente, che aveva in seguito sporto denuncia penale contro ignoti, la banca era tenuta a rimborsare il pagamento avvenuto senza suo ordine. Faceva valere il fatto che le altre banche presso cui deteneva dei conti, che erano pure state vittime del medesimo tipo di truffa, o non avevano eseguito i pagamenti, o avevano reagito per tempo presso le banche destinatarie, ottenendo il rimborso dei pagamenti effettuati senza il suo ordine, cosicché egli non aveva subito alcun danno. Egli si era connesso al sistema e-banking attenendosi alla procedura d'accesso prevista e non era responsabile del fatto che, in tale frangente, terzi avessero potuto disporre dei suoi conti. Inoltre la banca avrebbe dovuto riconoscere il carattere inusuale del pagamento, ritenuto che egli non aveva mai effettuato pagamenti a favore di terzi attingendo a tale conto. Sempre a dire del cliente, successivamente alla segnalazione dell'accaduto, la banca aveva atteso troppo prima di contattare la banca destinataria, consentendo in tal modo agli autori di disporre del denaro. Infine, inizialmente la banca gli avrebbe confermato telefonicamente di aver potuto bloccare l'importo presso la banca destinataria. La banca ha dal canto suo respinto ogni obbligo d'indennizzo, dichiarandosi unicamente disposta a rimborsare al cliente, a titolo di cortesia, il 50% dell'importo trasferito. Il cliente si è quindi rivolto all'Ombudsman chiedendogli di avviare una procedura di mediazione.

All'Ombudsman la banca ha esposto in modo ancor più dettagliato la posizione già comunicata al

cliente. A suo avviso i trasferimenti contestati erano stati eseguiti successivamente all'inserimento dei necessari dati d'accesso nel sistema e-banking, senza che terzi avessero esercitato alcuna influenza sui sistemi della banca. In virtù degli accordi contrattuali in materia di e-banking, essa era autorizzata ad eseguire transazioni di questo tipo. Il cliente era tenuto a custodire accuratamente i mezzi d'accesso e a non fornirli a terzi, per nessun motivo. Inoltre, a suo dire, non sussisteva nessun obbligo contrattuale della banca di verificare anche la plausibilità di ogni pagamento impartito tramite e-banking. Era chiaro che nel caso in esame, stando alle dichiarazioni del cliente, dei terzi avevano intercettato i dati d'accesso del cliente infettando con un malware il suo apparecchio per l'inserimento dei dati d'accesso, misfatto che era stato compiuto al di fuori della sfera d'influenza della banca. Per la banca non era comprensibile il motivo per cui il cliente, successivamente al colloquio con il sedicente ingegnere del suo fornitore di servizi Internet, non avesse contattato la banca per informarsi se l'accesso ai suoi sistemi e-banking fosse effettivamente disturbato. Secondo la banca, in conformità con il contratto, i rischi connessi al sistema e-banking che esulano dalla sfera di competenza della banca devono essere sopportati dal cliente. Per il resto, la banca aveva potuto dimostrare di aver informato tempestivamente dell'accaduto la banca destinataria il mattino stesso in cui era venuta a conoscenza dell'accaduto e di aver richiesto la restituzione dell'importo accreditato. Purtroppo la banca destinataria non aveva reagito, cosicché era stato necessario indirizzarle un sollecito. Il cliente avrebbe ritenuto, a torto, che il primo intervento della banca fosse avvenuto al momento in cui, in realtà, era stato inviato il sollecito, giungendo così all'erronea conclusione che la banca avesse reagito tardivamente. Infine, quanto dichiarato dalla banca in merito al fatto che l'importo avrebbe potuto essere bloccato, concerneva un secondo bonifico contestato dal cliente, nel qual caso il denaro aveva effettivamente potuto essere bloccato tempestivamente e restituito al cliente.

Anche nei confronti dell'Ombudsman la banca ha respinto ogni obbligo di indennizzo, ribadendo tuttavia nuovamente l'offerta di rimborsare al cliente il 50% dell'importo a titolo di cortesia. Dopo aver ponderato gli argomenti di entrambe le parti, l'Ombudsman ha consigliato al cliente di accettare l'offerta transattiva della banca. Difatti, sulla base dei fatti descritti, anche a lui è parso plausibile che i truffatori avessero agito sul sistema del cliente e che tale atto, effettivamente, esulasse dalla sfera d'influenza della banca. Come da prassi in uso nel settore, era stato concordato contrattualmente che tali rischi dovevano essere sopportati dal cliente. Sulla base dei fatti descritti, restavano diversi dubbi in merito al fatto che il cliente fosse stato sufficientemente diligente in occasione del colloquio telefonico sopra descritto. All'Ombudsman non è inoltre nota nessuna decisione giudiziaria ai sensi della quale una banca sia tenuta a verificare la plausibilità degli ordini impartiti tramite e-banking ed eseguiti automaticamente. A suo avviso, la giurisprudenza sviluppata in relazione agli ordini impartiti fraudolentemente, che giungono alla banca per altri canali e che sono esaminati dai collaboratori, non è ipso facto applicabile al caso in esame. Inoltre, anche alla luce della giurisprudenza menzionata, il solo fatto che nessun ordine a favore di terzi fosse mai stato impartito dal conto in esame non rappresenta un criterio sufficiente per qualificare l'ordine come inusuale. La banca ha infine potuto dimostrare di aver tempestivamente informato la banca destinataria della truffa, non appena appreso l'accaduto. Per questi motivi, l'Ombudsman ha ritenuto adeguata la proposta transattiva della banca e per finire, su consiglio di quest'ultimo, il cliente l'ha accettata.