Richiesta di risarcimento danni per un pagamento e-banking attivato da ignoti

Oggetto: **Abuso e truffa** Numero del caso: **2020/14**

> Questo caso è un altro esempio di truffa di “phishing”. Una domenica, il cliente ha cercato senza successo di accedere al sistema di e-banking della banca per controllare il conto di risparmio di sua moglie. In seguito a questo tentativo, ha ricevuto un SMS che menzionava l’importo di 3’000 franchi, che ha scambiato per il saldo del conto. Lunedì mattina, il cliente ha potuto accedere di nuovo e senza problemi al sistema di e-banking. Egli ha allora notato un pagamento non autorizzato di oltre 3’000 franchi e ha immediatamente denunciato l’incidente alla banca. Quest’ultima ha contattato la banca destinataria per richiedere la restituzione dell’importo, ma solo alle 16:30 via SWIFT. Poiché i fondi non potevano essere bloccati sul conto del destinatario, il cliente ha chiesto alla banca un risarcimento per conto di sua moglie. Vista l’impossibilità di raggiungere un accordo con la banca, il cliente si è infine rivolto all’Ombudsman. La banca ha però continuato ad escludere qualsiasi concessione nella procedura di mediazione.

Per il suo sistema di e-banking, la banca utilizza un processo di autenticazione a due fattori con un codice di verifica (mTAN). Quando un cliente inserisce i suoi dati di accesso, questo codice viene inviato al telefono cellulare ch’egli ha precedentemente registrato. Il cliente deve inserire questo codice nel sistema e-banking per confermare il login. Nel caso in esame, quando, una domenica, il cliente ha inserito questo codice per connettersi, lo schermo è diventato nero ed è apparso un messaggio che indicava che erano in corso lavori di manutenzione sul sito di e-banking della banca. Il cliente ha poi interrotto il processo e ha provato ad accedere di nuovo, anche questa volta senza successo. Viste le circostanze, c’è ragione di credere che il computer del cliente sia stato probabilmente infettato e ch’egli abbia inserito i dati di accesso su un “sito di phishing”, che sembrava il sito della banca ma che era stato creato dai truffatori per permettere loro di intercettare i dati in questione. Utilizzando i dati rubati, i terzi sconosciuti si sono poi collegati al sistema di e-banking e hanno addebitato il conto della moglie a favore del conto che il “money mule” deteneva presso un’altra banca. Il procedimento penale avviato dal cliente ha rivelato che la destinataria era una studentessa, che è anche stata ingannata sulla vera natura della transazione e che ha trasferito il denaro ai truffatori in cambio del pagamento di un compenso. Tuttavia, non è stato possibile stabilire l’identità dei truffatori e reperire il denaro.

Il problema principale in casi del genere è che di solito l’importo trafugato non può essere recuperato presso chi ha approfittato della truffa. Si pone quindi la domanda se è il cliente o la banca a dover sopportare tutta o parte della perdita. La risposta a questa domanda dipende dalle disposizioni contrattuali applicabili. Di regola, queste stabiliscono che la banca può (e deve) eseguire qualsiasi ordine di pagamento inserito nel sistema di e-banking, a condizione che gli strumenti di legittimazione trasmessi siano corretti. Per quanto riguarda la responsabilità per uso improprio, i contratti si basano generalmente sulla cosiddetta teoria della “sfera di rischio”, secondo la quale ogni parte è in linea di principio responsabile degli errori che rientrano nella propria sfera d’influenza e che avrebbe potuto evitare esercitando la necessaria attenzione. Nel caso specifico, la banca si è basata su queste disposizioni contrattuali per escludere la propria responsabilità, sostenendo che i suoi sistemi funzionavano perfettamente e che il cliente era l’unico responsabile della sicurezza del suo

dispositivo, che molto probabilmente era stato infettato.

Tuttavia, nel caso in esame si poneva pure la questione di sapere se la banca avrebbe dovuto reagire più rapidamente presso la banca ricevente in modo che l'importo trasferito dai truffatori potesse ancora essere bloccato. Mentre la banca riteneva di aver agito per tempo, l'Ombudsman ha considerato ch'essa ha impiegato molto tempo.. Anche se il cliente aveva segnalato l'incidente la mattina presto, la banca aveva agito solo nel tardo pomeriggio. Secondo l'esperienza dell'Ombudsman, una caratteristica comune a questo tipo di frode è che gli autori o i muli di denaro, da loro istruiti quali ausiliari, ritirano il denaro dal conto del destinatario immediatamente dopo averlo ricevuto, evitando così che i fondi vengano bloccati. Poiché una discussione sui tempi di reazione della banca poteva essere risparmiata nell'ipotesi in cui un intervento immediato dopo la notifica della frode sarebbe stato comunque tardivo, dato che il denaro era già stato prelevato, l'Ombudsman ha contattato la banca destinataria per chiedere quando il prelievo ha avuto luogo. Tuttavia, la banca ha rifiutato di fornire informazioni dettagliate, appoggiandosi sul segreto bancario, e ha semplicemente dichiarato che elabora sempre tali notifiche senza ritardo. L'Ombudsman non è stato quindi in grado di chiarire questo punto come avrebbe voluto, ma ha informato il cliente che i documenti dell'indagine penale potrebbero essere utili a questo proposito.

Anche se l'Ombudsman ha riscontrato che le banche possono gestire incidenti di questo genere in modo molto diverso le une dalle altre, egli ha pure notato che a volte esse sono più generose della banca del caso in esame. Così, di fronte al rifiuto di quest'ultima di fare un gesto a favore del cliente, l'Ombudsman non ha purtroppo avuto altra scelta che chiudere il caso dopo aver inviato il suo parere finale al cliente.