Diritto Bancario

Frodi informatiche: brevi appunti

di **Fabio Fiorucci, Avvocato**

Le frodi informatiche mirano a catturare le credenziali di accesso ai servizi bancari online, al fine di effettuare operazioni di pagamento non autorizzate dal cliente. Una delle frodi più comuni è il phishing, in cui la vittima riceve un'e-mail che la invita a inserire dati personali attraverso un link a un sito che solitamente imita quello della propria banca. Esistono varianti di questa truffa, come il vishing, che avviene tramite telefonate, e lo smishing, che sfrutta messaggi SMS.

Frodi più sofisticate includono lo spoofing, in cui i truffatori mascherano la provenienza di e-mail, SMS o telefonate, facendo sembrare che il messaggio provenga dall'intermediario bancario. Un'altra tecnica avanzata è il "man in the browser," un tipo di malware che si interpone tra il computer della vittima e il sistema della banca. Un caso ancora diverso è il boxing, che consiste nell'intercettare e sottrarre carte di pagamento durante la loro spedizione al cliente tramite il servizio postale.

È consolidato il convincimento giurisprudenziale di legittimità secondo cui, in caso di operazioni eseguite con strumenti elettronici, è ragionevole addossare agli intermediari il rischio che i codici di accesso dei clienti siano usati da soggetti non autorizzati «anche al fine di garantire la fiducia degli utenti nella sicurezza del sistema»: si tratta di un rischio prevedibile ed evitabile con l'adozione di misure adatte a verificare la riconducibilità delle operazioni alla volontà del cliente. La responsabilità della banca è esclusa solo quando l'uso indebito degli strumenti di pagamento dipende da dolo del titolare o da suoi comportamenti talmente incauti da non poter essere fronteggiati in anticipo. In definitiva, chi eroga servizi di pagamento deve tenere un livello di diligenza particolarmente elevato al fine di assicurare la fiducia degli utenti nella sicurezza del sistema e, in caso di contestazione, deve fornire la prova della riconducibilità dell'operazione al cliente (Cass. n. 13204/2023; Cass. n. 26916/2020; Cass. n. 18045/2019).

Le frodi informatiche sono frequentemente trattate nei giudizi dell'Arbitro Bancario Finanziario. Di seguito, una breve rassegna dei più recenti orientamenti espressi:

in caso di spoofing tramite SMS l'utente risponde per colpa grave solo in presenza di indici gravi di inattendibilità o di anomalia dei messaggi inviati dai frodatori (ABF Bari n. 3606/2023);

in caso di boxing l'utente che comunica ai frodatori il PIN della carta può sopportare parte del danno subito (ABF Napoli n. 9104/2023);

la variazione del numero di telefono associato a un conto di pagamento richiede l'adozione di un'autenticazione forte (ABF Torino n. 3955/2023);

in caso di frode attuata mediante invio di un QR code al cliente per autorizzare un'operazione, l'intermediario non è tenuto al rimborso se sussiste la colpa grave del cliente (ABF Torino n. 92/2023):

se il cliente è vittima di una frode informatica sofisticata, come il man in the browser, la sua condotta non è generalmente caratterizzata da colpa grave, salva la sussistenza di ulteriori elementi (ABF Roma n. 3793/2023).