

Attenti ai rischi dell'home banking «Password per ogni operazione e standard di sicurezza adeguati»

Luigi Manfredi

■ MILANO

QUAL È la responsabilità della banca per le operazioni elettroniche poste in essere abusivamente da terzi a danno di clienti titolari di conti correnti e di carte di credito? E' caldissimo il tema delle implicazioni giuridiche dell'home banking. Lo affrontiamo con Simona Daminelli e Francesca Fiorito, rispettivamente partner e associate di 'La Scala società tra avvocati'.

Nel caso di home banking quali obblighi spettano alla banca per la verifica della riconducibilità alla volontà del cliente di un'operazione effettuata con strumenti elettronici?

«La banca è tenuta a fornire password associate univocamente alla singola operazione e, quindi, non riutilizzabili. Tale necessità è stata prevista dalla direttiva PSD2 (Payment Services Directive). La chiavetta fisica (il token, ndr) gradualmente scomparirà».

Quando la banca risponde o non risponde di un danno patito per un'operazione fraudolenta compiuta da terzi (orientamento della Suprema Corte 9158/2018 in tema di onere della prova)?

«La banca per andare esente da responsabilità è tenuta a dimostrare la riconducibilità dell'operazione al cliente e di aver approntato tutte le opportune cautele. Tale principio era già stato previsto da una pronuncia della Cassazione nel 2017 secondo la quale, ai fini del rigetto della domanda risarcitoria del cliente che subisce la sottrazione dei co-

dici di accesso e l'effettuazione di operazioni da parte di terzi, non è sufficiente dar rilievo al suo comportamento incauto, rientrando nell'area del rischio professionale del prestatore dei servizi di pagamento la possibilità che un terzo non autorizzato utilizzi i codici di accesso».

Dati sensibili: cosa dice il Codice di protezione dei dati?

«L'art. 15 prevede che chiunque cagioni un danno ad altri per effetto del trattamento dei dati personali è tenuto al risarcimento ai sensi dell'art. 2050 del codice civile (responsabilità per attività pericolosa). L'art. 31 dispone che i dati personali siano custoditi e controllati in modo da ridurre al minimo, mediante l'adozione di idonee misure di sicurezza, i rischi di distruzione o perdita dei dati, di accesso non autorizzato o di trattamento non consentito».

Quali accorgimenti deve attuare la banca per prevenire l'illegittima captazione dei dati?

«Tutti i dati e le informazioni sui siti delle banche o sulle App sono protetti da avanzati sistemi di crittografia. Inoltre, per l'accesso ai servizi on-line la banca deve richiedere una combinazione di password statiche e dinamiche, ossia un codice titolare (statica), un codice pin (statica) e un codice generato di volta in volta OTP (dinamica). In aggiunta, per le operazioni meno frequenti, viene utilizzato come elemento di ulteriore sicurezza un codice sms inviato al numero di cellulare del cliente».

Che tipo di responsabilità è quella ex articolo 2050 del codice civile?

«Si tratta di una forma di respon-

sabilità oggettiva ed extracontrattuale. L'esercente di un'attività pericolosa deve dimostrare, non solo di aver adottato tutte le misure idonee ad evitare il danno (cosiddetta 'prova liberatoria'), ma anche che tra l'attività pericolosa e l'evento non ci sia un nesso causale (ad esempio quando l'evento sia stato determinato da un fattore esterno imprevedibile ed inevitabile)».

Quale standard di sicurezza deve garantire comunque la banca?

«La norma ISO/IEC 27001 certifica lo standard di riferimento internazionale per la gestione nella sicurezza delle informazioni».

Phishing: quando l'istituto di credito è responsabile della sottrazione dei dati?

«E' responsabile ove non dimostri di aver approntato gli standard di sicurezza adeguati mediante la combinazione delle password identificative statiche e dinamiche. E' invece esente da responsabilità ove l'evento sia stato determinato dal dolo del titolare o sia imputabile a comportamenti talmente incauti da non poter essere fronteggiati in anticipo».



La sentenza della Cassazione

In caso di operazione fraudolenta compiuta da terzi, la Suprema Corte stabilisce che «la banca per andare esente da responsabilità è tenuta a dimostrare la riconducibilità dell'operazione al cliente e di aver approntato tutte le opportune cautele»



SERVIZI ONLINE PROTETTI

**Sotto Simona
Daminelli,
partner di 'La
Scala società
tra avvocati',
tra i principali
studi legali
italiani nel
contenzioso
bancario e
fallimentare e
leader
riconosciuto
nell'attività
giudiziale di
recupero
crediti.
Comprende
attualmente
circa 190
professionisti
e uno staff
di oltre
100 persone**



Peso:65%