**Convegno Orizzonti del Diritto Commerciale**

 **L’evoluzione tecnologica e il diritto commerciale**

 **Prof.Marilena Rispoli Farina**

 **Università di Napoli FedericoII**

**ABSTRACT: La Strong Customer Authentication**

**Settore :I servizi di pagamento on line**

La Direttiva Payment Service Directive 2 ha radicalmente innovato non solo l’ambito dei servizi di pagamento, comprendendo in essi anche quelli prestati *online*, ma anche le modalità attraverso le quali gli utenti dei servizi di pagamento potranno usufruire dei servizi medesimi:introducendo, cioè, una modalità di accesso“forte”, denominata a tal fine “*strong customer authentication*”.

Scopo del *Paper* che si intende presentare al Convegno è quello di mostrare le interazioni tra *strong customer authentication* e le regole generali di applicazione della PSD 2: quest’ultima, infatti, statuisce che il cliente che usufruisca di un servizio di pagamento non sopporterà alcuna perdita derivante da un utilizzo illecito dello strumento di pagamento medesimo, laddove la banca non dimostri che aveva approntato correttamente tutte le misure necessarie volte a garantire al cliente un accesso sicuro.

Per accesso sicuro si intende il possesso, da parte del cliente, di almeno due tra tre elementi: *Knowledge*, cioè qualcosa che egli conosce (come ad esempio un PIN o una password); *Ownership*, e cioè qualcosa che possiede (per esempio smartphone, chip, token); oppure *Inherence*, e cioè una connotazione essenziale del cliente ed a lui riconducibile univocamente (e.g. impronta, retina). I due elementi prescelti devono essere tra loro indipendenti, e l’eventuale compromissione dell’uno non deve inficiare anche l’altro.

Sulla base della previgente regolamentazione della prestazione dei sevizi di pagamento, introdotta con la PSD1, la dottrina e la Giurisprudenza dell’Arbitro Bancario ( alle cui copiose decisioni si

rinvia) si erano espresse in senso non sempre favorevole al cliente consumatore in punto di responsabiltà per operazioni fraudolente nei servizi on line.

La regola generale prevista dalla PSD 2 è che la *strong customer authentication* sia obbligatoria in tutti i casi in cui il cliente acceda al suo conto di pagamento online; quando dispone un’operazione di pagamento elettronico; quando effettua una qualunque operazione, tramite un canale a distanza, che possa comportare un rischio di frode nei pagamenti o abusi. Le statuizioni immediate derivanti da tale disciplina si sono avute nell’introduzione del comma 2 - *bis* all’art. 12 de d.lgs. n. 11/2010, come modificato dal d.lgs. 218/2017, di attuazione della nuova direttiva. Tale comma espressamente stabilisce che: “*Salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente. Il beneficiario o il prestatore di servizi di pagamento del beneficiario rimborsano il danno finanziario causato al prestatore di servizi di pagamento del pagatore se non accettano l'autenticazione forte del cliente*”. Il legislatore nazionale, quindi, ha voluto tutelare in maniera adeguata il cliente del prestatore del servizio di pagamento nell’eventualità in cui il prestatore del servizio non sia stato in grado di proteggere il conto di pagamento di questi e, più in generale, le sue informazioni personali dagli accessi fraudolenti.

A conforto della difficoltà di percepire il valore del nuovo disposto si può menzionare una recentissima decisione dell’ABF, Collegio di Bologna, n. 7393/2018, che si è posta in controtendenza sia con la più stringente regolamentazione proposta dal legislatore nazionale ed europeo, sia con il precedente orientamento dell’Arbitro Bancario Finanziario, sanzionando più severamente il cliente che fosse vittima, inconsapevole, del noto fenomeno del *phishing*: avendo inserito i propri dati personali in risposta ad una mail inviata da un soggetto che artatamente fingeva di essere l’intermediario presso il quale era radicato il conto di pagamento. In taleo casi il Collegio ha ritenuto di dover respingere il ricorso del pagatore, non facendo buon conto detto dell’esplicito dettato della nuova direttiva che ritiene responsabile il cliente dell’intermediario soltanto in caso di colpa grave.

**BIBLIOGRAFIA ESSENZIALE**

DE MATTEIS A., *La strong customer authentication*, in *Atti del convegno Recepimento PSD2 e novità sui servizi di pagamento. Decreto Legislativo 15 dicembre 2017 n. 218 (G.U. n. 10 del 13 gennaio 2018)*, Milano, 28 marzo 2018.

CASCINELLI F. - PISTONI V. - ZANETTI G., *La Direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno*, in *dirittobancario.it*, 2016.

RISPOLI FARINA M., *Responsabilità degli intermediari bancari e finanziari e sistemi di internet banking: aggressione informatica e protezione del cliente*, in *Innovazione e Diritto*, 6, 2014.