Circolare n. 285 del 17 dicembre 2013 «Disposizioni di Vigilanza per le banche» - 16° aggiornamento. Sicurezza dei pagamenti via internet

1. Premessa

Con il presente aggiornamento è modificato il Capitolo 4 "Sistemi informativi" del Titolo IV, Parte Prima della Circolare, introducendo, tra l'altro, una specifica Sezione VII volta a disciplinare gli obblighi imposti alle banche che prestano servizi di pagamento tramite canale internet.

Sono in tal modo recepiti nell'ordinamento italiano gli "Orientamenti in materia di sicurezza dei pagamenti tramite internet" emanati dall'Autorità Bancaria Europea (*European Banking Authority* – EBA) ([1]) con l'obiettivo di accrescere il livello di sicurezza del settore, favorendo l'adozione di requisiti minimi comuni su base europea.

Gli obblighi facenti capo alle banche in forza delle "*Recommendations for the security of internet payments*" (di seguito "Raccomandazioni") del 31 gennaio 2013, applicabili dal 1° febbraio 2015 ([2]), sono pertanto sostituiti dagli obblighi previsti dagli Orientamenti secondo quanto specificato nella Sezione VII sopra richiamata.

2. Contenuto dell'intervento

Le nuove Disposizioni si applicano alle operazioni di pagamento effettuate tramite il canale internet identificate dagli Orientamenti ([3]). Gli obblighi imposti integrano e specificano le disposizioni sul Sistema informativo con riferimento ai seguenti profili: *governance* e organizzazione del sistema informativo; gestione del rischio informatico; requisiti per assicurare la sicurezza informatica e il sistema di gestione dei dati.

Specifici presidi di natura fisica, logica e organizzativa sono imposti agli operatori con l'obiettivo di ridurre il rischio di frodi e assicurare una corretta gestione delle informazioni sensibili detenute dalla banca. In particolare, le banche sono chiamate ad adottare:

- modalità rafforzate di verifica dell'identità del cliente (c.d. "autenticazione forte"), per l'avvio di un'operazione di pagamento, nonché per l'accesso ad informazioni sensibili, secondo gli standard stabiliti dall'Orientamento n. 7;
- limiti ai tentativi di log-in/accesso ad aree riservate e alla durata delle sessioni di lavoro;
- meccanismi di monitoraggio dell'operatività, al fine di prevenire, identificare, bloccare eventuali operazioni fraudolente.

Le banche sono inoltre chiamate ad accrescere il grado di protezione offerto alla propria clientela, assicurando la disponibilità di informazioni accurate e tempestive sulle tecnologie in uso, sulle loro modalità di utilizzo, nonché sugli strumenti di tutela disponibili in caso di frode. Tali aspetti sono inoltre specificamente inseriti nei contratti.

Gli Orientamenti forniscono, infine, alcuni esempi di prassi applicative degli obblighi in essi contenuti. Tali esempi non hanno natura vincolante. Resta ferma la possibilità per le banche di tenerne conto nella definizione delle modalità di attuazione delle disposizioni in esame.

---

[1] http://www.eba.europa.eu/documents/10180/1004450/EBA_2015_IT+Guidelines+on+Internet+Payments.pdf/b9c5dee9-78bd-47c5-a80c-4d2f3f8a1de2

[2] Cfr. 15° aggiornamento della Circolare 263/2006, trasfuso nella Circolare 285/2013 con l'11° aggiornamento del 21 luglio 2015.

[3] Si tratta, in particolare, di: (a) esecuzione dei pagamenti con carta; (b) esecuzione di bonifici; (c) emissione o modifica di mandati elettronici di addebito diretto e (d) trasferimento di moneta elettronica tra due conti di moneta elettronica.

In linea con l'impostazione generale della disciplina in materia di controlli interni e gestione dei rischi e fermi restando i casi in cui gli Orientamenti prescrivono obblighi specifici (come nel caso dell'utilizzo dell'"autenticazione forte"), le banche applicano le presenti disposizioni secondo il principio di proporzionalità, cioè tenuto conto della dimensione e complessità operativa, della natura dell'attività svolta, della tipologia dei servizi prestati.

3. Destinatari

Le disposizioni del presente aggiornamento si applicano alle banche, alle capogruppo di gruppi bancari, alle succursali di banche extracomunitarie autorizzate in Italia e al Bancoposta.

4. Entrata in vigore

Le presenti disposizioni entrano in vigore il giorno successivo a quello di pubblicazione nel sito informatico della Banca d'Italia.

Le banche si adeguano agli obblighi imposti entro il 30 settembre 2016. Per l'assolvimento degli obblighi che richiedono una modifica di rapporti contrattuali, le banche adeguano i contratti in essere alla data di entrata in vigore delle presenti disposizioni alla prima scadenza contrattuale. Entro il 30 ottobre 2016 esse trasmettono alla Banca Centrale Europea o alla Banca d'Italia una relazione, approvata dall'organo con funzione di supervisione strategica, sugli interventi effettuati sulla struttura organizzativa e di controllo nonché sui sistemi informativi al fine di assicurare il rispetto degli obblighi introdotti con il presente aggiornamento.