



Finanstilsynet uddyber kravene til procedurer for anvendelse af stærk kundeautentifikation



Martin Christian Kruhl
Partner, Ph.D.

I juli 2020 gennemførte Finanstilsynet en inspektion i landets største udbyder af betalingstjenester, Nets Danmark A/S (Nets), for at bedømme, om Nets, som udbyder af betalingstjenester, havde anvendt stærk kundeautentifikation ved betalingstransaktioner.

I et sammendrag af redegørelsen om inspektionen, der er offentliggjort på Finanstilsynets hjemmeside, har Finanstilsynet uddybet, hvordan disse særlige regler om anvendelse af stærk kundeautentifikation i betalingsloven skal fortolkes. Mere konkret har Finanstilsynet konkretiseret tre forskellige forhold vedrørende autentifikation, der gennemgås nedenfor.

Lovgivning på området

Betalingsloven implementerer EU's 2. betalingsdirektiv, også kaldet PSD2.

I henhold til betalingsloven, skal en udbyder af betalingstjenester sikre, at betalingstransaktioner kun kan gennemføres, hvis der anvendes stærk kundeautentifikation.

Stærk kundeautentifikation kaldes også to-faktor autentifikation og indebærer, at brugeren skal kunne påvise sin identitet ved at anvende to eller flere uafhængige elementer. Disse elementer skal være enten *viden* (fx et

kodeord), *besiddelse* (fx et betalingskort) eller *iboende egenskab* (fx stemmegenkendelse). To uafhængige elementer kan således udgøre kombinationen af et kodeord og en engangskode, hvor sidstnævnte sendes til kundens mobiltelefon eller mobile enhed.

Finanstilsynets uddybning af kravene

#1 - Ubemandede terminaler

Først gør Finanstilsynet rede for, hvorfor der i forbindelse med betalingstransaktioner via ubemandede terminaler, som fx parkeringsautomater og billetautomater, kræves anvendelse af stærk kundeautentifikation.

Finanstilsynet gør det klart, at en betalingstjenesteudbyder *kan* afvige fra brug af kundeautentifikation i de tilfælde, hvor brugeren betaler en befordringsbillet eller et parkeringsgebyr; dette kræver dog, at betalingstjenesteudbyderen i sit eget system er i stand til at identificere, at betalingstransaktionen bliver iværksat med netop det formål. Hvis udbyderen ikke er i stand til at identificere dette, skal der anvendes stærk kundeautentifikation.

#2 - Aflæsning af chip uden mulighed for brug af anden identifikation

Dernæst gør Finanstilsynet opmærksom på, at en betalingstjenesteudbyder ikke må indløse betalinger i situationer, hvor betaling kan igangsættes via betalingsterminaler, hvor transaktionen alene baseres på aflæsning af chip i kreditkortet, dvs. uden at der kræves kodeord eller andet "viden"-element.

#3 - Magnetstribe som besiddelselement

Afslutningsvis fremfører Finanstilsynet sit synspunkt om brug af magnetstribe som besiddelselement i en stærk kundeautentifikationsproces.

Finanstilsynet finder, at en magnetstribe - i sin nuværende form - ikke kan regnes som besiddelselement, fordi en magnetstribe relativt let kan enten kopieres eller genskabes.

Da en magnetstribe er utilstrækkelig som besiddelselement, vil betalingstransaktioner, der er igangsat med brug af magnetstribe i kombination med et kodeord ikke kunne anses for at være to-faktor godkendt.

Fagområder	Regulatoriske forhold i den finansielle sektor, International handel, investeringer, reguleringer og compliance, FinTech
------------	--------------------------------------------------------------------------------------------------------------------------

Sektorer	Financial Services
----------	--------------------
