

JUNI 2019

Internetforretninger skal være særligt opmærksomme på nye EU-regler for betalinger



Krav om stærk kunde- autentifikation fra 14. september 2019

Stærk kundeautentifikation betyder, at der skal anvendes mindst to faktorer ved godkendelse af en betaling.



Internetforretninger skal især være opmærksomme

Internetforretninger skal sikre, at de er klar til at modtage betalinger godkendt med stærk kundeautentifikation. Er man i tvivl, bør man tage kontakt til sin kortindløser eller gateway-udbyder.



Forretninger kan blive afskåret fra at modtage betalinger

Betalinger, der ikke er godkendt med stærk kundeautentifikation, kan som udgangspunkt ikke gennemføres fra den 14. september 2019.

Nye EU-regler for betalinger

Den 14. september 2019 træder nye EU-regler for betalinger i kraft. Reglerne udspringer af det reviderede betalingstjenestedirektiv, PSD2, som blev implementeret i dansk lov i januar 2018. Reglerne, der er specificeret i en delegeret forordning fra Europa-Kommissionen¹, skal bl.a. medvirke til at gøre det mere sikkert at lave elektroniske betalinger. Dette sker først og fremmest ved, at der indføres et krav om stærk kundeautentifikation.

Stærk kundeautentifikation – eller tofaktor-autentifikation – indebærer, at der skal anvendes mindst to faktorer til at godkende en betaling. De to faktorer skal være noget, betaleren ved (fx et password); noget, betaleren er (fx et fingeraftryk); eller noget, betaleren har (fx et betalingskort).

Ifølge tal fra Nationalbanken blev der i 2018 begået misbrug med danske betalingskort for ca. 301 mio. kr. Heraf udgjorde misbrug i onlinehandel ca. 236 mio. kr., og dermed knap 80 pct. af det samlede misbrug. Det er bl.a. dette misbrug, de nye regler skal være med til at dæmme op for.

Krav om stærk kundeautentifikation

I fysisk handel i Danmark anvendes der allerede i dag stærk kundeautentifikation i form af autentifikation via chipkort (noget, betaleren har) og pinkode (noget, betaleren ved).

I ikke-fysisk handel, primært inden for onlinehandel, har der derimod traditionelt set ikke været anvendt stærk kundeautentifikation i vidt omfang i Danmark. Ofte anvendes alene de oplysninger, der fremgår af kortet til at gennemføre betalingen.

Med de nye regler skal der fra den 14. september som udgangspunkt anvendes stærk kundeautentifikation, når en betaler foretager en elektronisk betaling. Det indebærer, at en online kortbetaling skal godkendes med et ekstra element, eksempelvis ved indtastning af en engangskode modtaget via sms.

Undtagelser fra kravet om stærk kundeautentifikation

Reglerne om stærk kundeautentifikation gælder ifølge lov om betalinger for alle betalinger, der ikke er eksplicit undtaget herfra. Mulighederne for undtagelse fra kravet om stærk kundeautentifikation fremgår af den delegerede forordning fra Europa-Kommissionen.

I fysisk handel omfatter undtagelserne fra kravet primært betalinger på op til 375 kr. med kontaktløse kort og betalinger i ubemandede terminaler til offentlig transport og parkering, såsom rejsekort og BroBizz.

I ikke-fysisk handel omfatter undtagelserne fra kravet bl.a. små betalinger på op til 225 kr. og betalinger til personer eller virksomheder, som betaleren selv har opført på en liste over betroede modtagere. Det er derudover ifølge reglerne muligt at undlade at anvende stærk kundeautentifikation ved tilbagevendende betalinger på samme beløb til den samme modtager, hvis bare den første betaling i rækken er godkendt med stærk kundeautentifikation.

Hvad kommer det til at betyde?

For forretninger og andre erhvervsdrivende

De nye regler vil først og fremmest påvirke forretninger og andre erhvervsdrivende, der modtager betaling fra forbrugere i online handel. Forretninger, der alene modtager betaling i fysisk handel, vil som udgangspunkt ikke blive påvirket, da der som nævnt allerede i dag anvendes stærk kundeautentifikation ved fysisk handel.

Før en betaling kan foregå med stærk kundeautentifikation, er det nødvendigt, at alle led i kæden i forbindelse med gennemførelse af en betalingstransaktion

¹ Kommissionens delegerede forordning om reguleringsmæssige tekniske standarder for stærk kundeautentifikation og fælles og sikre åbne standarder for kommunikation ([link](#)).

understøtter dette teknisk. Det omfatter både kortudstedere og kortindløserne samt internetforretninger og de såkaldte betalingsgateways, der leverer tekniske løsninger til internetforretningerne. Alle disse led i kæden skal sikre, at de har løsninger klar, der teknisk understøtter brugen af stærk kundeautentifikation.

Kortindløserne og kortudstedere i Danmark, fx Nets og bankerne, tilbyder i vidt omfang allerede løsninger til stærk kundeautentifikation. Derimod er der mange internetforretninger, der ikke nødvendigvis er teknisk klar til at anvende stærk kundeautentifikation fra den 14. september 2019.

Konsekvensen for internetforretninger, der ikke er klar, kan være vidtrækkende. Disse forretninger vil i vidt omfang være afskåret fra at modtage betaling. Det skyldes, at betalinger, der ikke er godkendt med stærk kundeautentifikation, som udgangspunkt ikke må gennemføres fra den 14. september 2019.

Internetforretninger, som ikke vil risikere at få afvist deres kunders betaling, skal altså sikre, at de teknisk er klar til at modtage betalinger, der er godkendt med stærk kundeautentifikation.

Er man som forretning i tvivl om, hvorvidt man kan modtage betalinger med stærk kundeautentifikation, bør man tage kontakt til sin kortindløser eller gateway-udbyder, som vil kunne hjælpe. Hvilke undtagelsesmuligheder der i praksis kan anvendes, vil ligeledes afhænge af, hvad en kortindløser eller gateway-udbyder kan tilbyde.

For forbrugere

I fysisk handel vil danske forbrugere ikke opleve nogen ændring med de nye regler. I online handel vil

danske forbrugere fra den 14. september 2019 opleve, at de i højere grad end tidligere vil blive bedt om eksempelvis at indtaste en sms-engangskode som et ekstra sikkerhedselement.

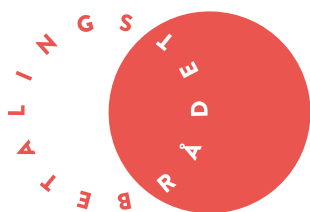
Første gang man handler online fra den 14. september, kan man blive bedt om at oplyse sit telefonnummer. Telefonnummeret skal oplyses, for at der kan fremsendes en sms-kode, hvis man ikke tidligere har oplyst sit telefonnummer til sit pengeinstitut.

Ansvar ved manglende brug af stærk kundeautentifikation

Hvis undtagelserne i de nye regler anvendes, er det vigtigt at være opmærksom på, hvem der pålægges ansvaret for eventuelt misbrug.

I de tilfælde, hvor kortudsteder, kortindløser eller forretning vælger at tilbyde betalinger uden brug af stærk kundeautentifikation, vil den virksomhed, som træffer det valg, som udgangspunkt hæfte for alle tab i forbindelse med et eventuelt misbrug. Det gælder, med mindre andet er aftalt mellem forretning, kortindløser og kortudsteder. I praksis vil det ofte være sådan, at det er forretningen, som skal træffe denne beslutning. Dermed vil det typisk være forretningen, som kommer til at hæfte.

De nye regler medfører derudover, at en forbruger som udgangspunkt ikke hæfter for tab ved svigagtige betalinger, hvis der ikke er anvendt stærk kundeautentifikation.



KONTAKT

Ole Mikkelsen
Kommunikations-
og presserådgiver

omi@nationalbanken.dk
+45 3363 6027

SEKRETARIAT
OG KOMMUNIKATION