



Clearhaus

PSD2 forklaret

Regler og muligheder for
webshops



Indholdsfortegnelse

1. Baggrund

1.1 Introduktion	3
1.2 Hvad er PSD2?	4
1.3 Hvorfor PSD2?	4
1.4 Fra PSD1 til PSD2	5
1.5 Tidslinje for PSD	7

2. Fokusområder for webshops

2.1 Surcharging af Betalinger

2.1.1 Sådan overholder du de nye regler om surcharging	10
2.1.2 Opsummering af surcharging-regler og undtagelser	11

2.2 Strong Customer Authentication (SCA)

2.2.1 Hvad er SCA?	12
2.2.2 Sådan overholder du de nye SCA-regler	12
2.2.3 Undtagelser fra SCA	15
2.2.4 En opsummering af regler og undtagelser for SCA	17

3. Nye Forretningsmuligheder

3.1 Payment Initiation Service Providers (PISP'er)	18
3.2 Account Information Service Providers (AISP'er)	20
3.3 Hvordan udnytter man de nye muligheder?	22

4. Resumé

5. Ordforklaring

Disclaimer

Den Europæiske Unions (EU's) lovgivning, som diskuteres i dette dokument, det Reviderede Betalingstjenestedirektiv (PSD2), har et bredt omfang og vil få konsekvenser for organisationer på forskellig vis. Egne jurister bør rådgive på området, da det vedrører din virksomhed. Dette er alene et informativt dokument og bør derfor ikke anses som juridisk rådgivning.

1. Baggrund

1.1 Introduktion

Uanset om vi taler GDPR eller PSD2, gør EU alt hvad de kan for at øge sikkerheden for de europæiske forbrugere² - og med god grund. Scenen for online betalinger har ændret sig meget i løbet af det seneste årti; med denne udvikling er det første betalingsdirektiv, PSD1, blevet forældet, og der har været et stort behov for en opdatering.

Hvis du er i detailbranchen, er du helt sikkert stødt på begrebet, der ofte florerer i medierne og på de sociale medier. PSD2 har et bredere omfang og går mere i dybden end PSD1 gjorde. Det vil påvirke alle, som er involveret i behandlingen af en europæisk betalingstransaktion, inklusive forbrugere, betalingstjenesteudbydere (PSP'er)², finansielle institutter² og butiksejere.

Selvom store banker og aktører inden for finansielle tjenester vil bære den største byrde af det nye direktiv, bliver webshopejere² også nødt til at reevaluere deres forretningsprocesser for at sikre, at de overholder PSD2.

Nogle dele af PSD2 er allerede indført, mens andre stadig ikke er kommet i spil. Nogle emner er helt åbne, mens andre fortsat er åbne for fortolkning. Der er utallige aspekter i PSD2, hvilket er årsagen til, at vi har udarbejdet denne e-bog. Formålet er at simplificere den tunge litteratur i et format, som er letfordøjeligt for webshops, store som små. Hensigten er at "afkode" PSD2, ved at forklare de emner, som er mest relevante for webshopejere.

Vi har flere års erfaring som betalingstjenesteudbydere og har derfor en dyb forståelse for betalingsprocesser, best practices og lovgivning. Da vi specialiserer os inden for e-handel, er e-bogens omfang begrænset til online betalinger og går derfor ikke i dybden med offline transaktioner.

Vi håber du kan finde både hjælp og information i bogen. God læselyst!



1.2 Hvad er PSD2?

Det Reviderede Betalingstjenestedirektiv (PSD2) er en efterfølger til PSD1 – som blev indført i 2007 – og er et fundamentalt skridt på vejen til at implementere Single Euro Payments Area (SEPA).

PSD2 blev foreslået i 2013, blev godkendt i 2015 og indført den 13. januar 2018. Direktivet indeholder 117 artikler, som er opdelt i 12 emner – disse kaldes mandater.

PSD1 havde til formål at oprette et enkelt marked for betalinger inden for den Europæiske Union. Omfanget af PSD2 er ikke blot bredere, men også dybere end dets forgængers. Det sigter mod at integrere det europæiske marked samt øge gennemsigtigheden, bes-

kytte forbrugere og fremme handel på tværs af landegrænser.

Da der er tale om et EU-direktiv, er de regler og love, som fremsættes i PSD2, minimumskrav. Hvert enkelt medlemsland er ansvarlig for at implementere disse regler i den nationale lovgivning. Resultatet er, at medlemslandene kan håndhæve reglerne på forskellige måder. Dog vil alle EU-borgere i sidste ende være underlagt de samme regler.

1.3 Hvorfor PSD2?

1

For at fjerne tvetydighed og smuthuller

Efter PSD1 trådte i kraft tilbage i 2007, er det blevet klart for Kommissionen, at nogle elementer fra det første direktiv var for tvetydige eller sidenhen er blevet forældede. Derudover har man opdaget flere smuthuller i det første PSD. For at sikre forbrugerbeskyttelse, reduceret risiko samt klare legale retningslinjer, vender man tilbage til disse elementer i PSD2.

For at beskytte forbrugere

2

PSD2 beskytter forbrugerne ved at sikre, at de får den nødvendige information om deres betalinger. Det gør også Strong Customer Authentication (SCA) lovpligtigt og fremsætter regler for overførsel og lagring af sensitiv data.

3

For at fremme konkurrence

Direktivet forsøger at sikre lige vilkår for udbydere af betalingstjenester. Dette vil øge gennemsigtigheden på det finansielle marked og på den måde øge konkurrence og effektivitet. Harmoniseret lovgivning er afgørende for at øge handlen mellem EU-lande og optimere markedspotentialer.

For at regulere nye betalingsmetoder

4

Meget har ændret sig siden PSD1. Verden er blevet introduceret til et utal af nye betalingsmetoder takket være de teknologiske fremskridt inden for elektronik, internet og mobilbetalinger – de fleste af disse var ikke reguleret under PSD1. Ved centralt at lovgive om disse nye betalingsmetoder vil

man opnå yderligere integration af det indre marked samt give nye innovationer hurtigere og lettere adgang til europæiske markeder.

5

For at regulere nye typer PSP'er

Digitaliseringen af betalinger har været katalysator for tilblivelsen af nye typer af betalingstjenesteudbydere (PSP'er). Her er der tale om Payment Initiation Service Providers (PISP'er)⁷ og Account Information Service Providers (AISP'er)⁷. Ingen af de to typer PSP er omfattet af PSD1, hvilket har gjort det til en udfordring at regulere dem. PSD2 opridser regler for de nye spillere på markedet for at beskytte forbrugere og fastsætte lige vilkår.

1.4 Fra PSD1 til PSD2

PSD2 overgår sin forgænger, PSD1, på 3 særlige områder:

Et bredere omfang

Nye services, nye spillere og transaktioner med lande uden for EU (one-leg-out⁸) er omfattet heraf.

Åben kommunikation

Fælles standarder for kommunikation for at sikre flowet af relevant information mellem udbydere af betalingstjenester (PSP'er), forbrugere og webshopejere.

Øget sikkerhed

Strong Customer Authentication, sikker overførsel af sensitiv data og central registrering af PSP'er for at øge gennemsigtigheden.

PSD1

PSD2

Godt at vide: One-leg-out (OLO) transaktioner

Omfanget af PSD2 er, i sammenligning med PSD1, blevet udvidet til at inkludere såkaldte one-leg-out-transaktioner. Det betyder, at følgende to typer transaktioner er omfattet af direktivet:

- Transaktioner i en valuta, som ikke er en af medlemsstaternes valuta, så længe både betalers¹ (kundens) PSP¹ og modtagers² (webshops) PSP² er inden for EU. Kun de dele af betalingstransaktionen, der foregår inden for unionen er omfattet.
- Transaktioner hvor enten betalers PSP eller modtagers PSP er inden for EU, mens den anden ikke er. Kun de dele af betalingstransaktionen, der foregår inden for unionen skal leve op til PSD2's krav.

Hvad skal man gøre som webshopejer?

One-leg-out-reglerne er mest relevante for PSP'erne. De gælder dog også for dig som webshopejer i et enkelt tilfælde. Forbuddet mod surcharging² af forbrugerkort gælder kun, når din kunde bruger en EU-baseret PSP. Det betyder, at du fortsat kan surcharge forbrugerkort, hvis kundens PSP er lokaliseret uden for EU – mere om det senere.

Da PSD2 trådte i kraft, blev PSD1 ophævet. Siden januar 2018 er 6 af de 12 mandater trådt i kraft.

Disse mandater er:

1. Regulatoriske Tekniske Standarder¹ for samarbejde og informationsudveksling i passporting²: Dette omhandler regler om rapportering og informationsudveksling mellem virksomheder, som har drift i mere end et EU-land, og myndighederne i de lande, hvori de har drift.

2. Retningslinjer for autorisation¹ og registrering: Klare regler for hvordan PSP'er (inklusiv PISP'er og AISP'er) skal autoriseres og registreres som udbydere af betalingstjenester.

3. Retningslinjer for minimumskrav til professionel erstatningsforsikring²: Dette omhandler reglerne om mindstekrav til den erstatningsforsikring, PSP'er (inklusiv PISP'er og AISP'er) skal have for at kunne reducere kundernes risiko for tab.

4. Retningslinjer for rapportering af hændelser: Fælles standarder for hvordan og hvornår PSP'er skal aflægge rapporter om hændelser samt regler, som kræver, at offentlige myndigheder deler information om hændelser med hinanden.

5. Retningslinjer for klager over mistænksomme overtrædelser: Klare standarder for hvordan PSP'er skal indgive klager til nationale tilsynsmyndigheder, samt hvordan disse myndigheder skal behandle klager og informere PSP'er om procedurerne.

6. Retningslinjer for sikkerhedstiltag for drifts- og sikkerhedsrisiko: Fælles regler for styring, sporing, risikovurdering, beskyttelse, driftskontinuitet, test af sikkerhedstiltag og kundepleje for at sikre lige vilkår.

Derudover er forbuddet mod surcharging af forbrugerkort² også trådt i kraft i januar 2018.

Mens vi overgår til PSD2, vil de eksisterende regler og nationale love fra PSD1 fortsat være gældende, men Den Europæiske Banktilsynsmyndighed

1. For eksempel kundens bank

2. For eksempel betalingsgateway eller indløser

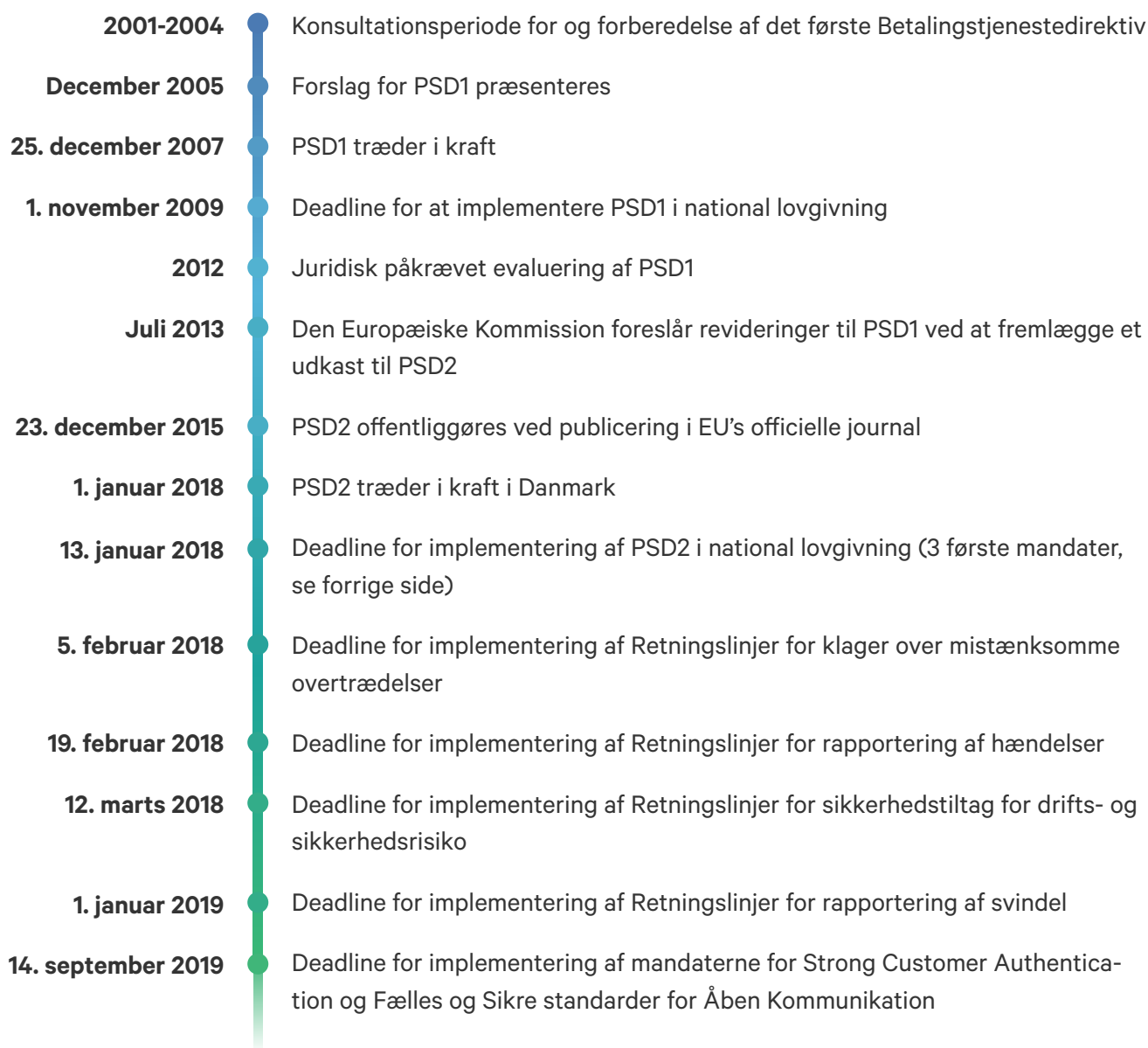
dighed (EBA) anbefaler på det kraftigste, at alle de parter, som påvirkes af PSD2, begynder at overholde reglerne i det nye direktiv så hurtigt som muligt.

europæiske betalingsmarked betydeligt. Det skyldes både reglerne for nye spillere på markedet samt nye regler for alle betalingstjenesteudbydere.

Implementeringen af PSD2 forventes at ændre det

1.5 Tidslinje for PSD

Betalingstjenestedirektivet har en lang historie. Her kan du danne dig et hurtigt overblik over hvordan direktivet har udviklet sig med tiden samt hvilke deadlines, der er blevet sat.



Hvornår de resterende 3 mandater senest skal implementeres, vides ikke endnu. Disse 3 mandater er:

- Regulatoriske Tekniske Standarder for Samarbejde mellem Hjem- og Værtsland
- Regulatoriske Tekniske Standarder for Den Europæiske Banktilsynsmyndigheds register
- Regulatoriske Tekniske Standarder for Centrale Kontaktområder

2. Fokusområder for webshops

Mens håndhævelse af PSD2 vil betyde øget beskyttelse af forbrugere, giver det også webshopejere mulighed for at reflektere over deres gældende forretningsgange og sikre deres webshops. Dette kapitel går i dybden med de dele af PSD2, som i højest grad har indvirkning på webshops – det vil forklare regler og undtagelser samt fortælle, hvordan du kan overholde

de nye love.

Omfanget af PSD2 er enormt, og det regulerer en lang række betalingsaktiviteter. For webshops er det dog kun to hovedområder, som vil blive aktuelle:

1. Surcharging af Betalinger
2. Strong Customer Authentication (SCA)

2.1 Surcharging af Betalinger

Du er højst sandsynligt bekendt med begrebet ”surcharging”. Det har været normen for webshops i efterhånden mange år. For en god ordens skyld har vi dog alligevel valgt at inddrage en ordentlig definition (som beskrevet af Wikipedia):

En surcharge, også kendt som betalingsgebyr eller kortgebyr, er et ekstra gebyr, som webshopejere pålægger betalinger med check, kreditkort, kontokort eller debetkort (men ikke kontanter). Gebyret dækker som minimum de omkostninger, som webshopejeren har ved at acceptere denne type betalinger, f.eks. det gebyr, som skal betales til kreditkortvirksomheden.

PSD2 opridser regler for, hvilke typer betalingskort man må og ikke må surcharge i en kortbaseret betalingstransaktion.

Pr. 13. januar 2018 (1. januar 2018 i Danmark) er det ikke længere tilladt at surcharge kunder, som betaler med forbrugerkort i B2C-transaktioner. Reglerne gælder ikke for firmakort², hvilket betyder, at B2B-transaktioner stadig kan surcharges.

Kort sagt kan webshopejere ikke længere lade gebyret for at kunne acceptere betalinger med debet/kreditkort gå videre til kunderne. Der er dog nogle scenarier, som er undtagelser fra reglen (mere om det senere).

Den nye lov om surcharging af B2C-transaktioner gælder udelukkende for betalinger hvor både kundens kortudstedende bank² og webshopejerens betalingstjenesteudbyder/indløser² er beliggende inden for EU/EØS.

Med andre ord kan man surcharge et forbrugerkort, hvis kundens betalingstjenesteudbyder (for eksempel kundens kortudstedende bank) er beliggende uden for EU.

Tabel 1: Typer af transaktioner som kan og ikke kan surcharges

Transaktioner, som ikke kan surcharges:	Transaktioner, som kan surcharges:
Betalingstransaktioner, som foretages med forbrugerkort – både debit og kredit (når begge PSP'er er inden for EU)	Betalingstransaktioner, som foretages med firma-kort
Betalingstransaktioner, som foretages med betalingsservice ² eller kreditoverførsel ² (kaldes SEPA-betalinger ²)	Betalingstransaktioner, hvor kun en af betalings-serviceudbyderne er beliggende inden for Europa. Med andre ord hvis: • Kundens kortudstedende bank ikke er beliggende inden for EU/EØS, men webshoppens indløser er. • Den kortudstedende bank er beliggende inden for EU/EØS, men webshoppens indløser ikke er.

På transaktioner, som gerne må surcharges, må surcharge-gebyret ikke overstige de direkte omkostninger, som webshopejeren pålægges for at kunne acceptere den givne betalingsmetode.

Hvis webshopejeren eksempelvis bruger en betalings-

serviceudbyder – f.eks. en indløser – som tager 2% for hver transaktion, som behandles, må webshopejeren ikke tage (surcharge) mere end 2 kr. i gebyr for et køb på 100 kr.

2.1.1 Sådan overholder du de nye regler om surcharging

Det er vores erfaring, at webshopejere håndterer de nye regler om surcharging på forskellige måder:

1

Hæve prisen på produkter/services

Vi har set, at nogle virksomheder vælger at inkludere kortgebyret i priserne på de produkter/services, de sælger.

Betale gebyrerne selv

2

Vi har også set, at nogle virksomheder vælger slet ikke at lade kunderne betale kortgebyrerne. I stedet accepterer de dem som en del af virksomhedens administrative omkostninger.

3

Kun acceptere firmakort

Nogle B2B-webshops, hvis kunder hovedsageligt er andre virksomheder, vælger kun at acceptere firmakort. Det gør de ved tydeligt at forklare deres kunder, at alle kort vil blive pålagt et kortgebyr, dvs. surcharged.

Konsekvenserne af ikke at overholde reglerne

Hvert enkelt medlemslands myndigheder bestemmer selv, hvordan de vælger at håndhæve de nye regler om surcharging. Det betyder, at regler kan håndhæves forskelligt i de forskellige medlemslande. For at give et eksempel på hvordan reglerne kan håndhæves, gennemgår vi her proceduren for en overtrædelse af surcharging-reglerne i Danmark:

Hvis forbrugere oplever surcharging i en webshop, kan de anmelde overtrædelsen til **Konkurrence- og For-**

brugerstyrelsen. Den første klage udløser et påbud[?] fra Konkurrence- og Forbrugerstyrelsen. Dette anses som en advarsel. Hvis webshoppen bliver ved med at surcharge forbrugerkort, betalingsservice og kreditoverførsler kan Konkurrence- og Forbrugerstyrelsen udstede daglige eller ugentlige tvangsbøder. Hvis webshoppen fortsat overtræder reglerne om surcharging, bliver sagen overgivet til politiet, som kan udstede egentlige bøder.

2.1.2 Opsummering af surcharging-regler og undtagelser

Der kan opstå en række forskellige scenarier, når vi taler surcharging. Her er en tabel, som opsummerer dem alle:

Tabel 2: En opsummering af surcharging-reglerne

	Type af Betalingstransaktion	Er der tale om en one- leg-out-transaktion? ³	Er surcharging tilladt?
Scenarie 1	Forbrugerkort	JA	JA
Scenarie 2	Forbrugerkort	NEJ	NEJ
Scenarie 3	Firmakort	JA/NEJ	JA
Scenarie 4	SEPA-betaling (betalingsservice)	NEJ	NEJ
Scenarie 5	SEPA-betaling (kreditoverførsel)	NEJ	NEJ

Denne tabel viser de vigtigste scenarier. Andre scenarier er udeladt, da de ikke mulige.

3. Når enten kundens kortudstedende bank eller webshoppens betalingstjenesteudbyder er beliggende uden for EU/EØS.

2.2 Strong Customer Authentication (SCA)

Dette er det andet område, som er vigtigt for webshops. PSD2 kræver en proces, som kaldes "Strong Customer Authentication" (SCA) eller sikkerhed autentificering af kunder, på transaktioner over 30€.

I forbindelse med online betalinger er "autentificering" en verificering af, at den kunde, som skal til at gennemføre en betaling i en webshop, er den retmæssige ejer

af det kort, som bruges i transaktionen. Autentificering foregår ofte i forbindelse med check-out og anses som et supplement til **autorisering**.

2.2.1 Hvad er SCA?

Traditionel autentificering gennemføres normalt ved brug af et enkelt sikkerhedselement, som eksempelvis et statisk password eller en kode (f.eks. CVV). SCA er en mere avanceret form for autentificering.

I processen bedes kunden om at oplyse to eller flere af de følgende typer sikkerhedselementer (2-faktora-autentificering eller multifaktora-autentificering²) for at gennemføre en betalingstransaktion:

1. Noget "kendt" – noget kun kunden "ved". For eksempel et statisk password, en PIN osv.
2. Noget "ejet" – noget kun kunden "har". For eksempel et engangs-password (OTP/one-time password), som sendes til kundens registrerede mobilnummer eller e-mail. Et andet eksempel er en QR-kode, som vises på skærmen, og som kunden

skal scanne med den enhed, som han har registreret. Her bruges værktøjer som f.eks. Google Authenticator App.

3. Noget "nedarvet" – noget kun kunden "er". For eksempel en biometrisk egenskab såsom fingeraftryk, som linkes til kundens enhed.

Ved at oplyse den korrekte information i sikkerhedstrinene, bliver kunden autentificeret og betalingen godkendt. Hvis kunden ikke passerer autentificeringen, bliver betalingen afvist.

2.2.2 Sådan overholder du de nye SCA-regler

Hvornår er deadline for implementering af SCA?

Selvom PSD2 allerede blev implementeret i national lov i EU/EØS-landene pr. 13. januar 2018, er reglerne om Strong Customer Authentication endnu ikke trådt i kraft, da der er en omstillingsperiode på 18 måneder. Det betyder, at webshops har mulighed for at fravælge

2-faktora-autentificering/multifaktora-autentificering indtil d. 14. september 2019. Formålet med denne omstillingsperiode er, at betalingstjenesteudbydere kan tilpasse sig de nye regler og de ændringer, som Strong Customer Authentication medfører.

Hvornår er SCA påkrævet?

SCA er påkrævet for transaktioner, hvor en af de følgende betingelser gør sig gældende:

- Kundens kortudstedende bank og webshoppens indløser er begge beliggende i EU/EØS.
- Kundens kortudstedende bank er ikke beliggende i EU/EØS, men webshoppens indløser er.

I det tilfælde, hvor kundens kortudstedende bank er beliggende i EU/EØS, men webshoppens indløser ikke er, er SCA, ifølge PSD2, ikke påkrævet for indløseren.

Dette er normalt tilfældet, når kunder fra EU/EØS køber noget fra en webshop uden for EU/EØS.

Desuden fremgår det klart af direktivet, at SCA er påkrævet for transaktioner, som er igangsat af betaler (kunden). Pr. definition er kreditoverførsler igangsat af betaler. Kortbetalinger online, i apps og ved POS betragtes også som igangsat af kunden, da kunden sætter betalingen i gang, mens webshoppens blot faciliterer den.

Hvordan overholder man SCA?

Som webshopejer kan man drage fordel fra SCA, idet risikoen for svigagtige transaktioner i webshoppens reduceres betydeligt. Uden SCA vil det i nogle tilfælde være tilstrækkeligt med kortoplysninger for at kunne foretage en betaling i en anden persons navn uden at have fået tilladelse hertil. Ved at kræve to eller flere sikkerhedselementer reduceres mængden af indsigelser, som skyldes svindel.

Den bedste måde at overholde reglerne om Strong Customer Authentication på er i) ved at implementere 3-D Secure i sin webshop, og/eller ii) ved at acceptere betalinger med sikre betalingsmetoder, som f.eks. Apple Pay.

Lad os tage et kig på disse muligheder:

3-D Secure er en sikkerhedsfeature, som anvender SCA i et pop-up-vindue eller en inline-frame. Når kunden shopper online, vil et pop-up-vindue eller en inline-frame dukke op, når check-out nås. Her vil kunden blive bedt om at oplyse information om to eller flere af de sikkerhedselementer, som er nævnt tidligere (noget man ved, noget man har eller noget man er). Hvis denne information er korrekt, er kunden autentificeret, og betalinger er godkendt, hvis ikke afvises betalin-

gen. 3-D Secure udbydes af Visa – som en del af deres ”Visa Secure” – og af Mastercard – som en del af deres ”Mastercard SecureCode”. Nogle indløserne, såsom Clearhaus, tilbyder en nem integration, så 3-D Secure hurtigt kan sættes op i din webshop.

Figur 1: Screenshot af 3-D Secures verificeringsproces

3-D Secure Verification

Merchant: merchant.com
Amount: \$42.00
Date: 31/10/2017
Card Number: **** * 6918
Message: Cardholder since 07/2017

SMS Code: Didn't receive the code?

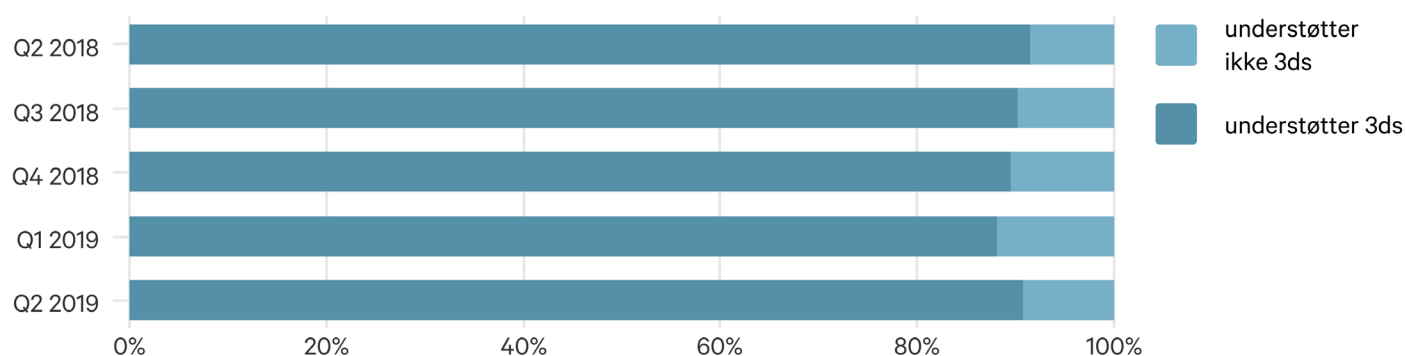
Enter SMS code Next

En af fordelene ved at bruge 3-D Secure er ansvarsskiftet². Hvis der anvendes 3-D Secure på en transaktion, og kunden har succes med at blive autentificeret, er det kundens kortudstedende bank og ikke webshoppen, som er ansvarlig, hvis transaktionen viser sig at være svigagtig. Dette kaldes ”ansvarsskiftet”. Ansvarsskiftet finder sted så længe webshoppen, i samarbejde med sin indløser, anmoder om at anvende 3-D

Secure på transaktionen – uanset om den kortudstedende bank understøtter 3-D Secure eller ej.

I dag understøttes 3-D Secure af hele 90% af de kortudstedende banker inden for EU/EØS. Et stigende antal banker understøtter sikkerhedsfunktionen og kombineret med de nye PSD2-regler, forventes andelen at stige i de kommende år.

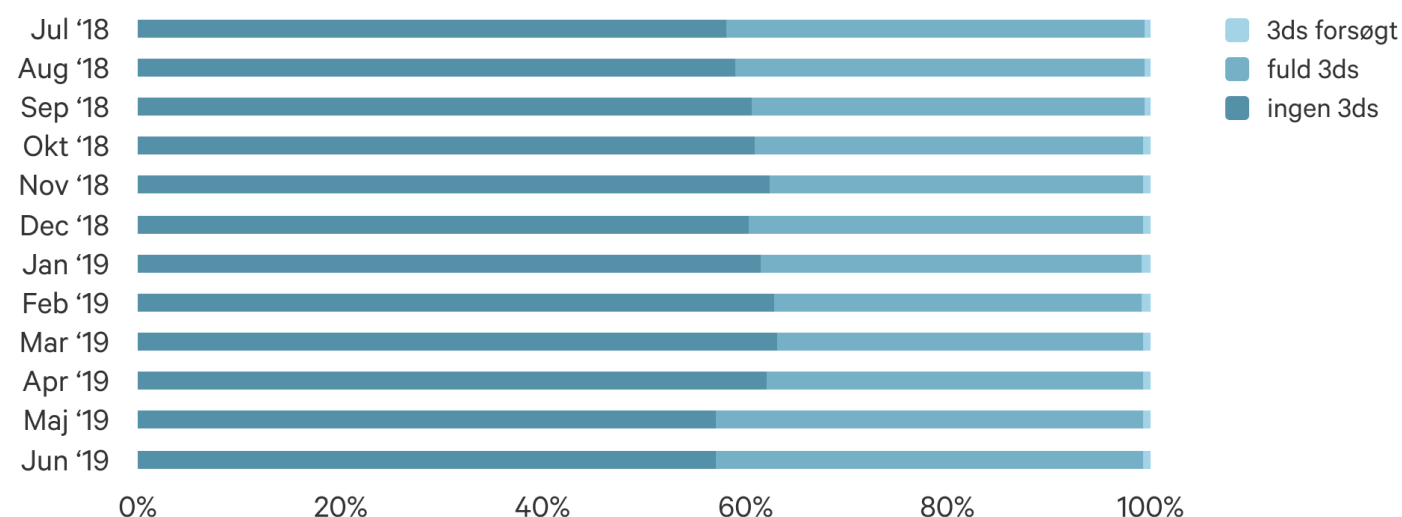
Figur 2: Kortudstedende Banker i EU/EØS, som Understøtter 3-D Secure (Observeret)



På trods af fordelene ved 3-D Secure har europæiske webshopejere endnu ikke taget sikkerhedsfeatures til sig. Vi ser dog en stigning i brugen. Clearhaus har

over 9.000 webshops i sin kundeportefølje, og vores data viser, at der er 3-D Secure på omkring 40% af alle EU-transaktioner.

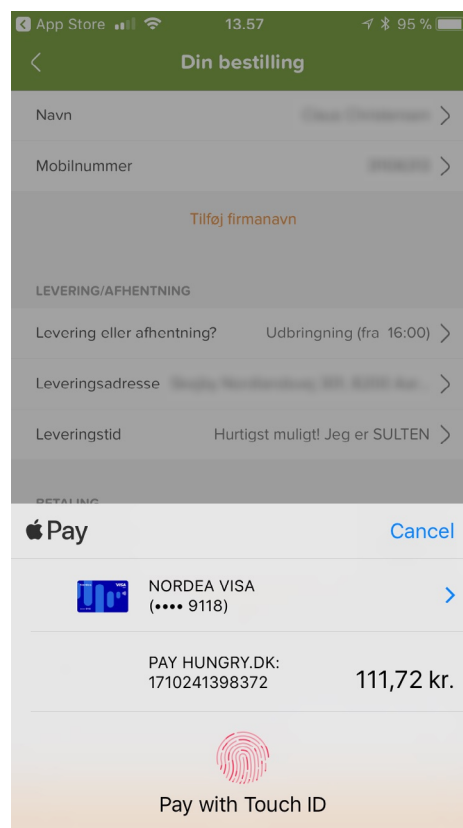
Figur 3: Brug af 3-D Secure i EU/EØS i Løbet af de Seneste 12 måneder (Antal)



Clearhaus giver webshops mulighed for at implementere betinget 3-D Secure på sine betalinger. Det betyder, at webshopejere på baggrund af specifikke kriterier, kan vælge hvilke transaktioner, der skal have 3-D Secure på.

Apple Pay er en sikker mobilbetalings- og digital wallet service, som er udviklet af Apple Inc. Apple Pay anvender et token-system til at garantere sikre betalinger. Når en bruger tilføjer sit kredit- eller debetkort, oprettes en virtuel token. Denne token krypteres og gemmes på brugerens mobile enhed - ikke i skyen eller på Apples servere. Man kan kun få adgang til denne token ved biometrisk identificering, hvilket betyder at kortinformationen er sikret mod svindlere. Det betyder også, at Apple Pay overholder PSD2's krav om SCA.

Apple-produkter som iPhone, iPad og Apple Watch er alle populære hos de europæiske forbrugere – det har Apples produkter altid været - men Apple Pays succes afhænger af, hvor gode banker, betalingsgateways² og indlødere er til at inddrage betalingsmetoden i deres sortiment. Indtil videre ser udsigterne gode ud, da 100+ banker understøtter betalinger med Apple Pay.



Clearhaus giver webshops mulighed for at acceptere betalinger med Apple Pay. Læs mere om det (på engelsk) [her](#).

2.2.3 Undtagelser fra SCA

Ifølge de Regulatoriske Tekniske Standarder (RTS), er Strong Customer Authentication ikke påkrævet for følgende typer af betalinger:

1

Online betalingstransaktioner under 30 Euro

Online betalinger under 30 Euro betragtes som transaktioner af lav værdi og er derfor undtaget fra reglerne om SCA. Dog skal SCA anvendes på hver femte transaktion. Derudover er SCA påkrævet, hvis den samlede værdi af flere transaktioner, som hver især ikke er underlagt SCA, overstiger 100€.

2

Abonnementsbetalinger

For virksomheder, der modtager abonnementsbetalinger eller andre gentagne transaktioner, gælder det, at SCA skal anvendes på den første transaktion, men ikke på de efterfølgende. Dette gælder såfremt abonnementsbetalingerne kvalificeres som lavrisikotransaktioner, hvilket vil sige transaktioner, som vurderes at have en meget lav risiko. I tabellen nedenfor kan du se, hvor grænsen for en lavrisikotransaktion er.

Det skal dog bemærkes, at selvom PSD2 oplyser disse regler, er det endnu ikke helt sikkert, hvordan de vil fungere i praksis. Meget kan ske, inden SCA træder i kraft i september 2019, og vi vil anbefale, at man i de kommende måneder, holder sig opdateret på yderligere afklaring. Vi vil forsøge at holde dig opdateret om de vigtigste udviklingstiltag på vores blog.

3

Lavrisikotransaktioner

Hvis en transaktion betragtes som værende lavrisiko, er SCA ikke påkrævet. Indløseren laver en real-time risikoanalyse for at afgøre, om en transaktion kan kvalificeres som lavrisiko. Hvis det er tilfældet, kan indløseren anmode om en undtagelse, når transaktionen skal behandles. Anmodningen sendes til kundens bank, som også vurderer risikoniveauet og tager den endelige beslutning om, om SCA skal anvendes.

For at kunne anmode om disse undtagelser må hverken bankens eller indløserens svindelniveau overstige følgende grænser:

Tabel 3: Højest tilladte Reference Fraud Rate (%)

Transaktionsværdi	Højest tilladte Reference Fraud Rate (%) for:	
	Kortbaserede betalinger	Kreditoverførsler
EUR 500	0,01	0,05
EUR 250	0,06	0,01
EUR 100	0,13	0,015

Kilde: Oversat fra engelsk fra Den Europæiske Banktilsynsmyndigheds Final Report on Draft Regulatory Technical Standards on SCA and CSC

4

Transaktioner til en selv

Kreditoverførsler mellem konti (hos samme indløser/kortudstedende bank), som ejes af samme enhed/kunde er ikke underlagt reglerne om SCA.

5

Sikre forretningstransaktioner

Overordnet set er SCA påkrævet for transaktioner med firmakort. Dog kan betalinger med firmakort være undtaget, hvis de gennemføres via såkaldte ”dedikerede betalingsprocesser eller -protokoller”, da sikkerheden i disse systemer sikres på andre måder end via autentificering. Denne protokol er noget som aftales mellem webshop og kunde og som godkendes af myndighederne.

6

Betalinger igangsat af merchant

Betalinger, som igangsættes af webshoppens, falder uden for PSD2's lovgivning. Disse kaldes også MIT (merchant initiated transactions). SCA er altså ikke påkrævet for denne type betalinger. Det er typisk abonnementsbetalinger (med undtagelse af første betaling), som igangsættes af webshoppens. I de fleste tilfælde vil abonnementsbetalinger nemlig blive automatiseret ved at gemme kundens kortinformation, og på den måde kan webshoppens opkræve betalinger fra kundens kort, uden kunden selv er involveret.

Der er to betingelser for en betaling, som igangsættes af webshoppens. 1) SCA er påkrævet for den første betaling, som kunden foretager. Den første betaling er typisk også igangsat af kunden selv. 2) Der skal være en eksplicit aftale om, at webshoppens regelmæssigt kan trække penge fra kundens kort.

OBS: Disse regler gælder kun for nye abonnements. Eksisterende abonnements vil ikke blive påvirket af reglerne for SCA.

2.2.4 En opsummering af regler og undtagelser for SCA

Tabel 4: En opsummering af hvilke scenarier, der kræver SCA

NÅR BÅDE KORTUDSTEDENDE BANK OG INDLØSER ER I EU ELLER NÅR KORTUDSTEDENDE BANK IKKE ER I EU, MEN INDLØSEREN ER ⁴		
	Type af betalingstransaktion	Er SCA påkrævet?
Scenarie 1	Værdi ≥ 30 Euro	JA
Scenarie 2	Højrisiko	JA
Scenarie 3	Abonnementsbetalinger/gentagne transaktioner	Kun for første transaktion
Scenarie 4	Betalingsservice	NEJ
Scenarie 5	Værdi < 30 Euro	NEJ
Scenarie 6	Lavrisiko	NEJ
Scenarie 7	Til en selv	NEJ
Scenarie 8	B2B-transaktioner, som følger en godkendt protokol	NEJ
Scenarie 9	B2B-transaktioner, som ikke følger en godkendt protokol	JA

4. I transaktioner, hvor kortudstedende bank er i EU, men indløseren ikke er, gælder SCA ikke. Med andre ord er SCA påkrævet for webshops inden for EU)

Den aktuelle status på SCA

I øjeblikket (pr. maj 2018) vides det endnu ikke, hvordan SCA vil blive anvendt i praksis, eller hvordan det vil blive indført på tværs af betalingsindustrien. Hvis der

er ændringer eller opdateringer på området, vil Clearhaus informere sine kunder herom, så de hele tiden er opmærksomme på de vigtigste aspekter.

3. Nye Forretningsmuligheder

I takt med at e-handel har udviklet sig, har betalingsteknologier gjort det samme. Der er sket meget siden PSD1 blev fremlagt, og det har ført til tilblivelsen af nye typer finansielle virksomheder, som håndterer forskellige aspekter af online betalinger.

I løbet af de seneste år, er der dukket to nye, men meget forskellige, typer virksomheder op – Payment Initiation Service Providers (PISP'er) og Account Information Service Providers (AISP'er). Det faktum, at der ikke var en klar lovgivning for disse typer virksomheder, var en af hovedårsagerne til, at EU besluttede sig for at udarbejde PSD2.

Selvom der allerede findes mange af disse betalingst-

jenester, vil den nye lovgivning formentlig booste deres tilstedeværelse. For potentielle iværksættere vil det blive lettere at navigere i markedet, og det vil blive lettere for eksisterende PISP'er og AISP'er at gøre entre på nye EU-markeder.

Men hvad laver disse nye virksomheder og hvordan bliver de påvirket af PSD2?

3.1 Payment Initiation Service Providers (PISP'er)

I PSD2 bliver en Payment Initiation Service² defineret som: "en tjeneste, som igangsætter en betalingsordre efter anmodning fra brugeren af betalingstjenesten², i forbindelse med en betalingskonto hos udbyderen af betalingstjenesten."

Med andre ord sørger en PISP for overførsel af penge mellem en webshop og betalers bankplatform. I stedet for at betale med betalingskort, giver betaler PISP'en tilladelse til at overføre penge fra sin konto til webshoppen – ofte øjeblikkeligt, så varerne kan sendes med det samme. PISP'er kan betragtes som et billigere alternativ til betalingskort.

PSD2 har en række krav til Payment Initiation Service Providers:

- Det er gjort klart, hvornår de er ansvarlige for betalinger, hvilket vil give dem et incitament til at implementere de sikkerhedselementer, der er nødvendige for at beskytte dem selv og deres kunder.
- PISP'er er underlagt reglerne om databeskyttelse og sikkerhedskrav, som er fremsat i direktivet eller specificeret i de Regulatoriske Tekniske Standarder.
- PISP'er er underlagt standarderne for åben kommunikation.
- PISP'er skal leve op til visse sikkerhedskrav på linje med dem, andre finansielle institutter ifølge PSD2 skal overholde.
- PISP'er skal fremsætte klar information om sig selv til betaleren før betalingen igangsættes. Desuden skal de levere information om betalingen, efter at den er gennemført.
- PISP'er må ikke holde på pengene mellem overførsel fra betaler til modtager.
- PISP'er skal informere kundens bank om, at det ikke er en kunde/et individ, som igangsætter betalingen.
- PISP'er skal have professionel erstatningsforsikring.

Eksempler på Payment Initiation Service Providers

Sofort

Hvad er det?

Sofort er en tysk PISP. Det er en online bankservice, som er udbredt i alle tysktalende lande i EU samt i Belgien.

Hvordan virker det?

Når kunden når kassen i en webshop, kan han vælge at bruge Sofort i stedet for andre tilgængelige betalingsmetoder (f.eks. kort eller faktura). Kunden videregives nu til Soforts hjemmeside, hvor han vælger bank og konto (hvis han har mere end en).

Al nødvendig information vil være udfyldt på forhånd, hvilket gør betalingsmetoden nem og hurtig. Betalingen bekræftes på samme måde, som kundens bank normalt autentificere betalinger.

Webshoppen får øjeblikkelig besked om godkendelsen af betalingen, så shoppen kan sende ordren afsted med det samme. Beløbet afstemmes inden for én hverdag.

Amazon Dash Buttons

Hvad er det?

Amazon Dash Buttons er en checkout-metode, som er tilgængelig for Prime-kunder på Amazons hjemmeside.

Hvordan virker det?

Kunden kan oprette dash buttons for de produkter, som han oftest køber. Knappen kan fås i to versioner. Den ene er en virtuel knap, som gemmes på din "mine dash-buttons"-side. Den anden er en fysisk knap, som man kan bestille og klistre fast rundt omkring i hjemmet. For eksempel kan du bestille en knap til vaske-middel og klistre den fast på vaskemaskinen.

Når som helst en kunde ønsker at genbestille en vare,

skal han bare trykke på den tilhørende dash button for at sætte en ordre i gang.



Andre velkendte PISP'er er PayPal og MobilePay.

3.2 Account Information Service Providers (AISP'er)

I PSD2 bliver en Account Information Service² defineret som: "en online service, som giver samlet information over en eller flere betalingskonti, som brugeren af betalingstjenesten har hos enten en anden betalingstjenesteudbyder eller hos flere betalingstjenesteudbydere."

Kort sagt tilbyder Account Information Service Providers en online brugerflade, hvor kunden kan få et overblik over alle sine konti, selvom disse konti er i forskellige banker. Målet er at give kunden et nemt og hurtigt overblik over sin finansielle situation.

PSD2 har en række krav til Account Information Service Providers:

- AISP'er er, med undtagelse af få artikler, underlagt reglerne i PSD2 på linje med andre betalingstjenesteudbydere.
- Det er gjort klart, hvornår AISP'er kan tilgå information fra deres kunders konti.
- AISP'er er underlagt reglerne om databeskyttelse og sikkerhedskrav, som er fremsat i direktivet eller specificeret i de Regulatoriske Tekniske Standarder.
- AISP'er er underlagt standarderne for åben kommunikation.
- Det er gjort klart, hvornår, hvorfor og hvordan kunders finansielle data kan lagres og overføres af AISP'en.
- Når de interagerer med andre betalingstjenesteudbydere, skal AISP'er altid identificere sig selv, så det er gjort klart, at det er AISP'en og ikke kunden selv, som beder om adgang til informationen.
- AISP'er skal have professionel erstatningsforsikring.
- En AISP, som er registreret i et EU/EØS-land, kan drive forretning i alle andre EU/EØS-lande uden yderligere autorisering (reglerne om passporting).

Eksempler på Account Information Service Providers

Spiir

Hvad er det?

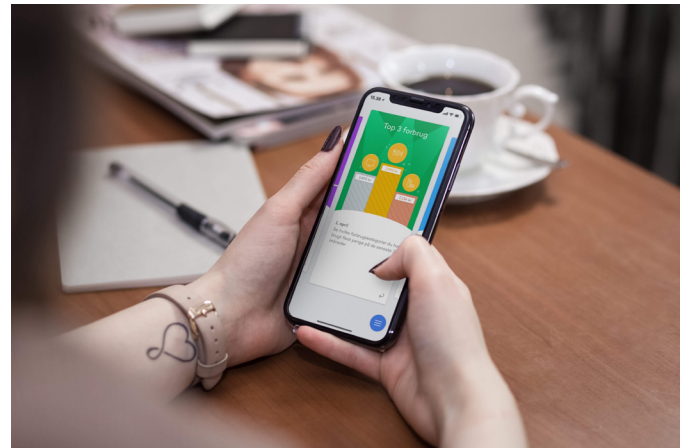
Spiir er en dansk AISP, som hjælper forbrugere med at holde styr på deres konti og udgifter.

Hvordan virker det?

Når du registrerer dig hos Spiir, giver du dem tilladelse til at tilgå data fra dine bankkonti. Du kan tilføje konti fra flere forskellige banker.

I Spiir-appen eller på deres hjemmeside kan du få et overblik over dine konto og dine penge. Dine udgifter bliver opdelt i forskellige kategorier og du kan sætte begrænsninger på, hvor mange penge du vil bruge på hver kategori. Du kan også lægge et månedligt budget, så hjælper appen dig med at overholde det.

Spiir tracker endda dine faste omkostninger, f.eks. telefon- og elregning, og foreslår billigere alternativer – blot for at hjælpe dig med at spare penge.



Moneybox

Hvad er det?

Moneybox er en engelsk finansiel service, som hjælper dig med at opspare og investere dine penge.

Hvordan virker det?

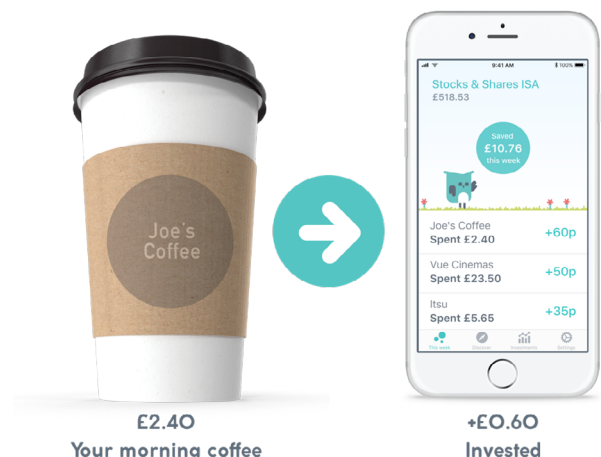
Når du registrerer dig hos Moneybox, tilknytter du dit betalingskort eller bankkonto til din Moneybox-konto. Herefter vælger du, om du ønsker at bruge engangsbetaling, et ugentligt beløb eller afrundinger til at spare penge.

Hvis du vælger afrundinger, vil Moneybox anbefale dig at opspare et vist beløb, hver gang du foretager dig et køb. For eksempel anbefaler de måske at du sparer 5 kr. op, når du køber din morgenkaffe til 15 kr.

De penge, du vælger at spare op, bliver sat ind på din Moneybox-konto hver onsdag. Herefter vil dine penge blive investeret i enten kontanter, globale aktier eller

ejendomsfonde. Hvordan investeringen fordeles mellem de tre, baseres på, om du vælger "forsigtig", "afbalanceret" eller "eventyrlysten" når du opretter din bruger.

Du kan til enhver tid følge din investering, og du kan hæve dine penge når som helst.



3.3 Hvordan udnytter man de nye muligheder?

Formålet med de nye PSD2 regler er at gøre brugen af Payment Initiation Service Providers og Account Information Service Providers mere sikker og gennemsigtig – for både webshopejere og forbrugere. Den Europæiske Banktilsynsmyndighed håber desuden, at lovgivningen vil øge konkurrencen og innovationen på området.

Derudover åbner den nye lovgivning op for nye forretningsmuligheder – både for tredjepartsudbydere² (som Spiir og Sofort) og for banker og webshops. Webshops kan for eksempel øge deres omsætning ved at blive PISP'er – ligesom Amazon med deres dash buttons.

Ved at blive PISP kan webshops få adgang til kundernes bankkonti og selv hæve pengene for betalinger – uden at involvere (og betale for) kortorganisationer eller andre mellemhænd. For at blive PISP skal man have en startkapital på 50.000 €, men der er ingen krav

til driftskapital. Det er dyrt at blive PISP, og der er en lang liste af betingelser, som skal opfyldes, før man kan blive godkendt. Desuden er professionel erstatningsforsikring påkrævet. Når det er sagt, er fordelene for PISP'er, at de kan gøre checkout mere enkel for deres kunder, hvilket vil reducere mængden af kunder, som falder fra ved kassen.

Reguleringen af AISP'er og PISP'er giver bankerne nye muligheder. Ved at fungere som en AISP, kan banken tilføje en ekstra service til deres portefølje. Med en mere dybdegående indsigt i kundernes konti, kan banken i højere grad give finansiell rådgivning – selv til små kunder.

Banker får også mulighed for at oprette et PISP-system. De kan på den måde få en ekstra indtægt, da de kan tage et lille gebyr for servicen.

4. Resumé

Webshops bliver ikke påvirket af PSD2 på samme måde som betalingstjenesteudbydere og andre finansielle institutter gør. Det er dog alligevel vigtigt at man – som webshopejer eller e-handelsekspert – forstår de få, men essentielle, regler, som vil berøre ens virksomhed.

De vigtigste love omhandler forbuddet mod surcharging og kravene for Strong Customer Authentication. Det første problem er ret nemt at løse – du skal simpelthen bare stoppe med at surcharge forbrugerkort. Det har du forhåbentlig allerede gjort. Det andet problem er lidt mere tricky, men det kan løses ved hjælp af teknologi, såsom 3-D Secure, og sikre betalingsmetoder, såsom Apple Pay.

PSD2 kan også være en velsignelse for de, der søger nye udfordringer i fintech-industrien. Takket være de nye regler, som regulerer AISP'er og PISP'er, er det nu mere åbenlyst hvordan man kan starte denne type virksomhed.

Overordnet set vil PSD2 påvirke betalingsindustrien i en positiv retning. Med lige vilkår, åben kommunikation og øget forbrugerbeskyttelse vil forbrugere kunne drage fordel af den øgede sikkerhed – som vil styrke tilliden til online shopping. I sidste ende vil webshopejere opleve stigende forbrugertillid og salg.

5. Ordforklaring

3-D Secure

En sikkerhedsfeature, som anvender SCA i et pop-up-vindue eller en inline-frame. Når kunden shopper online, vil et pop-up-vindue eller en inline-frame dukke op, når vedkommende når kassen. Her vil kunden blive bedt om at oplyse information om mindst to af følgende faktorer: noget man ved, noget man har eller noget man er. Hvis denne information er korrekt, er kunden autentificeret og betalingen er godkendt, hvis ikke afvises betalingen.

Abonnementsbetalinger

Også kaldt gentagne betalinger. Når en forbruger giver en webshop autorisation til jævnligt at hæve et specifikt beløb på deres kredit- eller debetkort. F.eks. månedlige, kvartalsvise eller årlige betalinger for produkter eller services.

Account Information Service

En online service, som giver samlet information om en eller flere betalingskonti, som brugeren af betalingstjenesten har hos enten en anden betalingstjenesteudbyder eller hos flere andre betalingstjenesteudbydere.

Account Information Service Provider (AISP)

Enhver onlineudbyder, som ønsker at samle online-information fra en eller flere betalingskonti hos en eller flere betalingstjenesteudbydere. Informationen bliver typisk vist til kunden i et enkelt dashboard.

Ansvarsskifte

Overgang af ansvar fra webshopejer til kortudstedende bank, når der laves en indsigelse på en svigagtig transaktion, som er blevet autentificeret via 3-D Secure.

Autentificering

Den proces (oftest i forbindelse med checkout), som omfatter at tjekke, at den kunde, som er i gang med at gennemføre en betaling i en webshop, er den retmæssige ejer af det betalingskort, som bruges i transaktionen.

Autorisation

Den proces (i løbet af et køb), hvor kortudstedende bank validerer den kortinformation, som kunden har indtastet og tjekker, at beløbet, som står på den konto, som kortet er tilknyttet, er tilstrækkeligt til at dække købet.

Betaler

En privat eller juridisk person², som ejer en betalingskonto og godkender en betaling fra den betalingskonto, eller, hvor der ikke eksisterer en betalingskonto, en naturlig eller juridisk person, som aflægger en betalingsordre.

Betalingsinstitut

En juridisk person, som er autoriseret til at udbyde og udføre betalingsservices.

Betalingsservicetransaktion

Også kaldt direct debit. En national eller udenlandsk betalingstjeneste, hvor betaler (kunde) giver modtager (webshop) lov til at trække et bestemt beløb fra betalers bankkonto. Husleje betales ofte via betalingsservice. Her giver forbrugeren banken autorisation til at foretage månedlige betalinger til udlejer.

Bemærk venligst at **betalingsservicetransaktioner** ikke er det samme som **abonnementsbetalinger**.

Betalingstjenesteudbyder

Kreditinstitutter, elektroniske pengeinstitutter[?], giroinstitutter som har tilladelse til at udbyde betalingstjenester, betalingsinstitutter[?], Den Europæiske Centralbank (ECB) og nationale centralbanker (når de ikke agerer som offentlige myndigheder), medlemsstater og lokale myndigheder (når de ikke agerer som offentlige myndigheder). Forkortet PSP – Payment Service Providers.

Bruger af betalingstjenester

En naturlig eller juridisk person, som bruger en betalingsservice – enten som betaler, modtager eller begge dele.

Elektronisk pengeinstitut

En juridisk person, som er autoriseret til at udstede elektroniske penge.

Erstatningsforsikring

En aftale i form af en kontrakt, hvori en part forpligter sig til at betale for en anden parts potentielle skader og tab.

Finansielt Institut

Et foretagende, som har til formål at behandle monetære transaktioner, f.eks. indskud, lån, valutaomveksling og investeringer. De mest velkendte finansielle institutioner er banker og indlødere, som i nogle tilfælde kan være den samme enhed.

Firmakort

Betalingskort (f.eks. debet/kredit), som udstedes til en virksomhed og er beregnet til forretningsrelaterede køb. Kortet er tilknyttet virksomhedens bankkonti. Kortet bruges til at købe forretningsrelaterede produkter/services, f.eks. en firmabil, betale en freelancer osv.

Forbruger

En privat person, som handler på vegne af sig selv og med egne, private behov for øje – ikke i forretningssammenhæng.

Forbrugerkort

Betalingskort (f.eks. debet/kredit), udstedt til et individ og til eget privat brug. Kortet er tilknyttet individets egne personlige bankkonti. Kortet bruges til at købe forbrugsvarer/services, f.eks. mad, tøj, fitnessmedlemskab osv.

Gateway

En betalingstjenesteudbyder, som står for betalingsvinduet hos en webshop. I dette vindue indtaster kortholder[?] sin kortinformation. Gatewayen håndterer desuden kortinformation og videresender det i krypteret form til indløseren. Gatewayen tilbyder en løsning, der gør det muligt for webshopejeren at acceptere kortinformation og administrere betalinger i sin webshop.

Indløser

En betalingstjenesteudbyder, som gør det muligt for en webshop (modtager) at acceptere kortbaserede betalinger. Indløseren behandler betalingerne, hvilket resulterer i, at pengene overføres til webshoppen.

Juridisk person

Et menneske eller ikke-menneskelig enhed, f.eks. en virksomhed, institution eller stat.

Kortholder

En person eller enhed, som ejer et betalingskort, der bruges til at foretage køb i en betalingstransaktion.

Kortudstedende bank

Den bank, som udsteder et debit/kreditkort til en kunde. Kundens bankkonto tilknyttes kortet. Under en betalingstransaktion bekræfter den kortudstedende bank betalingskorttransaktionen ved at verificere kortinformationen og beløbet på kortholders konto.

Kreditoverførsel

En national eller udenlandsk betalingstjeneste, hvor betalers (kundes) betalingstjenesteudbyder krediterer modtagers (webshops) betalingskonto med en eller flere betalingstransaktioner fra betalers betalingskonto, ved brug af de instruktioner, som betaler giver.

Lavrisikotransaktion

En betalingstransaktion, som af indløseren og kortudstedende bank vurderes til at være af lav risiko. Denne type transaktion er undtaget fra SCA-kravene.

Modtager

En privat eller juridisk person, som modtager et beløb som del af en betalingstransaktion.

Obligatoriske risikoanalyse

En analyse, som bestemmer, hvorvidt en betalingstransaktion kvalificeres som lavrisiko. Analysen er baseret på bestemte faktorer, inklusiv tidligere forbrugsmønstre for kunder, unormal aktivitet, kunders betalingshistorik og lokationen for kunden og webshoppen på tidspunktet for transaktionen.

One-leg-out

En situation, hvor en af betalingstjenesteudbyderne i transaktionen (enten kundens eller webshoppens) er beliggende uden for EU/EØS.

Passporting

Den rettighed en virksomhed, som er registreret i EØS, har til at drive forretning i andre medlemslande, uden at skulle have yderligere autorisation i hvert enkelt land.

Payment Initiation Service

En service, som igangsætter en betaling på opfordring af brugeren af betalingstjenesten. Betalingen igangsættes af en betalingstjenesteudbyder men i relation til en konto hos en anden betalingsserviceudbyder.

Payment Initiation Service Provider (PISP)

Enhver organisation, som igangsætter en betaling og leverer en bro af software mellem webshop og betalers online bank med det formål at igangsætte internetbetalinger i form af kreditoverførsler.

Påbud

Et forbud, som pålægges en part på baggrund af en retskendelse.

Regulatoriske Tekniske Standarder

En samling af tekniske krav, som skal følges i medlemsstaterne for at kunne drive virksomheden inden for bestemte områder, f.eks. de regulatoriske tekniske standarder for Strong Customer Authentication og fælles og sikre åbne standarder for kommunikation. Forkortes RTS.

SEPA-betalinger

Betalingstransaktioner med betalingsservice eller kreditoverførsler i Euro.

Surcharging

Når en webshop pålægger kunden ekstra gebyr udover køkets totale beløb for brug af en bestemt betalingsmetode.

Svigagtig transaktion

En ulovlig eller falsk transaktion. Inden for e-handel sker den mest almindelige form for svigagtig transaktion, når den gennemføres med et betalingskort, uden kortholder har givet tilladelse hertil.

To-faktor/multifaktor-autentificering

En proces, hvor man anvender to (for to-faktor) eller flere (for multifaktor) sikkerhedselementer for at autentificere en kortholder.

Tredjepartsudbydere (TPSP)

En enhed, som enten er Account Information Service Provider eller Payment Initiation Service Provider.

Webshop

En virksomhed, som sælger produkter eller services online mod penge fra online betalingstransaktioner.