BESTEMMELSER FOR SALG MOD BETALING MED KONTOKORT DISTANCEHANDEL (Card Not Present) (Oktober 2015)

Disse bestemmelser, "Bestemmelser om Distancehandel", gælder for salg mod betaling med Kontokort ved Distancehandel. Med "Distancehandel" forstås Salgsmetoder, hvor Kontokort ikke er til stede på betalingstidspunktet. De "Salgsmetoder" som omfattes af Bestemmelser om Distancehandel, er f.eks. salg via internettet, salg efter postordre og/eller telefonisk ordre, mobilbetalinger, tilbagevendende betalinger med lagret kortnummer (såkaldt "Account on File") og abonnementsbetalinger (såkaldte "Recurring Payments").

Bestemmelserne om Distancehandel udgør et supplement til de Generelle betingelser om indløsning af kontokorttransaktioner, der gælder for den aftale om Indløsning af Kontokorttransaktioner ("Hoveddokumentet"), som er indgået mellem Salgsvirksomheden og Bambora. Ved eventuelle uoverensstemmelser mellem Hoveddokumentet og Bestemmelser om Distancehandel skal Bestemmelser om Distancehandel have forrang. Ord, som indledes med en versal, dvs. stort bogstav, refererer til et ord, som har fået en særligt betydning/definition i Hoveddokumentet og skal i disse Bestemmelser om Distancehandel have samme betydning, som i Hoveddokumentet.

1. Generelt om salg mod betaling med Kontokort ved Distancehandel

Ved salg med Kontokort via internet accepteres samtlige Kontokort iht. Aftalen samt i pågældende tilfælde MasterPass og V.me med undtagelse af Maestro-kort, som kun kan accepteres, hvis 3D Secure er installeret og aktiveret. Ved Telefonisk ordre eller Postordre accepteres dog aldrig Maestro.

2. Særlige forpligtelser ved Distancehandel

Salgsvirksomheden forpligter sig til:

- på bestillingsformularen eller internetsiden klart at informere kortindehaveren om, inden betalingsinstruktionerne, i hvilket land Transaktionen sker, samt i hvilket land Salgsvirksomheden betaler moms,
- på sin hjemmeside ikke at have informationer eller links til hjemmesider med ulovlige og/eller efter Bamboras vurdering uetiske aktiviteter eller til virksomheder, som på et objektivt grundlag må anses for at skade Bamboras anseelse,
- omgående at underrette Bambora, hvis den pågældende hjemmeside, på hvilken Salgsvirksomhedens salg foregår, skifter www-adresse, og/eller der indføres nye www-adresser, som Salgsvirksomheden anvender til sit salg med kontokort.

3. Kontroller

Salgsvirksomheden skal ved debitering af kortindehaveren udføre nedenstående kontroller.

3.1 Autorisation
Autorisation skal altid ske på betalingstidspunktet, uanset købets beløb. Autorisationen skal kodes med korrekt Salgsmetode.

Ved kontrol af status på Kortindehaverens Kontokort (kontrol af kortstatus) skal der altid anvendes en såkaldt "nulværdi-autorisation".

3.2 Identificering af Kortindehaveren

3.2.1 Internet
Korttransaktionen skal være gennemført iht. 3D Secure, hvis der ikke er aftalt anden mellem parterne.

3.2.2 Telefonisk ordre og postordre
Ved Telefonisk ordre og Postordre kan Salgsvirksomheden ikke sikre Kortindehaverens identitet. Salgsvirksomheden bærer derfor altid risikoen for samtlige købstransaktioner ved Telefonisk ordre og Postordre. Dette indebærer, at Bambora har ret til at tilbagedebitere Salgsvirksomheden for beløb, der reklameres af Kortindehavere. Dette gælder uanset om Kortindehaverens indsigelse er berettiget eller ikke.

3.2.3 Postordre
Postordredokumentationen skal kræves i lukket forsendelse til Salgsvirksomheden og indeholde:

- Salgsvirksomhedens navn, by og CVR-nummer,
- kortindehaverens navn,
- kortindehaverens adresse (leveringsadresse),
- kortindehaverens telefonnummer,
- navn på Kortudsteder,
- kontokortnummer,
- kontokortets udløbsdato,
- bestillingsdato,
- bestillingens samlede beløb,
- oplysninger om moms,
- beskrivelse af de bestilte varer, samt
- kortindehaverens underskrift.

3.2.4 Arkivering
Salgsvirksomheden skal i mindst 18 måneder arkivere ordreformular/bestillingsdokumentation iht. Payment Card Industry (PCI) Data Security Standard (DSS). På Bamboras anmodning skal Salgsvirksomheden inden for fem (5) bankdage fremlægge en ordreformular/bestillingsdokumentation vedrørende enkelte Transaktioner.

3.3 Modtagelsesbevis
Ved leverance af fysisk leverbare varer eller billetter, anbefales leverance som postpakke eller brev, hvor det er muligt at få et underskrevet modtagelsesbevis med legitimationskontrol ved udleveringen. Ved leverance af højrisikovarer kræves dog et modtagelsesebevis, se punkt 5.2. Hvis Kortindehaveren reklamerer køb, og der er anvendt modtagelsesbevis, bliver den efterfølgende undersøgelse lettere. Undersøgelsen kan dog påvise, at Bambora alligevel har ret til Tilbagedebitering af den indløste Korttransaktion iht. reglerne i Generelle betingelser.

Salgsvirksomheden bærer hele risikoen for Tilbagedebiteringer af indløste Korttransaktioner iht. reglerne i Generelle betingelser, hvis Kortindehaveren bestrider at

have modtaget varen eller tjenesten uanset, hvordan Kortindehaveren har identificeret sig iht. punkt 3.3.

4. Rapportering

4.1 Indsendelse af købstransaktioner m.m.
Elektronisk indsamlede købstransaktioner skal senest inden for to (2) dage fra betalingsdagen overføres til Bambora. Ved "betalingsdagen" forstås dagen for autorisationen. For miljøer som f.eks. hoteller, hvor en såkaldt præliminær autorisation sker, skal købstransaktionen være Bambora i hænde inden for tredive (30) dage.

4.2 Transaktionsinformationer
Salgsvirksomheden skal ved leverance af varer eller tjenester fremlægge Kortindehaverens Kundekvittering via e-mail eller sammen med varen/tjenesten ved leverance. Kundekvitteringen skal indeholde følgende informationer:

- Ordet "kvittering" i overskriften,
- Salgsvirksomhedens navn. Navnet skal være det samme som det, der er angivet i Aftalen til Bambora og som dermed angives på Kortindehaverens kontoudtog,
- telefonnummer og e-mailadresse til Salgsvirksomhedens kundeservice,
- i det pågældende tilfælde, Salgsvirksomhedens hjemmeside (webadresse),
- trunkeret kontokortnummer,
- korttransaktionens beløb sammen med transaktionsvaluta,
- transaktionsdato og klokkeslæt,
- unikt transaktionsnummer/ordrenummer, som identificerer transaktionen,
- modtaget Kontrolnummer fra Autorisation,
- i det pågældende tilfælde, oplysning om at det betegner en internettransaktion,
- transaktionstype (køb eller returnering),
- beskrivelse af de bestilte varer og tjenester,
- returnerings- og tilbagebetalingsregler,
- øvrige oplysninger iht. den til enhver tid gældende anvendte lov,
- ved telefonisk ordre skal Salgsvirksomheden på Kortindehaverens kvittering skrive "TO" eller "Telephone Order" samt
- ved Postordre skal Salgsvirksomheden skrive "MO" eller "Mailorder".

I de tilfælde, hvor der ikke foreligger en fysisk kvittering på gennemført og rapporteret Korttransaktion, f.eks. ved visse former for Internethandel, skal Salgsvirksomheden oprette og gemme Transaktionslog og på Bamboras anmodning udlevere følgende informationer om;

Korttransaktionen:
- Salgsvirksomhedens navn,
- Salgsvirksomhedens rapporteringsnummer hos Bambora,
- i det pågældende tilfælde Salgsvirksomhedens hjemmeside (webadresse),
- beskrivelse af varer eller tjenester,
- modtagerens navn og leveringsadresse samt i det pågældende tilfælde modtagerens metode for at autorisere sig f.eks. 3D Securekode,
- trunkeret Kontokortnummer,

- korttransaktionens beløb sammen med transaktionsvaluta og moms,
- transaktionsdato og klokkeslæt,
- unikt transaktionsnummer/ordrenummer, som identificerer transaktionen,
- modtaget Kontrolnummer fra Autorisation,
- transaktionstype (køb eller returnering),
- indikator for elektronisk handel,
- bestillerens IP-adresse.

Transaktionsloggen skal opfylde kravene iht. PCI DSS.

Salgsvirksomheden skal på Bamboras anmodning forevise informationer om Korttransaktioner fra systemer, der håndterer 3D Secure. Hvis det pågældende system håndteres af Payment Service Provider (PSP), skal Salgsvirksomheden sikre, at PSP kan forevise disse informationer på Salgsvirksomhedens anmodning. Dette gælder også ved anmodning om informationer om Korttransaktioner i Transaktionslog.

5. Øvrigt

5.1 Salgssted
Salgsstedets salgsplads på internettet skal som minimum indeholde følgende informationer:

- Salgsvirksomhedens navn. Navnet skal være det samme som det, der er angivet til Bambora i Aftalen og som dermed angives på Kortindehaverens kontoudtog,
- landet hvor Salgsvirksomheden har sit hjemsted,
- beskrivelse af de tilbudte varer og tjenester,
- priser,
- transaktionsvaluta,
- skatter og andre myndighedsafgifter,
- reklamationsregler, returnerings- og tilbagebetalingsregler samt leveringsbetingelser,
- fragtomkostninger,
- kundeservicekontakt, e-mailadresse og telefonnummer,
- Salgsvirksomhedens besøgsadresse,
- eventuelle eksportrestriktioner,
- logoskrifttyper til Kontokort som Salgsvirksomheden accepterer,
- i det pågældende tilfælde logoskrifttyper for Verified by Visa og MasterCard SecureCode og V.me og MasterPass samt
- øvrige oplysninger iht. den til enhver tid gældende lov, der er anvendelig for Salgsvirksomheden,

Salgsvirksomheden påtager sig at fremlægge korrekte informationer og løbende opdatere informationerne på hjemmesiden angående ovenstående punkter.

5.2 Risikoreduktion
Aktiveret understøttelse af 3D Secure, MasterPass og V.me på Salgsvirksomhedens hjemmeside på internettet indebærer, at Salgsvirksomheden får en såkaldt

risikoreduktion, hvilket betyder, at Kortudstederen normalt ikke kan reklamere falske Korttransaktioner.

Denne risikoreduktion gælder for Kontokort med varemærkerne Visa, MasterCard og Maestro samt ved accept af MasterPass og V.me. For Kontokort med varemærket Visa omfatter risikoreduktionen i øjeblikket dog ikke virksomhedskort og indkøbskort (såkaldte corporate/commercial cards) udstedt af Kortudstedere uden for Europa.

Bambora er ikke ansvarlig for at informere Salgsvirksomheden om korttyper og udstedelsesland eller for advarsler og/eller kontroller, hvis Kontokort omfattes af risikoreduktionen.

Bambora har ret til at ophæve retten til risikoreduktion, hvis bedrageriniveauerne iht. Kortnetværkets vurdering overskrider de aktuelt tilladte niveauer.

Salgsvirksomheden er indforstået med, at 3D Secure, MasterPass og V.me ikke er en garanti for at beskytte sig mod falske Korttransaktioner.

Ved salg af højrisikovarer som f.eks.: hjemmeelektronik, ure, smykker og gavekort er Salgsvirksomheden indforstået med sin risikoeksponering for falske Korttransaktioner, da dette er varer, der oftest udsættes for kortbedragerier. Der kræves et modtagelsesbevis på leverancerne.

Salgsvirksomheden skal for egen regning implementere eller skaffe systemer til at forhindre falske bestillinger.

Salgsvirksomheden bærer hele risikoen for Korttransaktioner, hvis risikoreduktion som findes iht. 3D Secure, MasterPass og V.me ikke anvendes.

5.3 Specielt vedrørende Recurring Payments (tilbagevendende betalinger) ved salg via internet

- Når Salgsvirksomheden tilmelder en ny Kortindehaver til tilbagevendende betalinger, og debitering ikke er aktuel på tilslutningstidspunktet, så skal der gennemføres en såkaldt kontrol af status på Kortindehaverens Kontokort en såkaldt "nulværdi-autorisation".
- Når Salgsvirksomheden tilmelder en ny Kortindehaver, som betaler med Kontokort sender Salgsvirksomheden den første debiteringstransaktion iht. 3D Secure. For denne transaktion gælder den aktuelt gældende risikoreducering iht. 3D Secure.
- Ved efterfølgende tilbagevendende kortbetalinger (debiteringer) gælder risikoreduceringen iht. 3D Secure ikke, hvilket betyder at Salgsvirksomheden bærer hele risikoen, såfremt intet andet er aftalt.
- Når en Kortindehaver tilslutter sig og indgår aftale om tilbagevendende kortbetaling, skal Kortindehaveren modtage en kvittering pr. e-mail. Kvitteringen skal indeholde teksten "tilbagevendende kortbetaling" og indeholde informationer om beløbets størrelse, hvor ofte debitering sker og hvor længe aftalen gælder. Det skal fremgå, om det drejer sig om et fast beløb eller et variabelt.

- Når en Kortindehaver betaler varer og/eller tjenester hos Salgsvirksomheden, må Salgsvirksomheden ikke tilslutte Kortindehaveren til Recurring Payments uden at dette fremgår tydeligt og uden at dette accepteres af Kortindehaveren.
- Kortindehaveren skal modtage en e-mailmeddelelse før hver debitering.
- Kortindehaveren skal modtage en e-mailmeddelelseføר udløbet af eventuelle "gratisperioder" eller andre typer af introduktionstilbud.
- Kortindehaveren skal løbende informeres via e-mailmeddelelse om eventuelle ændringer i debiteringerne f.eks. ændring af beløb og dato for debitering.
- Kortindehaveren skal kunne afbryde sin tilbagevendende kortbetaling med umiddelbar virkning.
- Salgsvirksomheden må ikke gemme Kontokortnummer og øvrige Kontokortinformationer i deres eget system, hvis der ikke er gennemført og godkendt sikkerhedsvalidering og i det pågældende tilfælde certificering iht. Kortnetværkets krav (PCI DSS).
- Salgsvirksomheden skal kunne udarbejde dokumentation fra softwaren, som håndterer 3D Secure og Kundekvitteringen vedrørende Kortindehaverens valg af debiteringsfrekvens og tidsperiode, som Recurring Payments er blevet tilladt af Kortindehaveren.
- Korttransaktionen skal indeholde informationer om Recurring Payment. Salgsvirksomheden har ansvaret for de krav, der stilles i forhold til PSP, så korttransaktionernes indhold er i overensstemmelse med Generelle betingelser, Bestemmelser og Instruktioner.
- Korttransaktionen skal altid kontrolleres gennem Autorisation før hver debitering. Hvis Autorisation nægtes, må debitering ikke gennemføres.
- Det beløb, som iht. aftalen med Kortindehaveren skal debiteres, må ikke ændres uden Kortindehaverens accept.

5.4 Specielt vedrørende Account on File ved salg via internet

- Når Salgsvirksomheden tilslutter en ny Kortindehaver, som betaler med Kontokort sender Salgsvirksomheden den første transaktion iht. 3D Secure. For denne transaktion gælder den aktuelt gældende risikoreducering iht. 3D Secure.
- Når Salgsvirksomheden tilmelder en ny Kortindehaver til tilbagevendende betalinger og debitering ikke er aktuel på tilslutningstidspunktet, så skal der gennemføres en såkaldt kontrol af status på Kortindehaverens Kontokort en såkaldt "nulværdi-autorisation".
- Ved efterfølgende kortbetalinger (debiteringer) gælder risikoreduceringen iht. 3D Secure ikke, hvilket betyder at Salgsvirksomheden bærer hele risikoen, såfremt intet andet er aftalt.

6. Sikkerhed

6.1 Håndtering af bestemte kontokortinformationer

Med henblik på dels at bevare et højt sikkerhedsniveau i de globale kortbetalingssystemer, dels at styrke tilliden til Kontokort som betalingsmiddel, er det af yderste vigtighed, at alle, som håndterer Kontokortinformationer, gør det på en sikker måde. Med "Kontokortinformationer" forstås sådanne informationer, som er præget eller trykt på Kontokortets for- og bagside, inklusive informationer som er lagret i Kontokortets magnetspor og chip. Derfor har Kortnetværkene vedtaget en fælles standard for håndtering af Kontokortinformationer. Standarden kaldes Payment Card

Industry (PCI) Data Security Standard (DSS) og er udviklet af de internationale kortnetværk Visa og MasterCard.

Salgsvirksomheden forpligter sig til at overholde standarden PCI DSS i den udformning, der til enhver tid er offentliggjort på www.pcisecuritystandards.org.

6.2 Godkendelse af systemer
Systemer, som leverer Transaktioner til Bambora, skal være godkendt af Bambora eller anden tredjepart, som Bambora anviser. Bambora kan stille krav til særlig kontrol af komponenter, der er følsomme ud fra et sikkerhedsmæssigt synspunkt. Denne kontrol eller scanning udføres af en i samråd med Bambora udvalgt aktør.

6.3 Specielt vedrørende Payment Service Providers
Hvis Salgsvirksomheden anvender en tredjepart (såkaldt Payment Service Provider) til dele af eller al Distancehandel, skal Salgsvirksomheden sikre, at denne opfylder alle krav iht. PCI DSS.

6.4 Ændringer i systemer m.m.
Ændringer i systemet, som påvirker de gældende forudsætninger på tidspunktet for godkendelsen, må ikke gennemføres uden Bamboras godkendelse.

Salgsvirksomheden skal gennemføre en af Bambora anvist test af opkoblingen til Bamboras modtagelsessystem, inden Transaktioner må indsendes til Bambora. Salgsvirksomheden skal informere Bambora om enhver form for installation, flytning eller afvikling af udstyr, som er teknisk tilsluttet til Bambora eller en anden indsamler af Transaktioner, der arbejder efter ordre fra Salgsvirksomheden inden for rammerne af denne aftale.

6.5 Dataangreb og IT-forensisk undersøgelse
Hvis Bambora har mistanke om, at Salgsvirksomhedens kassesystemer, it-systemer eller lignende har været udsat for angreb, manipulation eller lignende, som efter Bamboras mening på nogen måde berører Parternes samarbejde iht. denne Aftale, har Bambora ret til at foretage en såkaldt IT-forensisk undersøgelse ("Undersøgelsen") af det pågældende udstyr. Undersøgelsen må foretages af Bambora eller af en IT-forensisk virksomhed, der er engageret af Bambora.

Tidspunkt og dermed relaterede spørgsmål/rutiner, som kan henføres til Undersøgelsens gennemførelse, skal, hvis Bambora ikke vurderer dette som ubelejliget, om muligt aftales mellem Parterne. Bambora må dog også, hvis det efter Bamboras mening er mest formålstjenligt, besøge Salgsvirksomheden og gennemføre Undersøgelsen, uden at Salgsvirksomheden underrettes herom på forhånd.

Det påhviler Salgsvirksomheden i rimeligt omfang at medvirke ved Undersøgelsen og lette gennemførelsen, således at formålet med Undersøgelsen, dvs. at konstatere hvorvidt der har været angreb/manipulation, kan opnås.

I tilfælde af, at det ved Undersøgelsen konstateres at Salgsvirksomhedens kassesystemer, it-systemer eller lignende, har været udsat for angreb, manipulation eller lignende, påhviler det Salgsvirksomheden på Bamboras anmodning at godtgøre Bambora omkostninger til Undersøgelsen.