

**FÖRESKRIFTER FÖR FÖRSÄLJNING MOT
BETALNING MED KONTOKORT
DISTANSHANDEL (Card Not Present)
(Oktober 2015)**

Dessa föreskrifter, "Distanshandelsföreskrifterna", gäller för försäljning mot betalning med Kontokort vid Distanshandel. Med "Distanshandel" avses Försäljningssätt där Kontokort inte är närvarande vid betalningstillfället. De "Försäljningssätt" som omfattas av Distanshandelsföreskrifterna är t.ex. försäljning över internet, försäljning mot post- och/eller telefonorder, mobilbetalningar, återkommande betalningar så som lagrat kortnummer (sk "Account on File") och abonnemangsbetalningar (sk "Recurring Payments").

Distanshandelsföreskrifterna utgör ett komplement till de Allmänna villkor för inlösen av kontokortstransaktioner som gäller för det avtal om Inlösen av Kontokortstransaktioner ("Huvuddokumentet") som slutits mellan Sälj företaget och Bambora. Vid eventuella konflikter mellan Huvuddokumentet och Distanshandelsföreskrifterna ska Distanshandelsföreskrifterna ha företräde. Ord som inleds med en versal, dvs. stor bokstav avser ett ord som givits en särskild innebörd/definition i Huvuddokumentet och ska i dessa Distanshandelsföreskrifter ha samma innebörd som de har i Huvuddokumentet.

1. Allmänt om försäljning mot betalning med Kontokort vid Distanshandel

Vid försäljning med Kontokort via internet accepteras samtliga Kontokort enligt Avtalet samt i förekommande fall MasterPass och V.me med undantag av Maestro-kort som endast kan accepteras om 3D Secure är installerat och aktiverat. Vid Telefon- och Postorder accepteras dock aldrig Maestro.

2. Särskilda åtaganden vid Distanshandel

Sälj företagets åtager sig att:

- På beställningsformuläret eller internetsidan tydligt informera kortinnehavaren, innan betalningsinstruktionerna, i vilket land Transaktionen sker samt i vilket land Sälj företaget betalar mervärdesskatt,
- På sin hemsida inte ha information eller länkar till hemsidor med olaglig och/eller enligt Bamboras bedömning oetisk verksamhet eller till verksamhet som på objektiva grunder måste anses skada Bamboras anseende,
- Omedelbart underrätta Bambora om den hemsida på vilken Sälj företagets försäljning sker; byter www-adress och/eller nya www-adresser införs som Sälj företaget använder för sin försäljning med kontokort.

3. Kontroller

Sälj företaget ska före debitering av kortinnehavaren utföra nedan angivna kontroller;

3.1 Auktorisation

Auktorisation ska alltid ske vid betalningstillfället, oavsett köpbelopp. Auktorisationen ska kodas med korrekt Försäljningssätt.

Vid kontroll av status på Kortinnehavarens Kontokort (kontroll av kortstatus) ska alltid en s.k. ”nollvärdesauktorisering” användas.

3.2 Identifiering av Kortinnehavare

3.2.1 Internet

Korttransaktion ska vara genomförd enligt 3D Secure om inte annat överenskommit mellan parterna.

3.2.2 Telefonorder och Postorder

Vid Telefon- och Postorder kan inte Sälj företaget säkerställa Kortinnehavarens identitet. Sälj företaget står av denna anledning alltid risken för samtliga köptransaktioner vid Telefon- och Postorder. Detta innebär att Bambora har rätt att återdebitera Sälj företaget sådant belopp som reklamerats av Kortinnehavare. Detta gäller oavsett om Kortinnehavarens invändning är berättigad eller inte.

3.2.3 Postorder

Postorderunderlaget ska begäras in i sluten försändelse till Sälj företaget och innehålla:

- Sälj företagets namn, ort och organisationsnummer,
- Kortinnehavarens namn,
- Kortinnehavarens adress (leveransadress),
- Kortinnehavarens telefonnummer,
- Namn på Kortutgivare,
- Kontokortsnummer,
- Kontokortets giltighetstid,
- Beställningsdatum,
- Beställningens totalbelopp,
- Uppgift om mervärdesskatt,
- Beskrivning av beställda varor, samt
- Kortinnehavarens namnteckning.

3.2.4 Lagring

Sälj företaget ska under minst 18 månader arkivera orderformulär/beställningsunderlag i enlighet med Payment Card Industry (PCI) Data Security Standard (DSS). På Bamboras begäran ska Sälj företaget inom fem (5) bankdagar tillhandahålla orderformulär-/beställningsunderlag avseende enstaka Transaktioner.

3.3 Mottagningsbevis

Vid leverans av fysiskt levererbara varor eller biljetter rekommenderas leveranssätt som exempelvis postpaket eller brev där signerat mottagningsbevis med Legitimationskontroll vid utlämningstillfället kan erhållas. Vid leverans av högriskvaror krävs dock mottagningsbevis, se punkt 5.2. Om Kortinnehavare reklamerar köp och mottagningsbevis använts underlättar detta efterföljande utredning. Utredning kan dock påvisa att Bambora ändå har rätt till Återdebitering av inlöst Korttransaktion enligt reglerna i Allmänna Villkor.

Sälj företaget står all risk för Återdebiteringar av inlösta Korttransaktioner enligt reglerna i i Allmänna Villkor om Kortinnehavaren bestrider att vara eller tjänst erhållits oavsett hur Kortinnehavaren identifierat sig enligt punkt 3.3.

4. Redovisning

4.1 Insändande av köptransaktioner m.m.

Elektroniskt insamlade köptransaktioner ska senast inom två (2) dagar från dagen för betalningen överförs till Bambora. Som "dagen för betalningen" avses dagen för auktorisationen. För miljöer som t ex hotell där en sk preliminär auktorisation sker ska köptransaktionen vara Bambora tillhanda inom trettio (30) dagar.

4.2 Transaktionsinformation

Sälj företaget ska vid leverans av vara eller tjänst tillhandahålla Kortinnehavaren Kundkvitto via e-post eller tillsammans med vara/tjänst vid leverans. Kundkvittot ska innehålla följande information:

- Ordet "kvitto" i rubriken,
- Sälj företagets namn. Namnet ska vara detsamma som uppgetts i Avtalet till Bambora och som därmed anges på Kortinnehavarens kontoutdrag,
- Telefonnummer och e-postadress till Sälj företagets kundtjänst,
- I förekommande fall, Sälj företagets hemsida (web-adress),
- Trunkerat Kontokortsnummer,
- Korttransaktionens belopp tillsammans med transaktionsvaluta,
- Transaktionsdatum och klockslag,
- Unikt transaktionsnummer/ordernummer som identifierar transaktionen,
- Erhållet Kontrollnummer från Auktorisation,
- I förekommande fall, upplysning om att det avser en internettransaktion,
- Transaktionstyp (köp eller retur),
- Beskrivning av beställda varor och tjänster,
- Retur- och återbetalningsregler,
- Övriga uppgifter enligt vid var tid gällande tillämplig lag,
- Vid telefonorder ska Sälj företaget på Kortinnehavarens kvitto skriva "TO" eller "Telephone Order" samt
- Vid Postorder ska Sälj företaget skriva "MO" eller "Mailorder".

I de fall fysiskt kvitto på genomförd och redovisad Korttransaktion inte föreligger, till exempel vid vissa former av Internethandel, ska Sälj företaget upprätta och spara Transaktionslogg och på Bamboras begäran utlämna följande information om;

Korttransaktionen:

- Sälj företagets namn,
- Sälj företagets redovisningsnummer hos Bambora,
- I förekommande fall Sälj företagets hemsida (webb-adress),
- Beskrivning av varor eller tjänster,
- Mottagarens namn och leveransadress samt i förekommande fall mottagarens metod för att autentisera sig t ex 3D Securekod,

- Trunkerat Kontokortsnummer,
- Korttransaktionens belopp tillsammans med transaktionsvaluta och moms,
- Transaktionsdatum och klockslag,
- Unikt transaktionsnummer/ordernummer som identifierar transaktionen,
- Erhållet Kontrollnummer från Auktorisation,
- Transaktionstyp (köp eller retur),
- Indikator för elektronisk handel,
- Beställarens IP-adress.

Transaktionsloggen ska uppfylla kraven enligt PCI DSS.

Sälj företaget ska på Bamboras begäran förevisa information om Korttransaktion från system som hanterar 3D Secure. Om detta system hanteras av Payment Service Provider (PSP) ska Sälj företaget säkerställa att PSP kan förevisa denna information på Sälj företagets uppdrag. Detta gäller även vid begäran om information om Korttransaktion i Transaktionslogg.

5. Övrigt

5.1 Säljställe

Säljställets försäljningsplats på internet ska innehålla minst följande information:

- Sälj företagets namn. Namnet ska vara detsamma som uppgetts till Bambora i Avtalet och som därmed anges på Kortinnehavarens kontoutdrag,
- Land där Sälj företaget har sin hemvist,
- Beskrivning av erbjudna varor och tjänster,
- Priser,
- Transaktionsvaluta,
- Skatter och andra myndighetspålagor,
- Reklamationsregler, retur- och återbetalningsregler, samt leveransvillkor,
- Fraktkostnader,
- Kundtjänstkontakt, e-postadress och telefonnummer,
- Sälj företagets besöksadress,
- Eventuella exportrestriktioner,
- Logotyper för Kontokort som Sälj företaget accepterar,
- I förekommande fall logotyper för Verified by Visa och MasterCard SecureCode samt V.me och MasterPass samt
- Övriga uppgifter enligt vid var tid gällande lag tillämplig för Sälj företaget.

Sälj företaget åtar sig att tillhandahålla korrekt information och att löpande uppdatera informationen på hemsidan angående ovanstående punkter.

5.2 Riskreduktion

Aktiverat stöd för 3D Secure, MasterPass och V.me på Sälj företagets hemsida på internet innebär att Sälj företaget erhåller en så kallad riskreduktion vilket innebär att Kortutgivaren i normalfallet inte kan reklamera bedrägliga Korttransaktioner.

Denna riskreduktion gäller för Kortkort med varumärkena Visa, MasterCard och Maestro samt vid acceptans av MasterPass och V.me. För Kortkort med varumärket Visa omfattar riskreduktionen för närvarande dock inte företagskort och inköpskort (så kallade corporate/commercial cards) utgivna av Kortutgivare utanför Europa.

Bambora ansvarar inte för att informera Sälj företaget om korttyper och utgivningsland eller för varningar och/eller kontroller om Kortkort omfattas av riskreduktionen.

Bambora har rätt att upphäva rätten till riskreduktion om bedrägerinivåerna enligt Kortnätverkens bedömning överskrider vid var tid tillåtna nivåer.

Sälj företaget är medvetet om att 3D Secure, MasterPass och V.me inte är en garanti för att skydda sig mot bedrägliga Korttransaktioner.

Vid försäljning av högriskvaror som till exempel: hemelektronik, klockor, smycken och presentkort är Sälj företaget medveten om sin riskexponering för bedrägliga Korttransaktioner då detta är varor som ofta utsätts för kortbedrägerier. Mottagningsbevis på leveranserna krävs.

Sälj företaget ska på egen bekostnad implementera eller införskaffa system för att förhindra bedrägliga beställningar.

Sälj företaget står all risk för Korttransaktioner, om riskreduktion som finns enligt 3D Secure, MasterPass och V.me inte tillämpas.

5.3 Särskilt gällande Recurring Payments (återkommande betalningar) vid försäljning över internet

- När sälj företaget ansluter ny Kortinnehavare för återkommande betalningar och debitering ej är aktuell vid anslutningstillfället, så ska en sk kontroll av status på Kortinnehavarens Kortkort en s.k. ”nollvärdesauktorisering” genomföras.
- När Sälj företaget ansluter ny Kortinnehavare som betalar med Kortkort skickar Sälj företaget den första debiteringstransaktionen enligt 3D Secure. För denna transaktion gäller vid var tid gällande riskreducering enligt 3D Secure.
- Vid efterföljande återkommande kortbetalningar (debiteringar) gäller inte riskreduceringen enligt 3D Secure varvid Sälj företaget står all risk, såvida ej annat avtalats.
- När en Kortinnehavare anmäler sig till och ingår överenskommelse om återkommande kortbetalning ska Kortinnehavaren erhålla en kvittens per e-post. Kvittens ska innehålla texten ”återkommande kortbetalning” och innehålla information om beloppets storlek, hur ofta debitering sker och hur länge överenskommelsen gäller. Det ska framgå om det avser ett fast belopp eller ett variabelt.
- När en Kortinnehavare betalar varor och/eller tjänster hos Sälj företaget får inte Sälj företaget ansluta Kortinnehavaren till Recurring Payments utan att detta tydligt framgår och att detta accepteras av Kortinnehavaren.
- Kortinnehavaren ska erhålla ett e-postmeddelande inför varje debitering.
- Kortinnehavare ska erhålla ett e-postmeddelande före utgången av eventuella ”gratisperioder” eller andra typer av, introduktionserbjudande.

- Kortinnehavare ska löpande informeras via e-postmeddelande om eventuella förändringar i debiteringarna t ex förändring av belopp eller datum för debitering.
- Kortinnehavaren ska kunna avbryta sin återkommande kortbetalning med omedelbar verkan.
- Säljföretaget får inte spara Kontokortsnummer och övrig Kontokortsinformation i eget system om inte säkerhetsvalidering och i förekommande fall certifiering enligt Kortnätverkens krav (PCI DSS) är genomförd och godkänd.
- Säljföretaget ska kunna ta fram dokumentation från programvaran som hanterar 3D Secure och Kundkvitto gällande Kortinnehavarens val av debiteringsfrekvens och hur lång tidsperiod som Recurring Payments tillåts av Kortinnehavaren.
- Korttransaktion ska innehålla information om Recurring Payment. Säljföretaget ansvarar för kravställandet mot PSPs så att korttransaktionernas innehåll är i linje med Allmänna Villkor, Föreskrifter och Instruktioner.
- Korttransaktion ska alltid kontrolleras genom Auktorisation inför varje debitering. Om Auktorisation nekats får ej debitering genomföras.
- Det belopp som enligt avtal med Kortinnehavare ska debiteras får inte ändras utan Kortinnehavares medgivande.

5.4 Särskilt gällande Account on File vid försäljning över internet

- När Säljföretaget ansluter ny kortinnehavare som betalar med Kontokort skickar Säljföretaget den första transaktionen enligt 3D Secure. För denna transaktion gäller vid var tid gällande riskreducering enligt 3D Secure.
- När säljföretaget ansluter ny kortinnehavare för återkommande betalningar och debitering ej är aktuell vid anslutningstillfället, så ska en sk kontroll av status på Kortinnehavarens Kontokort en s.k. ”nollvärdesauktorisering” genomföras.
- Vid efterföljande kortbetalningar (debiteringar) gäller inte riskreduceringen enligt 3D Secure varvid Säljföretaget står all risk, såvida ej annat avtalats.

6. Säkerhet

6.1 Hantering av viss kontokortsinformation

I syfte dels att behålla en hög säkerhetsnivå i de globala kortbetalningssystemen, dels att stärka förtroendet för Kontokort som betalningsmedel är det av yttersta vikt att alla som hanterar Kontokortsinformation gör det på ett säkert sätt. Med ”Kontokortsinformation” avses sådan information som finns präglad eller tryckt på Kontokortets fram- och baksida, inklusive information som finns lagrad i Kontokortets magnetspår och chip. Av denna anledning har Kortnätverken enats om en gemensam standard för hantering av Kontokortsinformation. Standarden kallas Payment Card Industry (PCI) Data Security Standard (DSS) och är framtagen av de internationella kortnätverken Visa och MasterCard.

Säljföretaget åtar sig att följa standarden PCI DSS i det utförande den vid var tid finns publicerad på www.pcisecuritystandards.org.

6.2 Godkännande av system

System som levererar transaktioner till Bambora ska vara godkända av Bambora, eller annan tredje part som Bambora anvisar. Bambora kan ställa krav på särskild granskning

av ur säkerhetssynpunkt känsliga komponenter. Denna granskning eller scanning utförs av en i samråd med Bambora utvald aktör.

6.3 Särskilt om Payment Service Providers

Använder Sälj företaget en tredje part (s.k. Payment Service Provider) för delar eller all Distanshandel måste Sälj företaget säkerställa att denna uppfyller alla krav enligt PCI DSS.

6.4 Ändringar i system m.m.

Ändringar i systemet, som påverkar de förutsättningar som gällde vid tidpunkten för godkännande, får inte vidtas utan Bambora godkännande.

Sälj företaget ska genomföra ett av Bambora anvisat test av uppkopplingen mot Bambora mottagningssystem innan Transaktioner får insändas till Bambora. Sälj företaget ska informera Bambora inför varje installation, omflyttning eller avveckling av utrustning som är tekniskt ansluten till Bambora eller annan insamlare av Transaktioner som verkar på uppdrag av Sälj företaget inom ramen för detta avtal.

6.5 Dataintrång och IT-forensisk undersökning

För det fall Bambora misstänker att Sälj företagets kassasystem, datasystem e.d. utsatts för intrång, manipulation e.d. som, enligt Bamboras bedömning, i något avseende berör Parternas samarbete enligt detta Avtal har Bambora rätt att genomföra en s.k. IT-forensisk undersökning ("Undersökningen") av utrustningen i fråga. Undersökningen får genomföras av Bambora eller av ett av Bambora anlitat IT-forensiskt företag.

Tidpunkt, och därmed sammanhängande frågor/rutiner hänförliga till Undersökningens genomförande, ska, om Bambora inte bedömer detta som olämpligt, i möjligaste mån överenskommas mellan Parterna. Bambora får dock även, om detta enligt Bamboras mening är mest ändamålsenligt, besöka Sälj företaget och genomföra Undersökningen utan att Sälj företaget underrättats härom i förhand.

Det åligger Sälj företaget att i skälig omfattning medverka vid Undersökningen och underlätta genomförandet så att syftet med Undersökningen, dvs. att konstatera huruvida intrång/manipulation har skett, kan uppnås.

För det fall det genom Undersökningen konstateras att Sälj företagets kassasystem, datasystem e.d. blivit utsatta för intrång, manipulation e.d. är Sälj företaget skyldigt att på Bamboras begäran ersätta Bambora kostnaderna för Undersökningen.