

FÖRESKRIFTER FÖR FÖRSÄLJNING MOT BETALNING MED KONTOKORT

I OBEMANNAD TERMINAL

(Oktober 2015)

Dessa föreskrifter, "Föreskrifter för obemannad terminal", gäller vid försäljning mot betalning med Kontokort i obemannade terminaler såsom parkeringsautomater, varuautomater och vägtullar.

Föreskrifterna utgör ett komplement till de Allmänna villkor för inlösen av kontokortstransaktioner som slutits mellan Sälj företaget och Bambora. Vid eventuella konflikter mellan Huvuddokumentet och Föreskrifterna ska Föreskrifterna ha företräde.

1. Typer av Terminaler för obemannad miljö

Typ 1 avser Obemannad terminal där auktorisation alltid ska genomföras 'online' oavsett beloppets storlek och där verifiering görs med PIN-kod, såsom t ex varuautomat.

Typ 2 avser Obemannad terminal där auktorisation ska alltid genomföras 'online' oavsett beloppets storlek men som saknar möjlighet till verifiering med PIN-kod. Transaktioner via parkeringsautomater (MCC 7523) i denna miljö får inte överstiga 50 EUR*. Transaktioner via varuautomater (se definition nedan) i denna miljö får inte överstiga 20 EUR*. I övrigt får transaktionsbeloppet aldrig överstiga EUR 100*.

* Eller motsvarande i lokal valuta.

Typ 3 Denna lösning är endast tillåten för Vägtullar (MCC 4784). Avser Obemannad terminal som endast är 'offline' och saknar möjlighet till verifiering med PIN-kod. Transaktioner i denna miljö får inte överstiga EUR 40 och kortet ska kontrolleras mot spärlista.

För obemannad bensinpump (MCC 5542) gäller särskilda föreskrifter.

2. Chip och Pin-terminaler

Terminaler som används för att genomföra transaktioner med Kontokort, ska stödja såväl magnetspårläst som EMV-chip teknologi. MasterCard/VISA kan komma att påföra Bambora en avgift för det fall att Sälj företaget bryter mot ovanstående. Sälj företaget är i detta fall enligt Huvuddokumentet skyldigt att ersätta Bambora för sådana avgifter.

Fr o m 1 januari 2016 ska alla nyinstallerade terminaler, oavsett typ, hos sälj företag som tidigare inte accepterat Kortbetalningar ha stöd för kontaktlösa transaktioner även kallat 'Contactless'. Detta gäller även sälj företag som byter ut samtliga sina kortläsare. Fr o m 1 januari 2020 ska samtliga terminaler ha stöd för kontaktlösa transaktioner.

3. Kundkvitto

Kundkvitto ska alltid lämnas och innehålla följande information:

- Sälj företagets namn, ort och organisationsnummer
- Datum
- Kontokortets nummer ska anges i trunkerad form dvs (endast de (4) sista siffrorna skrivs ut, inledande positioner trunckeras med '*').
- Belopp

- Uppgift om mervärdesskatt
- Referens/återsökningsnummer (unik identitet på Transaktionen)

4. Användning av PIN

Om Terminalen hanterar PIN ska kortinnehavaren ges tre (3) försök att identifiera sig med hjälp av PIN-kod. Matas fel PIN-kod in tre (3) gånger i följd ska utrustningen om möjligt behålla kortet. Dessa kort skickas ituklippta till resp. kortutgivare. Kortinnehavaren ska ha möjlighet att avbryta en transaktion i stället för att göra ytterligare försök med PIN-kod.

Om PIN inte är tillåtet för korttypen kan kortet inte användas i självbetjäningsutrustning med PIN-verifiering.

Med transaktioner via varuautomater avses varor och tjänster som kan säljas vid en obemannad terminal med undantag av:

- Parkeringsplatser, parkeringsautomater och garage (MCC 7523)
- Vägtullar (MCC 4784)
- Bensinpumpar (MCC 5542)
- Alla varor eller tjänster som enligt lag har en åldersgräns vid försäljning (exempelvis spel, tobaksvaror och alkohol)
- Alla varor eller tjänster som enligt andra regler eller föreskrifter har vissa restriktioner vid försäljning och som skulle kräva någon form av kund- eller kortinnehavarverifiering till exempel läkemedel).

4. Transaktionsinsamling

Insamling av köptransaktioner med Kontokort på vilket namn och/eller nummer inte är präglat (exempelvis Kontokort med varumärkena Maestro och Electron) får endast ske i Terminal Typ 1 och för parkeringsautomater (MCC 7523) Typ 2.

5. Redovisning

5.1 Insändande av köptransaktioner

Elektroniskt insamlade köptransaktioner ska senast inom två (2) dagar från dagen för betalningen överföras till Bambora. Som "dagen för betalningen" avses dagen för auktorisationen.

5.2 Transaktionsjournal

Sälj företaget ska föra en särskild journal över samtliga Transaktioner där ett Kontokort har använts, dvs. såväl genomförda som avbrutna Transaktioner. Denna journal ska utvisa:

- På vilket sätt Transaktionen har genomförts,
- Sälj företagets namn (firma), ort och organisationsnummer,
- Datum och klockslag,
- Kontokortets nummer (förutsatt att Terminalen så stödjer ska detta ske i trunkerad form),
- Transaktionstyp (betalning eller retur/kreditering) i klartext,
- Kassaidentitet,

- Kontrollnummer som bevis på auktorisation,
- Belopp att debitera,
- Referens/återsökningsnummer, och
- Svarskod.

5.3 Lagring

Sälj företaget ska under minst arton (18) månader arkivera Transaktionsjournalen i enlighet med de gällande reglerna för PCI DSS (se punkt 6.1 nedan). På Bamboras begäran ska Sälj företaget inom fem (5) dagar kunna tillhandahålla ett kvitto avseende en enskild Transaktion. Detta gäller även om Sälj företagets inlösenavtal med Bambora i övrigt har upphört.

6. Säkerhet

6.1 Hantering av 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 kortindustrin 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.

Sälj företaget 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

Terminal som levererar Transaktioner till Bambora ska vara godkänd av Bambora, eller annan tredje part som Bambora anvisar. Bambora kan ställa krav på särskild granskning av ur säkerhetssynpunkt känsliga komponenter.

6.3 Särskilt om s.k. Noder och Payment Service Providers

Använder Sälj företaget en tredje part (s.k. nod eller Payment Service Provider) som del av sin betalningslösning för hantering av Transaktioner, måste Sälj företaget säkerställa att denne uppfyller alla krav enligt PCI DSS.

6.4 Ändring av utrustning m.m.

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.

Ändringar i Terminal, som påverkar de förutsättningar som gällde vid tillfället för godkännandet, får inte vidtas utan Bamboras medgivande.

Sälj företaget ska, innan transaktioner får överföras till Bambora, genomföra ett av Bambora anvisat test av sin uppkoppling mot Bambora mottagningssystem.

6.5 Särskilt om kassasystem med integrerad kortläsare/Säkerhetsanvisningar

Sälj företag som använder kassasystem med integrerad kortläsare ska även tillse att av Bambora vid var tid särskilt meddelade Säkerhetsanvisningar följs.

6.6 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 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.

7. Liability Shift

Bambora tillämpar s.k. Liability Shift. Detta innebär att Sälj företaget, i förhållandet till Bambora enligt Avtalet, står risken för samtliga förluster hänförliga till magnetspårslästa Transaktioner företagna med obehörigt framställda kort där det korrekta Kontokortet, dvs. det av behörig/licensierad kortutgivare utfärdade Kontokortet med samma kortnummer som det obehörigt framställda, är försett med ett s.k. EMV-chip.