

FÖRESKRIFTER FÖR FÖRSÄLJNING MOT BETALNING MED KONTOKORT OBEMANNAD TERMINAL (Juli 2010)

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

Föreskrifterna utgör ett komplement till de allmänna villkor som gäller för det avtal om Inlösen av Kontokortstransaktioner ("Huvuddokumentet") som slutits mellan Sälj företaget och Euroline/Diners Club. Vid eventuella konflikter mellan Huvuddokumentet och Föreskrifterna ska Föreskrifterna ha företräde.

1. Typer av Terminaler för obemannad miljö

Typ 1 avser Obemannad terminal, såsom t ex varuautomat eller bensinpump där verifiering görs med PIN-kod och auktorisation från 0 kr. Om slutbeloppet inte är känt vid auktorisationstillfället gäller Eurolines/Diners Club vid var tid gällande rutinbeskrivning. Beloppet vid betalningen med Kontokort i denna miljö får inte överstiga 600 SEK.

Typ 2 avser Obemannad terminal som saknar möjlighet till verifiering med PIN-kod men med auktorisation från 0 kr.

Typ 3 avser Obemannad terminal där spärrkontroll sker mot lokalt spärrregister i Sälj företagets system. Rutiner för sådan spärrhantering specificeras i bilaga till Avtalet. Beloppet vid betalningen med Kontokort i denna miljö är får inte överstiga 500 SEK.

Chip och Pin-terminaler

Från och med den 1 januari 2011 skall terminaler som används för att genomföra transaktioner med Kontokort, stödja såväl magnetspärläst som EMV-chip teknologi. MasterCard/VISA och Diners Club International kan komma att påföra Euroline/Diners Club en avgift för det fall att Sälj företaget bryter mot ovanstående. Sälj företaget är i detta fall enligt punkterna 6.3 och 6.4 i Huvuddokumentet skyldigt att ersätta Euroline/Diners Club för sådana avgifter.

. 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 trunkerades med '*').
- belopp
- Uppgift om mervärdesskatt
- Referens/ återsökningsnummer (unik identitet på Transaktionen)

3. 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 självbetjäningstrustning med PIN-verifiering.

4. Transaktionsinsamling

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

5. Redovisning

5.1 Insändande av köptransaktioner

Elektroniskt insamlade köptransaktioner ska senast inom två (2) dagar från dagen för betalningen överföras till Euroline/Diners Club. 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),
- betalningssätt (se punkt 2.1 andra stycket ovan),
- transaktionstyp (betalning eller retur/kreditering) i klartext,
- kassaidentitet,
- kontrollnummer såsom bevis på auktorisation,
- belopp att debitera,
- referens/ återsökningsnummer, och
- svars kod.

5.3 Lagring

Sälj företaget ska under minst arton (18) månader arkivera Transaktionsjournalen i enlighet med de senast gällande reglerna för PCI DSS (se punkt 6.1 nedan). På Eurolines/Diners Clubs begäran ska Sälj företaget inom fem (5) dagar kunna tillhandahålla ett kvitto avseende en enstaka Transaktion. Detta gäller även om Sälj företagets inlösenavtal med Euroline/Diners Club 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.

Detta innebär bl.a. att Sälj företaget:

- inte under några som helst omständigheter får lagra eller skriva ut i) CVV/CVC (dvs. kortverifieringsvärdet i Kontokortets magnetremsa), ii) CVV2/CVC2 (dvs. den säkerhetskod som normalt finns i slutet av signaturpanelen på Kontokortets baksida) eller iii) iCVV/iCVC (dvs. verifieringsvärdet i ett Kontokort som är försett med chip). Sälj företaget åtar sig även att inte lagra eller skriva ut PVV (dvs. verifieringsvärdet för PIN koder),
- endast får lagra sådan Kontokortsinformation som är absolut nödvändig för Sälj företagets verksamhet (dvs. namn, Kontokortets nummer och Kontokortets giltighetstid),
- ska förvara/lagra media som innehåller Kontokortsinformation (t.ex. loggar, transaktionsrapporter, elektroniska kvitton eller avtal) på en säker plats och på ett sådant sätt att endast personer som med nödvändighet behöver tillgång till materialet i fråga bereds sådan tillgång,
- ska hantera all Kontokortsinformation konfidentiellt och att inte till tredje part yppa något om de personuppgifter (t.ex. namn och personnummer) som Sälj företaget kan komma att få del av,
- ska förvara information om Kontokortets nummer på ett sådant sätt att ingen obehörig användning kan förekomma,
- ska tillse att elektroniska kvitton och andra medium är skyddade mot obehörig åtkomst,
- omedelbart ska anmäla till Euroline/Diners Club om Sälj företaget upptäcker, eller misstänker, att Kontokortsinformation har använts obehörigt eller att sådan information på annat sätt har missbrukats. Vid misstanke om brott ska Sälj företaget på Eurolines/Diners Clubs begäran även polisanmäla händelsen,
- ska tillse att Kontokortets nummer inte exponeras för andra personer än sådan personal hos Sälj företaget som med nödvändighet behöver tillgång till detta,
- ska tillse att det finns dokumenterat hur Kontokortsinformation skyddas i Sälj företagets tekniska utrustning,
- ska tillse att det finns rutiner för säker hantering och distribution av Kontokortsinformation och att dessa rutiner regelbundet följs upp och granskas. Rutinerna, eller information om dessa, ska förstöras på ett säkert sätt, t.ex. genom dokumentförstörare, när rutinerna/informationen inte längre behövs enligt tillämplig lagstiftning och/eller Instruktionerna,
- ska tillse att det finns en förteckning över all teknisk utrustning och att denna utrustning förvaras på ett säkert sätt,
- ska tillse att Kontokortsinformation och/eller Kortinnehavare, så snart teknisk utrustning och/eller annat medium som innehåller sådan information inte längre ska användas av Sälj företaget, görs obrukbar.

6.2 Godkännande av system

Terminal som levererar Transaktioner till Euroline/Diners Club ska vara godkänd av Euroline/Diners Club, eller annan tredje part som Euroline/Diners Club anvisar. Euroline/Diners Club 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 Euroline/Diners Club inför varje installation, omflyttning eller avveckling av utrustning som är tekniskt ansluten till Euroline/Diners Club eller annan insamlare av Transaktioner.

Ändringar i Terminal, som påverkar de förutsättningar som gällde vid tillfället för godkännandet, får inte vidtas utan Eurolines/Diners Clubs medgivande.

Sälj företaget ska, innan transaktioner får överföras till Euroline/Diners Club, genomföra ett av Euroline/Diners Club anvisat test av sin uppkoppling mot Euroline/Diners Clubs mottagningssystem.

6.5 Särskilt om kassasystem med integrerad kortläsare/Säkerhetsanvisningar

Sälj företaget som använder kassasystem med integrerad kortläsare ska även tillse att av Euroline/Diners Club vid var tid särskilt meddelade Säkerhetsanvisningar följs.

6.6 Dataintrång och IT-forensisk undersökning

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

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

Det åligger Sälj företaget att i skäligen 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 Eurolines/Diners Clubs begäran ersätta Euroline/Diners Club kostnaderna för Undersökningen.

7. Liability Shift

Euroline/Diners Club kommer för Transaktioner företagna från och med den 1 januari 2009 att tillämpa ett s.k. Liability Shift. Detta innebär att Sälj företaget från och med denna dag, i förhållandet till Euroline/Diners Club 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.