

Sikkerhed ved modtagelse af kortbetalinger

Internethandel og post- og telefonordre

De fleste er ærlige ... heldigvis!

Hvert år gennemføres millioner af transaktioner med betalingskort, og heldigvis går langt de fleste godt.

Men i de situationer, hvor forretning og kunde ikke mødes, kan det være fristende for en svindler at forsøge at bruge stjålne kortoplysninger til at betale med. Der er ikke altid sikkerhed for, at kortet tilhører den, som betaler med det, og det er umiddelbart ikke muligt for Teller at verificere kunden over for din forretning. Det er derfor utrolig vigtigt, at du og dine medarbejdere er meget opmærksomme, når I modtager kortbetalinger, for du kan selv gøre meget for at reducere risikoen for misbrug.

Du kan undgå mange tilfælde af kortmisbrug ved at følge anbefalingerne i dette dokument. Sørg for, at dine medarbejdere er grundigt informeret om, hvad I kan gøre for at reducere risikoen for svindel, og hvad I skal gøre, hvis I får mistanke om forsøg på svindel.

Hvordan der kan svindles

- Kriminelle kan have stjålet kortoplysninger (kortnummer, udløbsdato og kontrolcifre) fra kortholder enten ved fysisk at have set kortet eller fx via e-mail eller forfalskede hjemmesider med fup-tekst (Phishing). Derefter bruger de kriminelle kortoplysningerne til at handle på internettet for.
- Ved stjålne kort kan kortoplysningerne anvendes på internettet og ved post- og telefonordre, inden kortet bliver spærret

Hvilke kort du kan modtage

Afhængig af din betalingskortaftale kan du modtage følgende kort i forbindelse med internethandel og post- og telefonordre:

- Dankort, inkl. Visa/Dankort
- MasterCard
- Visa
- Visa Electron (hvis udsteder tillader det)
- JCB
- American Express

Følgende kort kan desuden modtages i forbindelse med internethandel:

- eDankort
- Maestro (kun med MasterCard SecureCode)

Se brugervejledning for mere information

Forretningens ansvar ved internethandel og post- og telefonordre

- Din forretning skal anvende betalingssoftware, der er testet og godkendt af Teller
- Din forretnings website skal som minimum leve op til de krav, der er angivet i brugervejledning og generelle regler med hensyn til oplysninger mm.
- Kunden har mulighed for at gøre indsigelse mod transaktionen, fx hvis varen ikke er leveret. Derfor bør du sikre dig dokumentation for, at kunden har modtaget varen. Hvis du ikke kan levere en sådan dokumentation, kan Teller tilbageføre beløbet fra din konto
- Det er dit eget ansvar at gennemføre de sikkerhedsforanstaltninger, der er beskrevet i dette dokument.

Jo flere overvågningsparametre/sikkerhedskontroller der benyttes, jo større er chancen for at undgå misbrug!

Hvad du skal være opmærksom på

- **Kontrollér kundens oplysninger**
 - Få oplyst et telefonnummer ved ordren, som du kan sammenligne med leveringsadressen.
 - Ved alternativ leveringsadresse bør du kontrollere, at det oplyste telefonnummer passer med betalingsadressen og ikke leveringsadressen
 - C/o-leveringsadresse besværliggør en eventuel efterforskning. Bed derfor altid om yderligere oplysninger
 - Ved ordrer med mangelfulde oplysninger bør du altid kontakte kunden for at få flere oplysninger
 - Vær opmærksom på ordrer fra afsendere med gratis e-mail adresse, da afsenderen ikke kan spores. Bed derfor om kundens private e-mail adresse.
 - Undgå enhver form for anonymisering af kunderne. Jo mere anonymitet – Jo større er risikoen for misbrug!
 - Brug din sunde fornuft – Hvis det lyder for godt til at være sandt, er det måske ikke en reel kortholder
 - Afvis salget, hvis du er i tvivl.
- **Læg mærke til kundens adfærd**
 - Er det en meget stor ordre?
 - Er det en meget dyr vare?
 - Bestilles samme produkt flere gange?
 - Bestilles varerne om natten?
 - Bestilles en hastelevering – uanset omkostninger?
 - Bestiller samme kunde mange ting over relativ kort periode?
 - Beder kunden om opdeling af betalingen på flere kortnumre? (dette er ikke tilladt og ofte ensbetydende med svindel).
 - Er "Æ", "Ø" og "Å" udeladt af navn / leveringsadresser i Danmark?

- **Kontrollér den anvendte IP adresse (kan du ikke finde IP adressen – kontakt din leverandør af betalingsløsningen)**

- Den geografiske placering af IP adresser kan kontrolleres på nettet (fx på www.db.ripe.net/whois)
- Ved kontrol af IP adresser bør du være opmærksom på følgende:
 - Er der match mellem IP adressens geografiske placering og leveringsadressen?
 - Er der sammenfald i benyttede IP adresser? (Fx stigende antal ordrer fra forskellige kunder med tilnærmelsesvis matchende IP adresser)
 - Vi anbefaler, at du blokerer for IP adresser, der er relateret til misbrug (kontakt din betalingsløsningsleverandør for at høre nærmere om muligheden for at blokere IP-adresser)

- **Salg i Danmark – Hvad kan du selv gøre, for at minimere risikoen for misbrug af betalingskort i Danmark?**

Levering af varer til udlandet er ikke det eneste risikoscenarie I bør forholde jer til. Det er ligeledes vigtigt, at I kontrollerer leveringer til Danmark, der er under mistanke for at være relateret til misbrug.

I forbindelse med misbrug på nationalt plan, er det ikke et ukendt fænomen, at borgere bliver ansat til at modtage og videresende pakker. I langt størstedelen af denne type sager, er de pågældende borgere i god tro, og har ingen idé om, at de er blevet ansat af et svindelforetagende med kortmisbrug for øje. Derfor vil kunderne, i sådanne situationer, også bekræfte at de ønsker varen leveret.

Derfor anbefales det, at I kontakter kunden og spørger ind til nedenstående, når I har mistanke om kortmisbrug i Danmark.

- Har kunden selv foretaget bestillingen?
- Er den pågældende ordre foretaget på kundens eget kort?
- Skal kunden sende pakken videre?
- Er kunden ansat til at modtage/videresende pakker?

- **Salg til udlandet – Misbrug af betalingskort på nettet er et globalt fænomen**

- Du skal specielt være opmærksom på fremsendelse af varer til "Risikolande". Betegnelsen "Risikolande" kan ikke fast defineres, da det afhænger af udviklingen i misbrug.
- Du bør derfor være opmærksom på, om ordrerne virker realistiske fx er mobiltelefoner sendt fra Danmark til Ghana eller cykler sendt til Singapore ikke umiddelbart realistiske!

- **Afviste transaktionsforsøg**

- Såfremt det er teknisk muligt, bør du have oplysninger om alle transaktionsforsøg, herunder afvisninger. Oplysningerne bidrager til dit samlede overblik over kundernes adfærd
- Mange afvisninger forud for en godkendt betaling indikerer som regel, at der er tale om forsøg på misbrug
- Dit betalingsmodul kan sættes op til at begrænse, hvor mange transaktioner/afvisninger der må være på det enkelte kortnummer inden for en given periode.

- **PCI-DSS (Payment Card Industry-Data Security Standard)**

Du skal sikre, at leverandøren af din betalingsløsning lever op til sikkerhedskravene i PCI-standarden, som de internationale kortselskaber (Visa, MasterCard, American Express, JCB og Discover) har udarbejdet i fællesskab. Teller deltager naturligvis også, og derfor er Dankort også omfattet. Overordnet går PCI-DSS ud på at overholde nedenstående 6 punkter. Læs mere på www.pbs.dk.

- Hav et sikkert netværk
- Beskyt kortdata
- Håndter sårbarheder med faste procedurer
- Implementer en stærk adgangskontrol
- Overvåg og test jeres netværk løbende
- Oprethold en sikkerhedspolitik

Du skal kunne dokumentere, at du lever op til kravene i PCI-DSS standarden.

- **MasterCard SecureCode, Verified by Visa og J/Secure**

Dit betalingsmodul bør understøtte denne fælles sikkerhedsstandard, som MasterCard, Visa og JCB har udarbejdet til brug ved modtagelse af disse betalingskort på nettet (inkl. Maestro). Ud over kortnummer, udløbsdato og kontrolcifre skal kortholderen identificere sig med en valgfri personlig adgangskode. Kortudsteder tjekker automatisk, om adgangskoden og kortet passer sammen. Kontakt din leverandør, hvis dit betalingsmodul ikke understøtter denne fælles sikkerhedsstandard.

Når din internetforretning understøtter denne sikkerhedsstandard, reducerer du din økonomiske risiko betragteligt. Dog er det væsentligt at pointere, at det ikke fritager dig for den øvrige kontrol af kunden og ordren.

Husk, at selv om du benytter 3 D Secure, skal du kunne levere dokumentation for transaktionen, herunder at varen er modtaget af kunden.

Kontrolcifre

Når du modtager betalingskort på internettet eller i post- og telefonordre, skal kontrolcifre medsendes transaktionen. Det betyder, at kortholderen udover kortnummer og udløbsdato skal opgive betalingskortets kontrolcifre ved kortbetaling på internettet.

Kontrolcifrene er et trecifret tal – typisk de tre sidste cifre i en talrække – som er trykt bag på betalingskortet (dog 4 cifret på forsiden af American Express).

Husk, at det ikke er tilladt at lagre eller på anden måde gemme kontrolcifrene, når betalingstransaktionen er gennemført. Det er din forretnings ansvar at sikre, at dette ikke sker. Ved post- og telefonordre skal du fx sørge for, at kontrolcifrene destrueres eller overstreges, når betalingstransaktionen er gennemført.

Forretningens risici ved salg over internettet eller via post- og telefonordre

Ved salg via internettet eller post- og telefonordre har din forretning risikoen for tredjemandsmisbrug, uanset om det drejer sig om Dankort eller internationale betalingskort. Det betyder med andre ord, at hvis rette kortholder på tro og love erklærer, at han/hun ikke har foretaget transaktionen, vil hele beløbet inkl. indsigelsesgebyr (se mere i generelle regler og prisliste) blive tilbageført fra din forretnings konto. Derfor skal du altid foretage de sikkerhedsforanstaltninger, vi har beskrevet her, så du reducerer din risiko for tab. Det er ikke nok at få en autorisationsgodkendelse på kortet. Brug af 3 D Secure nedsætter dog væsentligt din risiko for indsigelser på grund af tredjemandsmisbrug ved internethandel.

Derudover er der ligesom i den fysiske verden en begrænset dækningsgaranti på Dankort og Visa/Dankort. Se nærmere information i Generelle regler for Dankort punkt 5. Dækningsgarantien gælder ikke ved 3. mandsmisbrug.

Du bærer risikoen, hvis varen er beskadiget, stjålet el. lign., før den er afleveret til kunden, uanset om det er dig selv eller et andet firma, der står for fragten. Varen må ikke sættes i garage, afleveres hos naboen eller lign. medmindre det er aftalt med kunden.

Det er hovedreglen, at kunden har 14 dages fortrydelsesret; de kan undlade at modtage eller afhente den bestilte vare. Du skal så godtgøre kunden med det samme dog senest inden 30 dage.

Autorisation på internationale betalingskort

På de kort, der er omfattet af betalingskortaftalen for internationale kort, betyder en godkendt autorisation, at kortet er gyldigt, og at det i autorisationsforespørgslen angivne beløb reserveres. For at undgå problemer for kortholder, hvis du fx alligevel ikke kunne levere varen, er det vigtigt, at du sikrer dig, at du ikke autoriserer og dermed reserverer det samme beløb flere gange.

En autorisationskode er ikke ensbetydende med, at det er den rigtige kortholder, der bruger kortet. Derfor skal du altid foretage de sikkerhedsforanstaltninger, vi har beskrevet i dette dokument.

Hvis du ikke kan levere de varer, som kortholder har bestilt, inden for 7 dage efter bestillingen, eller du er i tvivl om, du kan levere, så må du ikke sende en autorisationsforespørgsel til Teller på hele ordrebøbet. Så kan du vælge at sende en forespørgsel på fx 1 krone for at sikre dig, at kortet ikke er spærret. Herefter kan du autorisere, når du er klar til at levere varen.

Du kan også opdele leverancen i flere delleverancer. Det betyder blot, at du skal sende en autorisationsforespørgsel på det aktuelle beløb ved hver delleverance.

Hvis du har foretaget en autorisation og alligevel ikke kan levere, eller kunden afbestiller sin ordre, så skal du annullere autorisationen med det samme.

Det samme gælder, hvis du benytter MasterCard SecureCode, Verified by Visa og J-Secure. Her skal du gemme autentifikationssvaret, indtil du er klar til at gennemføre autorisation.

De krav, Teller stiller til betalingsmodul-leverandørerne/betalingsgateways, efterlever ovenstående funktioner. Men det er dit ansvar, at din leverandør håndterer dine transaktioner korrekt.

Kontrolforespørgsel på Dankort

Når du modtager betalinger med Dankort, skal du sørge for, at systemet laver en kontrolforespørgsel på kortet indeholdende kortnummer, udløbsdato og kontrolcifre. Hvis forespørgslen bliver afvist, må du selvfølgelig ikke gennemføre transaktionen. Hvis forespørgslen bliver godkendt, betyder det, at kortet ikke er spærret. Du skal stadig foretage de sikkerhedsforanstaltninger, vi har beskrevet i dette dokument.

Husk at kontrolcifre aldrig må opbevares, og du skal derfor få slettet kontrolcifre, modtaget ved kortholders bestilling, når kortbetalingen er kontrolleret. Ved senere levering, delleverancer og abonnemeter bliver kontrolcifre kun medsendt ved første forespørgsel. Se mere information i Brugervejledning for Dankort under punkt 4.

Kontrolforespørgsel på eDankort

Ved eDankort bliver kunden og betalingstransaktionen godkendt i kortholders netbank. Det betyder, at du ikke risikerer indsigelser om tredjemandsmisbrug, og at du har en betalingsgaranti på 4.000 kr. for en eDankort-transaktion. Ved eDankort har du 31 kalenderdage til at levere varen og indsende betalingstransaktionen til Teller.

Husk, at du skal kunne levere dokumentation for ordren, herunder at kunden har modtaget varen.

