Gode råd

Forebyg misbrug med Dankort i din webshop

Den digitale centervagt

I de fysiske forretninger har man overvågningskameraer, butiksdetektiver, centervagter, alarmer ved ind- og udgang, og et personale der holder øje med mistænkelig/anderledes kundeadfærd.

På samme måde, bør I tænke det ind i håndteringen af jeres webordrer.

Hvilke tegn på misbrug kan du holde øje med?
Det kan være vanskeligt at opstille konkrete retningslinjer for, hvordan man udpeger og håndterer mistænkelige ordrer, da det afhænger af varekategori, kundetype mm. Her er dog nogle retningslinjer, som er gode at have for øje, men I kan tilpasse dem til præcis jeres webshop.

Udgangspunktet er: Sammenlign ordrene med de normale salg i din webshop.

Ordrer, der adskiller sig fra denne norm KAN være det første tegn på svindel.
Så når I skal vurdere en ordres troværdighed, skal I blandt andet holde den op imod jeres sædvanlige salg.

- Hvordan og på hvilke tidspunkter handler jeres kunder typisk?
- Hvilke varer bliver normalt lagt i samme kurv?
- Hvilken adfærd har jeres kunder sædvanligvis?

Varen

Tegn på misbrug kan fx være i forhold til, hvilken vare købet drejer sig om.

- Er det varer i den dyre ende af jeres sortiment?
- Er ordren meget større end jeres sædvanlige ordrer?
- Er det varer, som man let kan omsætte til rede penge?
- Er varesammensætningen usædvanlig?
- Har du indtryk af, at varerne er smidt hurtigt i kurven?
- Er I konkurrencedygtige på prisen?
- Vil man normalt kontakte jer inden køb?
- Hvis I taler med 'kunden', ved han/hun så noget om det produkt, som han/hun har bestilt?
- Hvis I taler med 'kunden', lyder han/hun uventet forvirret?
- Hvis ordren er bestilt fra udlandet: Ville man kunne købe varen billigere dér?

Kunden og kundeinformationerne

I kan også kigge på kunden og kundeinformationerne.
Igen er tommelfingerreglen: Kunder, der adskiller sig fra normen, KAN være tegn på svindel.
Så hvordan ser jeres sædvanlige kunde ud?

- Er der mange ordrer til samme kunde over relativ kort periode?
- Er der flere ordrer med fx samme telefonnummer, men forskelligt navn eller samme navn og forskellig adresse?
- IP-adresse og/eller leveringsadresse i forskellige lande?
- Er der anvendt anonyme ikke-sporbare kundeoplysninger fx taletidskort, gratis/anonyme mailkonti mm.
- Er det en hasteordre?
  Hvis man bruger stjålne kortoplysninger, er man ligeglad med ekstra forsendelses-omkostninger. Kriminelle ringer ofte for at få jer til at sende ordren hurtigt (inden den rigtige kortholder får sit kort spærret).
- Hvis I taler med 'kunden', stemmer hans oplysninger så med oplysningerne i ordren?
- Risikable adresser kan fx være områder, som I har dårlige erfaringer med, adresser i udlandet, på hoteller, c/o-adresser, sommerhuse, fabriksbygninger, postbokse ....

Meget af det, der er med til at få en ordre til at virke mistænkelig er ikke nødvendigvis alarmerende i sig selv.

Der er sikkert mange af jeres rigtige kunder, der har anonyme mailkonti eller taletidskort. Men jo flere af disse advarselslamper, der bliver tændt, jo større risiko er der ved ordren.

Brug sund fornuft ved vurderingen af ordrer - og vær ikke alt for optimistisk.

Vi anbefaler

- Lad misbrugsbekæmpelse få høj prioritet i jeres forretning og etablér en fast kontrolprocedure som en del af jeres ordrehåndtering.
- Definer, hvad der gør ordrer bemærkelsesværdige og hav fokus på at uddanne jeres personale, så alle ved, hvornår en ordre skal gennem en ekstra kontrol, og hvordan denne kontrol skal udføres.
- Det bør være tydeligt i jeres virksomhed, hvem der har ansvar for at afsløre og anmelde svindel samt processen herfor.
- Det optimale er at have nogle få medarbejdere, der står for vurderingen af ordrerne.
- Opsæt en politik for hvor mange og hvor store ordrer, I vil lade gå igennem på ét kort; hvor mange ordrer til samme person/samme kort/samme område vil I godtage?
- Fokusér især på risikable ordrer. Hvis I allerede har haft misbrug, så lav en analyse af, hvordan jeres normale ordrer adskiller sig fra misbrugs-ordrerne.
- Hvis I har få ordrer om dagen, kan screeningen gøres manuelt, ellers findes systemer, der automatisk flagger risikable ordrer, så I kan tage dem ud til ekstra kontrol.
- I kan eventuelt differentiere mellem nye kunder og eksisterende kunder ved at bruge kundens købshistorik og så sætte andre parametre op for nye kunder.
- Det er ofte muligt at få ekstra information fra jeres betalingsmodul fx om IP-adresser, afviste transaktioner mm.
  Flere betalingsmoduler tilbyder også at sende såkaldte 'fraud alerts' eller tilbyder deciderede fraud-moduler. Efterspørg disse services hos leverandøren af dit betalingsmodul.
- Specielt afviste transaktioner er interessante. Hvis fx et køb først er afvist på to forskellige Dankort og så går igennem på det tredje, er der stor risiko for svindel. Det er de færreste, der har adskillige Dankort, og blot tager det næste, når det første ikke virker.
- Det er bedre at forhindre misbrug end bagefter at skulle håndtere det. Det betyder, at I bør overveje, om I i tristrækkelig grad har både personale og processer på plads til at undgå, at svindlen får lov at finde sted.

Hvad er jeres parametre? Hvornår tager I en ordre ud til ekstra kontrol?

Révurder jævnligt de parametre, I har sat op. Er de stadig retvisende? Brug eventuelle chargebacks til at præcisere, hvordan misbrugsordrer adskiller sig fra de rigtige ordrer.

Opslag og kontroller

Lav tjekliste for håndtering af risikable ordrer, der eksempelvis kunne omfatte følgende opslag og kontroller:

- Er telefonnummeret relateret til kunden/adressen? Kontroller det oplyste nummer fx via 118.dk/Krak/De gule sider eller lignende services
- Er kunden registreret på den oplyste adresse? Kontroller begge adresser, hvis der er forskel på faktura- og forsendelsesadressen
- Ring fx til det telefonnummer, der er registreret på adressen (Hvis der er tale om misbrug, og I ringer til det oplyste nummer, får I netop fat i svindleren, og han vil selvfølgelig sige, at alt er OK)
- Sammenlign både navn, telefonnummer, adresse, e-mail, IP-adresse mm. Spørg evt jeres betalingsmodul efter oplysning om IP-adresser på jeres ordrer.

Hvem undersøger disse ting, og hvad gør vedkommende, hvis det ser mistænkeligt ud?

Brug sund fornuft ved vurdering af ordrer. Virker ordrer og oplysninger rimelige og forventelige, eller afviger de fra normen? Hvis noget virker usædvanligt eller underligt, er der god grund til at foretage grundige ekstra kontroller.

Hvad gør I nu, hvis I alligevel er i tvivl?

Det er jeres forretning, og I bestemmer selv, om I ønsker at annulere salget!

I kan afvise ordren eller eventuelt bede om yderligere dokumentation for, at kunden er dén, han giver sig ud for. Reelle købere bliver som regel ikke stødte over denne ekstra sikkerhed, idet de godt ved, at der finder svindel sted på nettet.

Hvis I stadig er i tvivl, efter at I har gennemgået alle de interne undersøgelser, kan I kontakte Dankort Fraud Management på tlf. 7211 2044. Vi kan som regel ikke give jer et entydigt svar på, om der er tale om svindel, men vi kan eventuelt se, om kortet er spærret.

Men vurderingen af ordrer er jeres ansvar, så opfat det ikke som en del af jeres faste kontrol-procedure, at I skal ringe til os.

Bemærk: Vi har IKKE lov at verificere kundens navn og adresse.