FORBRUKERRÅDET

DU SELGER DEG BILLIG

En rapport om betalingsløsninger og personvern

INNHOLD

1 | OPPSUMMERING

Forbrukerrådet har valgt å se nærmere på forbruker-utfordringer knyttet til nye og moderne betalings-tjenester. Rapporten gir et øyeblikksbilde av dagens betalingsløsninger, utbredelse og marked, samt en beskrivelse av betalingsløsninger vi kan forvente vil bli lansert i løpet av nærmeste fremtid.

Det er gjennom arbeidet med rapporten funnet områder som bør vies ekstra oppmerksomhet. Det viktigste er at bransjen i stor grad er selvregulert uten noen form for offentlig tilsyn. Det andre er at bransjen setter grensene for personvern og forbrukerinteresser under press.

Betalingstjenester er et vidt begrep, men avgrenses i denne rapporten til å omhandle moderne fysiske og virtuelle betalingstjenester benyttet i handel mellom forbruker og forretning.

Internettets nye valuta er personopplysninger. Men få forbrukere ser i dag verdien av egne data – og de får en heller liten del av verdiene disse dataene utgjør.

Det er nærmest umulig for forbrukerne å få tilgang til den informasjonen varehandelen og andre lagrer om dem. Like vanskelig er det å få disse data-ene slettet. Forbrukerrådet ønsker løsninger som sikrer at forbrukerne får mer kontroll og eierskap over egne opplysninger og hvordan disse skal kunne benyttes av andre.

I Norge er det strenge krav til bruk og lagring av personopplysninger. Dette byr på utfordringer etter hvert som flere utenlandske selskaper satser i det norske markedet.

I rapporten benyttes en del faguttrykk som er forklart i siste kapittel.

Den nye valutaen

Personopplysninger blir omtalt som internettets nye valuta. Når forbruker-informasjon har blitt et produkt, er det på tide at forbrukerne tar seg «betalt» også.

Hvorfor krever for eksempel en lommelykt-app tilgang til telefonens identitet, lokasjon og internett-tilkobling? Hvorfor må en bank-app ha tilgang til kontakt-listen, lokasjon, kamera, osv.?

I mange tilfeller vil det være slik at forbrukerne betaler med sine personopp-lysninger som så igjen benyttes for å generere inntekter på en måte som forbruker er uvitende om eller ikke ønsker.

Forbrukerne skal ha kontroll - eierskap til egne personopplysninger

Informasjonen betalingstjenesteleverandører og varehandelen besitter, kan og blir forsøkt koblet sammen med andre digitale spor forbrukere etterlater seg for å vite enda mer om vår adferd for så å markedsføre produkter og tjenester som datafangsten forteller at vi er interessert i. Enkelte aktører selger innhentede personopplysninger til for eksempel analyseselskaper og mar-kedsførere.

Forbrukerrådet ønsker løsninger som sikrer at forbrukerne får mer kontroll og eierskap over egne opplysninger. For å oppnå det må forbrukere bli informert om hvem som får tilgang til hvilken informasjon og mulighet til å reservere seg for videreformidling og bruk av personinformasjon.

Gjør personvernet tydelig - salgsbetingelser

I takt med at vi endrer måten vi betaler på, samt at nye betalings-løsninger er konstruert for å samle inn mest mulig informasjon om forbruker, kreves det nytenkning hva gjelder innhold i, presentasjon av og samtykke til salgsbetingelsene.

1 http://www.datatilsynet.no/Global/04_analyser_utredninger/2013/Internettsveipet%202013.pdf

Bruken av personopplysninger er en særskilt viktig del av salgsbetingelsene, og det er alarmerende at fire av ti norske nettbutikker mangler personvernerklæring[1]. Forbrukerrådet mener bruken av personopplysninger skal være skilt ut i en egen personvernpolicy hvor forbruker kan velge aktivt å samtykke til at brukersted kan benytte personopplysningene etter at de har gjennomført sine forpliktelser overfor forbruker

Norsk lov bør gjelde - aktører utenfor norsk regulering

Stadig flere globale nettbutikker etablerer seg i Norge eller fremstår som norske overfor forbrukerne. Så fremt aktørene fremstår som norske, så bør de følge norsk lov. Vi har under arbeidet med rapporten identifisert konkrete foretak som uttaler at de følger personopplysningsloven, men da med referanse til lovgivningen i landet hvor de har sitt organisasjonsnummer og ikke den strengere, norske lovgivningen.

Som følge av de norske bankenes krav til sikkerhet og autentiseringsmetode samt manglende evne til innovasjon, vil utenlandske betalingstjenesteleverandører trolig fortsette å kapre markedsandeler innen den virtuelle delen av betalingstjenesteområdet. Da er det viktig for Forbrukerrådet at disse følger norsk lov.

Gode produkter til forbrukerne - innovasjon på betalingstjenesteområdet

I Norge er BankAxept er den dominerende betalingsmetoden med en markedsandel på 88,2 prosent[2]. Det er en effektiv betalingsløsning som gir brukersteder svært lave kostnader sammenlignet med de internasjonale kortsystemene. De internasjonale kortsystemene har lagt opp til en forretningsmodell hvor kortinnløser godskriver kortholders bank med et formidlingsgebyr kalt «interchange». For å tjene på transaksjonene må kortinnløser kreve et høyere beløp fra brukersted enn de selv betaler til kortutsteder. Denne forretningsmodellen gjør at brukerstedene må betale anslagsvis 50 ganger mer for transaksjoner utført med Visa eller MasterCard enn med BankAxept. Dette er kostnader som igjen veltes over på kundene i form av økte enhetspriser.

Den lave inntjeningen på BankAxept fører til en økende interesse for bankene til å utstede internasjonale betalingskort som gir bankene større inntekter, men høyere kostnader for forbrukere og butikker. Bankenes lave inntjening på BankAxept antas å være en av årsakene til at produktet ikke videreutvikles.

Bankene har besluttet at de vil forretningsorientere BankAxept og oppretter selskapet NyBax AS. Selskapet som vil bli eid av bankene skal videreutvikle tjenester basert på BankAxept-infrastrukturen, som løpende tilfredsstiller markedets etterspørsel etter anvendelige, sikre og rasjonelle betalingsløsninger[3].

Det finnes ingen garanti for at bankene reelt kommer til å fornye BankAxept eller om produktet fases ut til fordel for de internasjonale kortløsningene. EU kommisjonens forslag til revisjon av betalingstjenestedirektivet, det såkalte PSD2[4], bidrar til ytterligere bekymring for fremtiden til BankAxept. Det foreslås blant annet å innføre forbud mot automatiske mekanismer som begrenser kortholders valg av korttype i kjøpsøyeblikket. Dette betyr at den såkalte "prioriteringsregelen" står for fall og kortholder må selv velge betalingsform i terminalen. Prioriteringsregelen som finnes i alle norske betalingsterminaler fungerer slik at terminalen prioriterer BankAxept i kombinerte kort. Om forslaget går gjennom, vil konsekvensene trolig bli økt bruk av internasjonale betalingskort og dermed økte enhetspriser for forbruker som følge av at butikkene må betale langt mer i brukerstedsprovisjon.

Forbrukerrådet mener bankene bør prioritere produktinnovasjon på betalingstjenesteområdet og kommer derfor til å følge utviklingen for å sikre at forbrukeres interesser ivaretas i denne prosessen.

[2] http://www.fno.no/PageFiles/50660/Eldar%20Skjetne%20-%20SpareBank%201%20Gruppen%20AS%20-%20BankAxept%20ny%20strategi%20og%20ny%20giv.pdf

[3] http://sparebankforeningen.no/asset/5085/1/5085_1.pdf

[4] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0547:FIN:EN:PDF

2 | BAKGRUNN

I løpet av det siste tiåret har det skjedd til dels store endringer innen betalingstjenesteområdet, både hva gjelder handlemønster, salgskanaler, betalingsmetoder og sikkerhet.

De største endringene finner vi innen e-handel og mobilhandel, men utviklingen av nye betalingstjenester begynner nå å røre på seg også innen varehandel i fysisk butikk. Konkurransesituasjonen på tilbydersiden av både teknologi og finansielle tjenester til varehandelen, har også endret seg som følge av at det stadig tilkommer nye aktører som ønsker å etablere seg i verdikjeden.

Endringene har bidratt til at betalingsløsningene er blitt langt sikrere. Primært som følge av innføringen av chip & PIN i fysisk varehandel og at bruk av 3D Secure i norske nettbutikker har blitt mer eller mindre standard. Innføringen av PCI DSS standarden (lagring av kortdata) som kortselskapene står bak, har også bidratt til at sensitiv kortinformasjon nå er langt bedre beskyttet enn tidligere.

Selv om vi altså har sett en del endringer innen området for betalingstjenester, er ikke disse så betydelige som bransje- og teknologieksperter har spådd. Leverandørsiden har vært for optimistiske hva gjelder brukerstеders vilje til å investere i ny teknologi, samt forbrukers vilje til å ta til seg betalingsløsninger som krever endring i handlemønstre. Produktutviklingen har vært teknologidrevet og da er det viktig å huske at Norge er et lite land som betyr at nye betalingsløsninger må kunne brukes av «alle» forbrukere for at det skal være interessant å investere fra brukerstedssiden. Det betyr at det vil være de store etablerte aktørene som vil ha de beste forutsetningene for å lykkes i å rulle ut breddeløsninger.

Vi er i startgropen på en tid hvor den teknologiske utviklingen forventes å gå raskt. Wilhelm Wisbech i Visa Europe uttaler at de forventer at halvparten av kjøp med Visa-kort vil bli foretatt mobilt innen 2020, teknologi som eksempelvis kontaktløs betaling er på vei, betalingsløsninger som samler inn detaljert informasjon om forbruker utvikles og apper som inkluderer betalingstjenester og nettbank har allerede blitt utbredt. Ettersom teknologien fornyes og blir mer avansert, blir også de kriminelle mer teknologisk bevisste. Når stadig flere betalingstjenester flyttes over på mobiltelefonen, blir det viktig at tjenestene sikres tilstrekkelig. Innbrudd og svindel via mobile enheter vil bli et satsningsområde for kriminelle i takt med økende utbredelse.

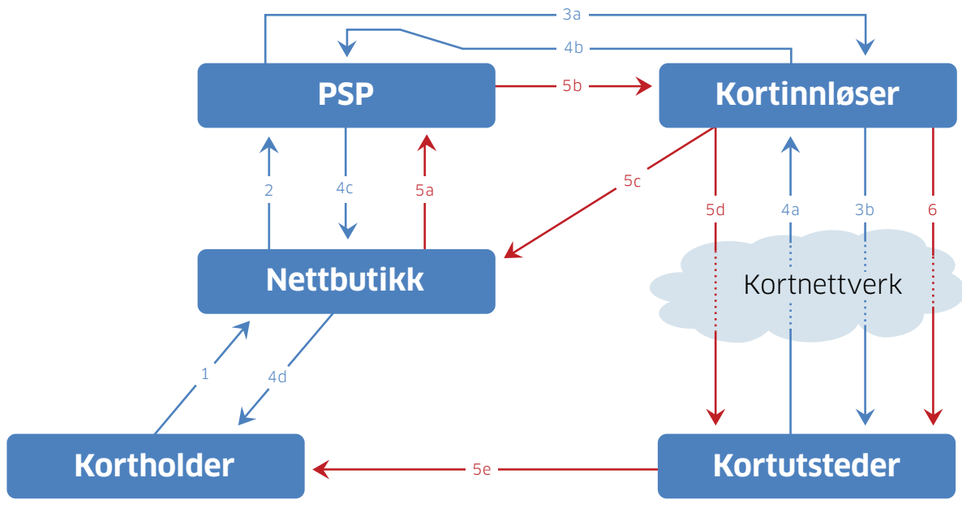
At vi nå står overfor store endringer på produktsiden gjør det viktig at det siktes inn mot sikkerhet i de nye løsningene. Det kan virke som om Finanstilsynet til dels deler Forbrukerrådets bekymringer for forbrukersikkerheten, men det savnes proaktivitet og mer aktivt tilsyn. Om forbrukernes handlemønster og betalingsløsninger til en hver tid er statiske, er det greit å benytte foregående års svindelstatistikk som styringsverktøy for hvordan regelverket skal forvaltes og hvilke sikkerhet som skal gjelde. Men nå rulles det ut nye løsninger, og da er det viktig at det tidlig legges et godt fundament for disse og kommende løsninger hva gjelder både transaksjonssikkerhet og personvern. Her er det viktig at bransjen selv også får en mer proaktiv holdning. Det kan virke som om mange har glemt utfordringene bransjen opplevde når e-handelen begynte å ta av i Norge. Da hadde man den samme tilnærming, og de finansielle aktørene hadde et svare strev med å håndtere all svindelen som oppstod.

Forbrukerne har stor tillit til den norske forbrukerlovgivningen. I følge EU kommisjonens «The Consumer Conditions Scoreboard», svarer 73 prosent at de stoler på at offentlige myndigheter beskytters deres forbrukerrettigheter mot et snitt på 59 prosent blant EU landene.[5] Mer bekymringsverdig er det at samme rapport viser at norske forbrukeres tillit til at varehandelen respekterer deres rettigheter har falt fra 70 til 58 prosent fra 2011 til 2012. Det er under gjennomsnittet i EU-landene.

[5] http://ec.europa.eu/consumers/consumer_research/editions/docs/7th_edition_scoreboard_en.pdf

3 | VERDIKJEDEN OG AKTØRENE

Ved kortbetaling i nettbutikk ser verdikjeden slik ut:



Autorisasjon

Kapital

Prosedyren ved handel er:

1. Kortholder legger sine varer i handlevognen og går til check-out for betaling.

2. Når betalingsform er valgt, presenteres kunde for en betalingsside som skal hostes av en sertifisert PSP (Payments Service Provider). En nettbutikk har ikke lov til å komme i kontakt med sensitiv kort-

informasjon uten å være PCI sertifisert, noe de færreste nettbutikker er. I Norge er det Nets, PayEx, Klarna og DIBS som dominerer PSP markedet.

3. Når kortnummer, utløpsdato og kontrollsiffer er tastet inn sendes det en autorisasjonsforespørsel via PSP, kortinnløser og kortnettverk til kortutstedende bank. Før kortutsteder svarer på autorisasjonen, vil kortholder i de aller fleste tilfeller bli bedt om å foreta en autentisering. Sikkerhetsløsningen heter 3D Secure og autentiseringen gjennomføres i de fleste tilfeller med bruk av Bank ID.

4. Etter autentisering utfører kortutstedende bank div. sjekker som saldo, om kort er sperret osv. Om alt er i orden gir kortutseder en positiv respons som sendes samme vei tilbake og kortholder skal umiddelbart få en bekreftelse på godkjent kjøp.

5. Ved godkjent autorisasjon reserveres kjøpsbeløpet på kortholders konto. Når varene sendes fra nettbutikk, sendes det en kommando til PSP som resulterer i at kortinnløser oppdaterer reskontroen til nettbutikk og utbetaler oppgjør i henhold til avtale, samt sørger for at kortholders autorisasjon erstattes med et reelt trekk. Teller, Elavon, Nordea og Swedbank er de største kortinnløserne i det norske markedet.

6. Kortinnløser utbetaler interchange/ formidlingsgebyr til kortutsteder.

Ved betaling i fysisk butikk er dataflyten mer eller mindre den samme. Hovedforskjellen er at BankAxept ikke inkluderer formidlingsgebyr og det er brukerstedets bank som er kortinnløser.

4 | NYE FORBRUKERE

Om ikke betalingstjenestene har endret seg drastisk i løpet av de siste årene, har definitivt forbrukerne endret seg. De kan nesten omtales som en ny generasjon forbrukere. De er kunnskapsrike, tar raskt til seg mulighetene ny teknologi gir og de forventer en sikker og enhetlig kundeopplevelse uavhengig av salgskanal.

Dette er en trend som endrer måten brukersteder tilnærmer seg kundene på, både før og etter handelen er gjennomført. Dette er både en mulighet og en trussel for brukerstedene. Evnen til raskt å endre seg vil være avgjørende. Når brukerstedene vil forsterke båndene med sine kunder ved å benytte de digitale sporene forbrukerne legger igjen etter seg, er det viktig at dette gjøres på en måte som ikke går ut over personvernet.

Ole Petter Nyhaug fra Onlive Research påpekte på Forbrukerrådets betalingskonferanse i november 2013, at de nye og yngre forbrukerne må forstås som en risikoreduserende gruppe forbrukere som er opptatt av forebygging og de søker trygghet og kontroll. Dette betyr at varehandelen og betalingsløsningene må oppleves som sikre og forbrukeren må få god informasjon tidlig i kjøpsprosessen. Forbrukerne er skeptiske i utgangspunktet og da er veien kort til at forbruker avbryter kjøpet om betingelsene er uklare eller om fraktomkostninger og andre kostnader først fremkommer helt til slutt i kjøpsprosessen. Den nye generasjonen forbrukere har også et forenklingsbehov hvor sømløshet er sentralt. De ønsker det skal være enkelt å betale på nett og man forventer å kunne «betale der du er nå». Vi ser i dag hvordan nettbutikker forsøker å forenkle kjøpsprosessen ved eksempelvis å lagre kundens kortnummer via sin PSP slik at kunden slipper å taste inn dette neste gang hun skal handle i nettbutikken. Andre butikker kutter ut bruken av sikkerhetsløsningen 3D Secure.

Mobilhandel

I følge DIBS e-handelsindeks har 61 prosent av oss smarttelefon eller nettbrett, og 18 prosent svarer at de har handlet på internett med enten brett eller smarttelefon de siste 12 måneder. Det er forbrukere mellom 18 og 34 år som benytter mobilhandel aller mest, og av disse handler 29 prosent mobilt. På samme måte som ved «ordinær» netthandel, er det reiser og billetter som utgjør den største delen av omsetningen men film og musikk er også betydelige varegrupper via denne kanalen. Det blir handlet varer og tjenester over et bredt spekter fra smarttelefon og nettbrett. En av grunnene er at de forbrukerne som har nettbrett i stor utstrekning bruker dette hjemme som en PC. Det må antas at vi etter hvert vil se tydelig mønstre av typiske varegrupper i de forskjellige kanalene. Smarttelefon er en god salgskanal for reisetjenester og billetter og selvsagt også for digitalt innhold som musikk og spill. For mange andre varegrupper vil nettbrettet være en bedre mobil salgskanal. Selv om handelen med enkelte varegrupper vil være mindre effektiv på mobile enheter med små skjermer, vil mobilen være en viktig kommunikasjons- og markedsføringskanal.

E-handel

E-handelen har opplevd solid vekst de siste årene og alt tilsier at e-handelen bare vil fortsette å vokse. Forbrukerne sier at de forventer å handle mer på nett og nettbutikkene sier de forventer å selge mer. Dette til tross for at vi allerede er den nasjonen i Europa som handler for aller mest per bruker. I følge e-handelsindekset til DIBS, estimeres e-handelsmarkedet i 2013 til 60,3 milliarder kroner som er en vekst på 17 prosent fra 2012. Dette vil si at en typisk nettbruker handler for ca. 18 000,- per år fordelt på 17 kjøp. I følge Distansehandel Norge og Posten Norge sitt netthandelsbarometer, har fysisk handel i butikk kun økt med 1,2 prosent de første månedene i 2013.

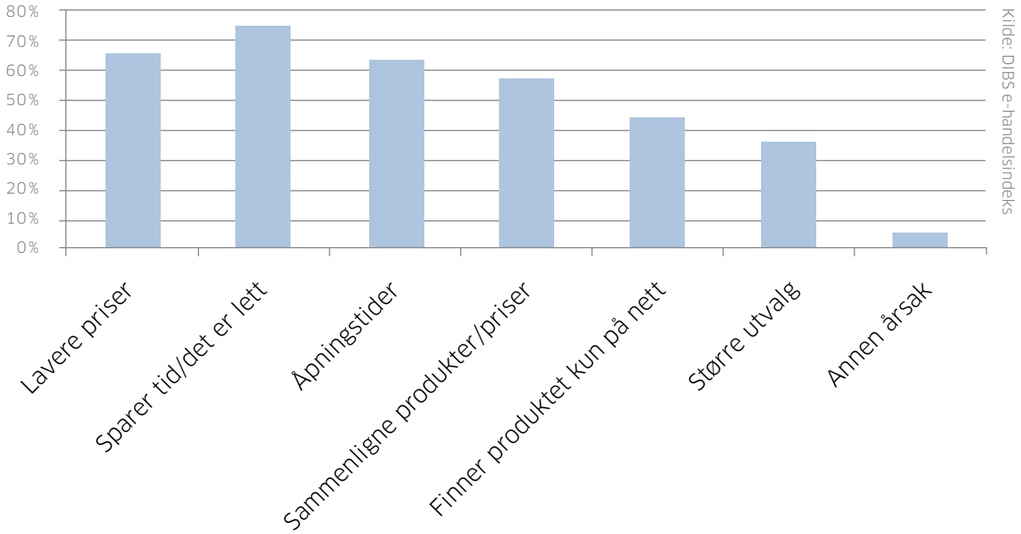
Grensene mellom e-handel og fysisk handel synes å bli mer uklare. Eksempelvis gjør Elkjøp stor suksess med sitt døgnåpne lager. Forbrukere kan dermed bestille varer på nett og hente de når de måtte ønske uten å tenke på åpningstider. Denne trenden vil vi nok se mer og mer av innen flere segmenter. Blant annet dagligvarebransjen ser ut til å ha store forventninger til denne metoden å selge på.

Selve den tekniske sikkerheten i løsningene må sies å ha blitt god. Innføringen av sikkerhetsstandarden PCI DSS (Payment Card Industry Data Security) som de internasjonale kortselskapene står bak, har gjort at sensitiv kortinformasjon nå er langt bedre beskyttet enn tidligere. PCI DSS er utarbeidet for å sikre at ingen uvedkommende skal få tilgang til kortdata. Å bli PCI DSS sertifisert er en tidkrevende og dyr prosess og det er ingen ordinære norske nettbutikker som har gjennomført en slik sertifisering.

Det finnes ingen statistikk som forteller noe om antallet norske nettbutikker som har en eller annen form for betalingsløsning, men et estimat vil være ca. 9 000 og det tilkommer ca. 1 500 nye per år mens 1000 blir lagt ned.

Når forbrukerne ble spurt hvorfor de handler på nett, svarte de slik:

Forbrukernes motivasjon for å handle på nett



Kilde: DIBS e-handelsindeks

Tidligere har lignende undersøkelser vist at viktigste årsak for å handle på nett har vært lave priser. Dette har endret seg, og nå er det hovedsakelig bekvemmelighet og enkelhet som er de største driverne for å handle online. Forbrukerne ønsker at kjøpsprosessen skal være oversiktlig, enkel og sikker. Her er tydelige salgsbetingelser og tydelig prising viktige elementer som mange nettbutikker fortsatt slurver med.

5 | PERSONVERN OG FORBRUKERINTERESSER

En stor andel forbrukere virker ukritiske til å legge igjen personlig informasjon på internett. Mange er nok heller ikke klar over hvordan informasjonen de legger igjen blir benyttet videre. Lav oppmerksomhet på eget personvern blant forbrukere, gjør at det hviler desto større ansvar på de kommersielle aktørene i verdikjeden.

Det må rettes søkelys på at nye og eksisterende betalingstjenester ivaretar personvernet på en god måte, at varehandelen tydelig informerer forbrukerne om hvordan de vil benytte informasjonen og at bruken av personopplysninger i større grad enn i dag baseres på aktivt samtykke. Det må også gjøres mulig for forbrukerne å gjennomføre en handel uten at butikken nødvendigvis skal benytte personinformasjonen etter at butikken har gjennomført sine forpliktelser overfor forbruker.

Når vi surfer på nett og handler i butikker legger vi igjen en rekke spor, og vi ser at butikker i økende grad benytter denne informasjonen i salg- og markedsføringsøyemed. I fysiske butikker har vi eksempelvis lojalitetsprogrammer hvor hva vi kjøper blir logget. På nett mottar vi tilbud og informasjon som tydelig tar utgangspunkt i digitale spor vi har lagt igjen. Vi må forvente at brukerstedene i langt større grad enn i dag vil bruke informasjon de sitter på om sine kunder på en mer «sofistikert» og aggressiv måte. Informasjonen de sitter med kan kobles sammen med andre digitale spor forbrukere etterlater seg for å få vite enda mer om vår adferd for så markedsføre produkter og tjenester som datafangsten forteller at vi er interessert i. Enkelte aktører selger også personopplysninger de sitter på til for eksempel analyseselskaper og markedsførere hvor personopplysninger er attraktive.

Forsker Petter Bae Brandtzæg ved SINTEF mener vi nærmer oss et samfunn hvor butikkvinduet forbruker passerer, skriker til deg: «Petter, vi har en skjorte her som passer deg perfekt!». Dette fordi forbrukers lokasjonsdata i stadig større grad kan kobles mot dine personlige preferansedata, noe for eksempel Facebook har kommet langt med.

Personopplysninger blir omtalt som internettets nye valuta. Få forbrukere ser i dag verdien av egne data og de får liten del av den verdien disse dataene utgjør. Når forbrukerinformasjon har blitt et personprodukt, er det på tide at forbrukerne også tar seg «betalt». Det er nærmest umulig for forbruker å få tilgang til informasjonen varehandelen og andre lagrer om dem og det samme gjelder sletting av data. Forbrukerrådet ønsker løsninger som sikrer at forbrukerne får mer kontroll og eierskap over egne opplysninger og hvordan disse skal kunne benyttes av andre.

5.1 | Betalingsløsninger utenfor norsk regulering

I Norge er det strenge krav for bruk av personopplysninger. Dette byr på utfordringer etter hvert som flere utenlandske selskaper satser i det norske markedet. Eksempler på leverandører av betalingsløsninger utenfor norsk regulering er PayPal og Klarna.

Svenske Klarna tilbyr betalingsløsninger til nettbutikker som gjør at forbruker kan betale med faktura i tillegg til betalingskort. Måten Klarna benytter fødselsnummer i sin løsning strider mot den norske personopplysningsloven**.** Personopplysningsloven sier at selv om fødselsnummeret ikke regnes som sensitivt, er det klare grenser for bruken av det. Fødselsnummeret kan bare brukes når det er saklig behov for sikker identifisering av en person og fødselsnummeret er nødvendig for slik identifisering. Dette gjelder for eksempel ved betaling med faktura hvor forbrukerne kredittsjekkes, men fødselsnummeret skal ikke lagres etter at kredittsjekken er gjennomført. I administrasjon av kundeforhold og medlemskap vil det som hovedregel være tilstrekkelig å benytte navn, adresse og fødselsdato for å sikre identifisering av person.

Da skal ikke fødselsnummeret brukes. For virksomheter er det også viktig å vite at et fødselsnummer ikke er legitimasjon[6]. Klarna benytter derimot fødselsnummer som kundeidentifikasjon og de lagrer også fødselsnummer slik at forbruker på www.klarna.no kan søke opp sine fakturaer basert på sitt fødselsnummer.

Klarna skriver følgende på sine sider: «Personopplysninger behandles i henhold til personopplysningsloven. Klarna håndterer personopplysninger for å utføre kundeanalyser, identifikasjoner, kredittvurderinger og markedsføring. Ditt personnummer er også ditt kundenummer hos Klarna». [7] I sine vilkår skriver de videre: «Norsk lov gjelder og eventuelle tvister skal avgjøres ved norske domstoler».[8] Faktum er at Klarna ikke følger personopplysningsloven, men mulig følger de den svenske personuppgiftslagen.

Svenske CDON har tidligere fått kritikk av Datatilsynet for sin bruk og lagring av fødselsnummer. Det ene punktet gikk på at de i en periode krevde fødselsnummer når kunde ønsket å avslutte sitt kundeforhold. Her har CDON endret sine prosedyrer. Det andre gikk på at de krever at kunde registrerer fødselsnummer ved opprettelse av kundeprofil. De sier at de trenger dette om kunde på et eller annet tidspunkt vil benytte seg av fakturabetalinger via Klarna og vil ikke endre på dette[9]. Norske nettbutikker som benytter Klarna, følger derimot personopplysningsloven og krever kun at fødselsnummer oppgis i kjøpsøyeblikket og informasjonen lagres ikke av butikken.

5.2 | Uklare betingelser om bruk av personopplysninger

Norske forbrukere er lite flinke til å lese gjennom salgsbetingelsene i nettbutikkene. I følge Europa kommisjonens «Special Eurobarometer 342» ligger vi helt på bunn.[10] Kun 23 prosent sier de leser betingelsene nøye, 32 prosent leser noe, mens 43 prosent leser de ikke i det hele tatt. 47 prosent av de spurte svarte at de dropper å lese betingelsene fordi de inneholder for mye tekst og tar lang tid å lese, 16 prosent svarer at de må jo akseptere betingel-

[6] http://www.datatilsynet.no/Sikkerhet-internkontroll/Fodselsnummer/

[7] https://cdn.klarna.com/1.0/shared/content/legal/terms/EID/nb_no/invoice?fee=0

[8] https://cdn.klarna.com/1.0/shared/content/legal/nb_no/account/terms.pdf

[9] http://www.dinside.no/832710/se-hva-du-maa-gjore-for-aa-melde-deg-ut

[10] http://ec.europa.eu/consumers/consumer_empowerment/docs/report_eurobarometer_342_en.pdf

sene uansett og 15 prosent svarer at skriftstørrelsen er for liten. Dette betyr at det er viktig at det gjøres et arbeid med å tenke nytt både hva gjelder innhold, hvordan innholdet presenteres samt metode for samtykke.

I salgsbetingelsene som forbrukere må godkjenne når de handler i en nettbutikk, skilles det ikke på det som går på «ordinære» salgsbetingelser og det som er relatert til bruk av personopplysninger. Her er et eksempel på hvordan CDON, en av Skandinavias største nettbutikker, beskriver hvordan de vil benytte informasjonen om forbruker:

«Ved å registrere deg og/eller bestille produkter eller tjenester samtykker du i at CDON og dets tilknyttede selskaper lagrer og bruker opplysninger om dine innkjøp samt de kontaktopplysningene du gir. Opplysningene blir lagret og brukt for at vi skal kunne oppfylle våre forpliktelser overfor deg, og for at vi bedre skal kunne tilfredsstille dine behov som kunde og gi deg bedre service, blant annet ved å gjøre nettsiden så personlig som mulig. Opplysningene blir også lagret og brukt til informasjons- og markedsføringsformål. Dette innebærer at CDON og dets tilknyttede selskaper, så sant du ikke skriftlig har motsatt deg det, kan benytte dine personopplysninger for å kontakte deg per e-post med nyhetsbrev, direkte markedsføring eller markedsundersøkelser. Du har selvsagt anledning til når som helst å informere oss skriftlig om at du ikke ønsker at dine personopplysninger skal benyttes til markedsføringsformål.»[11]

Teksten over er pakket inn i et salgsbetingelsesdokument bestående av mange sider med tekst. Det står heller ikke noe om hvilke type opplysninger som lagres. Lagres informasjon om hvilke nettsider forbruker var innom før vedkommende kom til nettbutikken, alder, kjønn, hvilke nettside forbruker går til etterpå, domenet forbruker bruker for internettilgang, IP adresse, hvor PC'en fysisk befinner seg osv.?

Det burde være en selvfølge at forbruker skal kunne få handle i butikken selv om forbruker ikke ønsker at butikk skal benytte personopplysningene etter at butikk har gjennomført sine forpliktelser. Bruken av personopplysninger anses som en særskilt viktig del av betingelsene, og bør skilles ut i en egen personvernpolicy hvor forbruker aktivt kan velge å samtykke til at brukersted kan benytte informasjonen etter at de har gjennomført sine forpliktelser. Dette vil typisk kunne være så snart angrefristen er utløpt. For å gjøre det enkelt for forbruker og se og evt. slette informasjonen butikk lagrer, bør denne informasjonen gjøres tilgjengelig for forbruker via en link som kunde kan klikke på via «Min side».

[11] http://cdon.no/kundeservice/personvern_policy/

5.3 | **Utforming og tydeliggjøring av salgsbetingelsene**

Det må tenkes nytt hva gjelder måten brukersted presenterer sine salgsbetingelser på. Salgsbetingelsesdokumentet Forbrukerombudet har utarbeidet[12], bør ligge enkelt tilgjengelig på brukerstedets hjemmeside. Fordi det er få forbrukere som leser dette, bør særlig viktig informasjon fremheves og presen-teres tidlig i kjøpsprosessen. Dette er spesielt viktig nå som mer og mer handel skjer via devicer med små skjermer.

5.4 | **Personvern i mobile applikasjoner**

I følge ABI Research laster en gjennomsnittlig smarttelefon-bruker ned 37 apper. Uavhengig om mobilapplikasjon inkluderer betalingstjenester eller ikke finnes det her en rekke utfordringer med hensyn til personvern. Hvorfor krever for eksempel en lommelykt-app tilgang til telefonens identitet, kontaktliste og internett-tilkobling? Hvorfor må en nyhets-app vite din nøyaktige lokasjon og ikke bare by eller fylke? I mange tilfeller vil det nok være slik at forbruker betaler med sine personopplysninger som benyttes for å genere inntekter på en måte som forbruker er uvitende om og gjerne ikke ønsker.

I desember 2013 kunne vi lese om lommelykt-appen Brightest Flashlight som samlet inn personopplysninger om mellom 50 millioner til 100 millioner Android-brukere og solgte disse videre til annonsører. Nordmenn har blitt rammet, men omfanget er uklart. 13

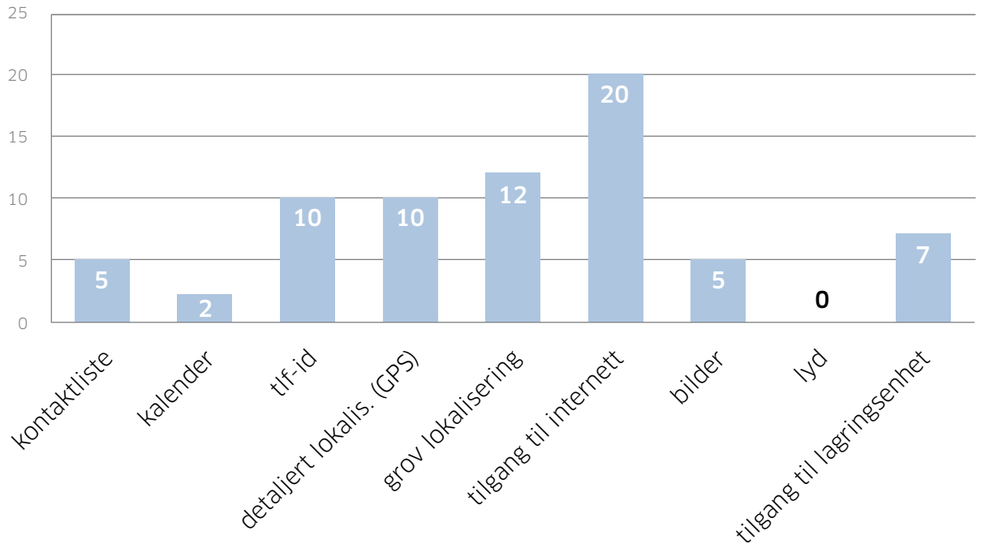
I forbindelse med Datatilsynets rapport «Hva vet appen om deg»,14 testet Datatilsynet i 2011 20 norske apper for å se hvilke informasjonselementer på telefonen som appene krever tilgang til. Tabellen under viser de mest sentrale informasjonselementene:

[12] http://forbrukerombudet.no/asset/3215/1/3215_1.pdf

[13] http://www.nrk.no/viten/lommelykt-app-samlet-inn-brukerdata-1.11402375

[14] http://www.datatilsynet.no/Global/04_veiledere/app_rapport_DT2011.pdf

Norske apper



Datatilsynet regner lokasjonsdata som en av de mest følsomme opplysningene som innhentes om oss. Ettersom mobiltelefonen er tett knyttet til eieren sin, vil lagring av telefonens bevegelsesmønster gi en svært detaljrik innsikt i privatlivet til eieren. Mobiltelefonen legger vi sjelden fra oss, og lokasjonsmønsteret som lagres om den enkelte vil derfor langt på vei være komplett.

Art 29 gruppen, som er en sammenslutning av personvernmyndigheter i EU, har publisert en egen vurdering om lokasjonstjenester på smarttelefoner. Dokumentet konkluderer med at aktører som ønsker å benytte lokasjonsdata må innhente aktivt samtykke fra brukeren.[15]

Det er vanlig å be om identifiserende opplysninger for å kunne opprette kommunikasjon med app-brukeren. Opplysninger som unikt kan identifisere brukeren har stor verdi for mange av aktørene i app-markedet. Slike opplysninger er interessante fordi de kan benyttes til mange andre innbringende formål enn det opprinnelige. For eksempel er de svært verdifulle med henblikk på å utarbeide gode profiler på kundemassen. Mange aktører vil derfor være lite interessert i å slette slike data selv om det innenfor europeisk lovgivning er det satt klare krav til håndtering av denne typen data.

[15] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_da.pdf

Applikasjonens innhenting av kontaktopplysninger på telefonen omfatter ikke bare app-brukeren selv, men også kontakter denne har registrert i sin mobiltelefon skriver Datatilsynet i sin rapport. Enkelte aktører henter ut hele kontaktlisten. Appene ber om samtykke til å gjøre dette, men det er ikke alltid lett for brukeren å få med seg at samtykke gis, eller hva samtykket i realiteten innebærer. Kontaktdata er interessant fordi det forteller noe om relasjoner. Det vil si at dataene forteller noe om brukeren og vedkommendes forhold til verden rundt seg (venner, interesser, jobb). De som står bak applikasjoner for sosiale nettsteder er spesielt interessert i denne typen data, det samme er virksomheter som driver markedsføring. Jo mer konkrete data som er tilgjengelige, særlig de som app-brukeren legger inn på selv på telefonen, jo høyere verdi.

Noen applikasjoner skriver til kalender eller henter kalenderdata. Kalenderopplysninger vil ikke bare kunne vise aktiviteter, men også fremtidig og historisk reisevirksomhet, samt relasjoner. Ved for eksempel synkronisering mot arbeidsgivers kalender, vil det være mulighet for at kalenderoppføringen også vil bli synlig for arbeidsgiver, kollegaer, samt andre aktører med tilgang til arbeidsgivers kalender, uten at brukeren nødvendigvis er klar over at dette skjer. I 2011 konkluderte Datatilsynet med følgende i rapporten «Hva vet appen om deg?»:

- App-brukeren er ikke i tilfredsstillende grad informert om hvilke opplysninger som samles inn om vedkommende, hva som er formålet med innsamlingen og hvordan opplysningene eventuelt brukes videre.
- Det fremstår som uavklart hvem som er behandlingsansvarlig for applikasjoner som behandler personopplysninger.
- App-brukerens rett til innsyn i personopplysningene som behandles er vanskelig når det ikke fremkommer hvem som håndterer personopplysningene (hvem som er behandlingsansvarlig).
- Muligheten til å legge ut informasjon om hvordan appen håndterer personopplysninger i App Store eller Android Market, benyttes sjelden. Dersom dette i større grad hadde blitt gjort ville brukeren før installasjonstidspunkt hatt et bedre grunnlag til å ta en kvalifisert beslutning om å installere appen eller ikke.

Fortsetter på neste side...

- Mulighet til å legge ut informasjon i selve appen om hvordan den håndterer personopplysninger, benyttes sjelden. Det er verdifullt å legge ut informasjon også her slik at brukeren har den lett tilgjengelig også etter at applikasjonen er lastet ned. Dersom informasjonen utelukkende ligger i selve appen, vil imidlertid brukeren først informeres etter at samtykke i forbindelse med nedlastning av appen er gitt – dette er feil rekkefølge.
- Mulighet til å legge ut informasjon om hvordan appen håndterer personopplysninger på nettsiden som app-ansvarlig råder over, benyttes sjelden. Dette er uheldig, ettersom en slik personvernerklæring ville økt tilgjengeligheten til informasjonen og fordi det ville bidratt til å synliggjøre hvem som er ansvarlig for appen. Det vil også ha klargjort hvilket lovverk (jurisdiksjon) appens håndtering av personopplysninger ligger inn under.

I media har det vært omtalt[16] hvordan norske bank-apper krever tilgang til kontaktliste, kamera, stedsangivelse, telefonlogg osv. for å fungere. Her forventer Forbrukerrådet at bankene legger om sin praksis. Det er forståelig at bankene ønsker å tilby sine kunder tilleggstjenester som kan kreve slike tilganger. Derimot så bør forbruker få tilgang til basistjenestene uten å måtte gi fra seg ovennevnte tilganger. «Sikkert som banken» er ikke lenger et gangbart uttrykk da det er mange som ikke stoler på bankene. Om forbruker ønsker å ta i bruk tilleggstjenester som for eksempel elektroniske kvitteringer som krever tilgang til kamera, skal forbruker bli informert tydelig om hvilke tilganger tjenesten trenger og hvordan tilgangene blir benytter. På denne måten kan forbruker benytte basistjenesten, og så ta et informert valg om bruk av tilleggstjenester.

[16] For eksempel Adresseavisen 29. jan 2014 «Frykter at bankene snoker».

6 | GJENTAGENDE BETALINGER/ ABONNEMENTSBETALINGER

Forretningsmodellen med gjentagende betalinger/ abonnementsbetalinger med betalingskort er utbredt. Tjenesten som hvilke som helst nettbutikk kan få tilgang til via sin PSP, ble i utgangspunktet utviklet for å håndtere nedbetaling av kostbare varer og som et alternativ til for eksempel autogiro.

I korte trekk fungerer det slik at nettbutikken via sin sertifiserte PSP oppretter tilgang til kortinformasjonen via en referanse som peker på kortnummeret som ligger trygt lagret hos PSP. Når så eksempelvis en bokklubb sender ut månedens bok, belastes kortholder uten at kortholder trenger å foreta seg noe. Dette er en grei og relativt sikker løsning, så fremt brukersted er seriøst og opptrer informativt overfor forbruker ved «avtaleinngåelse».

Løsningen kan dog enkelt misbrukes og Forbrukerrådet mottar mange henvendelser fra kunder i forbindelse med abonnementsbetalinger. Typisk har kunde handlet en vare eller tjeneste, men i kjøpsøyeblikket ikke mottatt informasjon om at man samtidig går inn i en abonnementsavtale hvor forbruker eksempelvis blir trukket for månedlige beløp. I FormLife saken mottok Forbrukerrådet klager fra over 1000 norske forbrukere som hadde blitt svindlet. Via blant annet annonser på Facebook bestilte forbrukere det de trodde var en gratis prøvepakke med slankepiller hvor de kun skulle betale frakt. FormLife registrerte så forbrukerne som abonnenter uten deres viten. Kort tid etter bestilling av prøvepakken, utførte de trekk for flere tusen kroner på «abonnentenes» Visa og MasterCard kort. Å trekke penger fra forbrukeres betalingskort uten samtykke er i strid med finansavtaleloven.

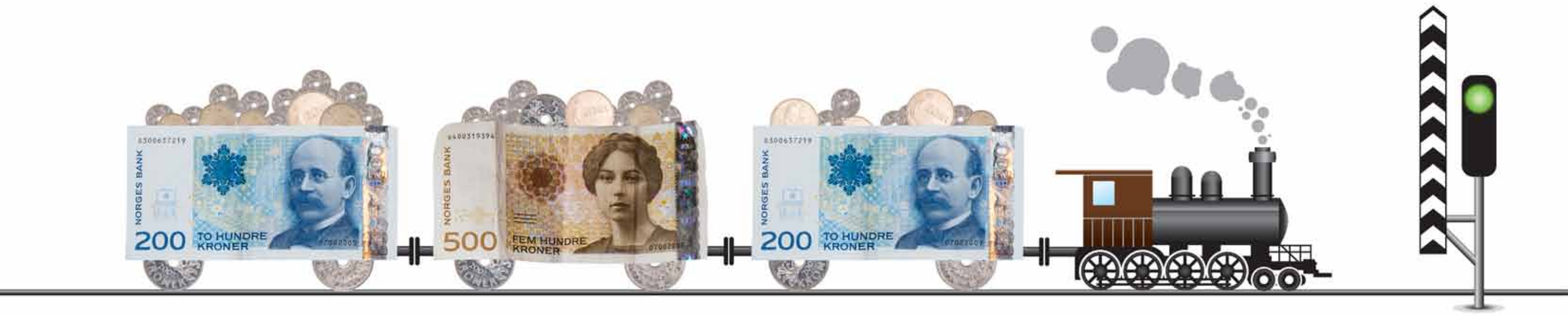
Lagring av kortnummer kommer vi til å se mer og mer til. En trend er at nettbutikk i kjøpsøyeblikket spør forbrukeren om de skal lagre kortnummeret slik at kunde slipper å ta frem kortet neste gang kunden besøker nettbutikken. På

den måten går betalingen raskere ved neste kjøp. Dette innebærer altså at det vil være svært mange nettbutikker som har tilgang til sine kunders kortinformasjon via referansen til kortnummeret. Det er nærliggende å tro at noen av de 9000 norske nettbutikkene vil utnytte muligheten de har til å øke sin egen omsetning uten kortholders viten. Det er også trolig et tidsspørsmål før vi ser flere svindlere som oppretter nettbutikker, der hele forretningsideen er å svindle på den måten vi erfarte i FormLife saken. De etablerer brukerstedsavtale med kortinnløser og en PSP, og selger så populære varer til lave priser og lagrer kortinformasjonen via PSP uten kortholders viten. Når de så har tilgang til tilstrekkelig med kortinformasjon begynner de å trekke kortholdere. Dette inntil kortinnløser mottar nok kortreklamasjoner til at de går brukerstedene i sømmene for så å lukke brukerstedsavtalen. FormLife benyttet flere kortinnløsere for innsamling av sine korttransaksjoner. Når den ene lukket deres brukerstedsavtale, inngikk de en avtale med en ny innløser. Hadde informasjonsflyten mellom kortinnløserne vært bedre enn i dag, kunne skadeomfanget av svindelen vært betydelig redusert.

I FormLife saken erfarte Forbrukerrådet at kortholderne opplevde vanskeligheter med å få sine kortutstedere til å tilbakebetale beløpene de ble svindlet for. Dette til tross for at kortselskapenes regelverk er tydelig ved slik svindel og det samme gjelder finansavtaleloven. Et relevant spørsmål er hvor godt de forskjellige kortutstederne har implementert regelverket til Visa og MasterCard. Det skal også legges til at oppgjørsgarantien til brukerstedet bortfaller ved denne typen kortbetalinger, da 3D Secure ikke benyttes. Risikoen overføres dermed fra kortutsteder til kortinnløser, noe som burde bidra til at saksgangen burde gå langt mer smidig enn det som var tilfelle i FormLife saken.

Det er viktig at kortinnløserne sikrer bedre styring på brukersteder som benytter abonnementsløsninger. Problemet er at så fremt det ikke er tekniske løsninger som sperrer for slike transaksjoner, er det bare å tegne en avtale med innløser og kjøpe tilgang til tjenesten fra en PSP. Dette kan hindres ved at kortinnløser via sitt prosesseringssenter avviser den typen transaksjoner som har til hensikt å generere den omtalte referansen som peker på kortnummeret som skal lagres. Dette kan enkelt gjøres samtidig med alle andre kontroller kortinnløser gjør via sitt prosesseringssenter når de mottar autorisasjonsforespørsler. Sjekken er så enkel som at «Er brukersted satt opp som abonnementsbrukersted? Hvis nei -> avvis».

Kortholder bør aktivt samtykke denne delen av salgsbetingelsene som går på inngåelse av abonnement og teksten bør standardiseres. Standardisering for hvordan avslutte abonnementet bør også utarbeides da mange nettbutikker gjør dette svært komplisert for abonnent og få lar sine kunder administrere sine forsendelser fra eksempelvis «Min side». Forbruker bør også kunne velge å motta en SMS/e-post i god tid fra brukersted før neste trekk vil skje hvor det er enkelt å avbestille, alternativt en SMS/e-post hvor forbruker må samtykke til at trekk skjer.



7 | BRUK OG MISBRUK AV DIGITALE SPOR

En nettbutikk kan ved hjelp av analyseverktøyer få mye ut av kundedataene sine. Det er enkelt å se hvor mange som er inne i butikken, hva det er mest aktivitet på nå, hva har økt mest siste timen, hvor forlater kundene handlevognen osv. slik at man kan få mer dynamiske og bedre tilpassede sider. Men dette kan dras så mye lengre.

Nettbutikk ønsker å gi de rette tilbudene til de rette kundene fremfor å presentere det samme innholdet til alle besøkende. De vil tilpasse nettsidene med individuelle tilbud og opplevelser basert på hvem kunden er, hva de har kjøpt tidligere og hvordan de kom til nettsiden osv. I mange markeder forventer nå forbrukere å bli møtt med tilpasset innhold når de besøker nettbutikker. Amazon er et eksempel på et selskap som har bygget hele sin suksess på data de handlende mer eller mindre frivillig deler for å få tilgang til selskapenes tjenester. Jo mer data Amazon kan lagre om sine brukere, jo bedre kan de målrettet tilpasse sine produkter. Amazon har kommet så langt med dette, at de basert på forbrukers kjøpshistorikk og interesser, vurderer å sende produkter i retning forbruker før forbruker har bestilt produktet. Når forbruker bestiller varen, ligger varen klar for sending i nærheten av forbrukers adresse og de kan på denne måten kutte ned leveringstiden betraktelig.

Vi vil nok i større og større grad se at nettbutikkene også sammenkobler egne kundedata med data om forbrukeren i andre datakilder.

«Big data» er et begrep vi hører stadig oftere. Big data kan defineres som en datamengde så stor at den ikke lar seg behandle av tradisjonelle verktøyer. Alle elektroniske spor vi legger igjen i løpet av en dag, via sosiale medier, nettbutikk, SMS'er, telefonsamtaler, googling osv. utgjør denne datamengden. Et viktig mål for brukere av big data, er å kunne ta bedre beslutninger basert på informasjon som virksomheten allerede har tilgang til i egne (og dels i andres) datakilder. På denne måten kan virksomheten erstatte usikre antagelser om kundene eller produktene med datadrevne beslutninger.

Hallvard Fossheim skriver i Dagsavisen, at når store mengder informasjon blir lagret, sammenkoblet og prosessert på rett måte, kan resultatet være at man på noen områder kan oppnå større oversikt over den enkelte enn den enkelte selv har.[17] En fellesnevner er ofte at det ikke er fortid man er interessert i, men framtiden. Med nok data kan man med overraskende høy grad av sannsynlighet forutsi eller påvirke hva folk vil foreta seg, eller som hva som vil skje med dem, enten det dreier seg om kjøpemønster, kriminalitet eller sosial tilhørighet og vaner.

Teknologirådet nevner tre paradokser knyttet til big data[18]:

1. Transparens: Det samles inn mer privat informasjon om oss enn noensinne. Samtidig er detaljene rundt bruken av denne informasjonen nesten fullstendig omslørt av rettslig og kommersielt hemmelighold.
2. Identitet: Big data lover oss mer personalisering og tilpasning, grupperer oss samtidig sammen og forteller oss «hvem vi er» og «hva vi ønsker oss».
3. Makt: Big data lover store forandringer for «hvermansen», men flytter samtidig makten fra individer til store selskaper og myndigheter.

Europakommisjonens forslag til personvernforordning om behandling av persondata som per februar 2014 fortsatt var under politisk behandling av Europaparlamentet og Ministerrådet, vil slik forslaget så ut, kunne rette opp noen av de skjevheter som i dag finnes på det digitale feltet. Forslaget vil redusere overvåkingsbelastingen på befolkingen og gi en sunnere konkurranse mellom butikkene.

[17] http://www.dagsavisen.no/nyemeninger/hfossheim/

[18] http://www.etikkom.no/Documents/Presentasjoner/Big%20data%207.10.13/Big%20data%20og%20etikk,%20Prabhu.pdf

7.1 | Kan reservasjon mot å bli sporet bli en realitet?

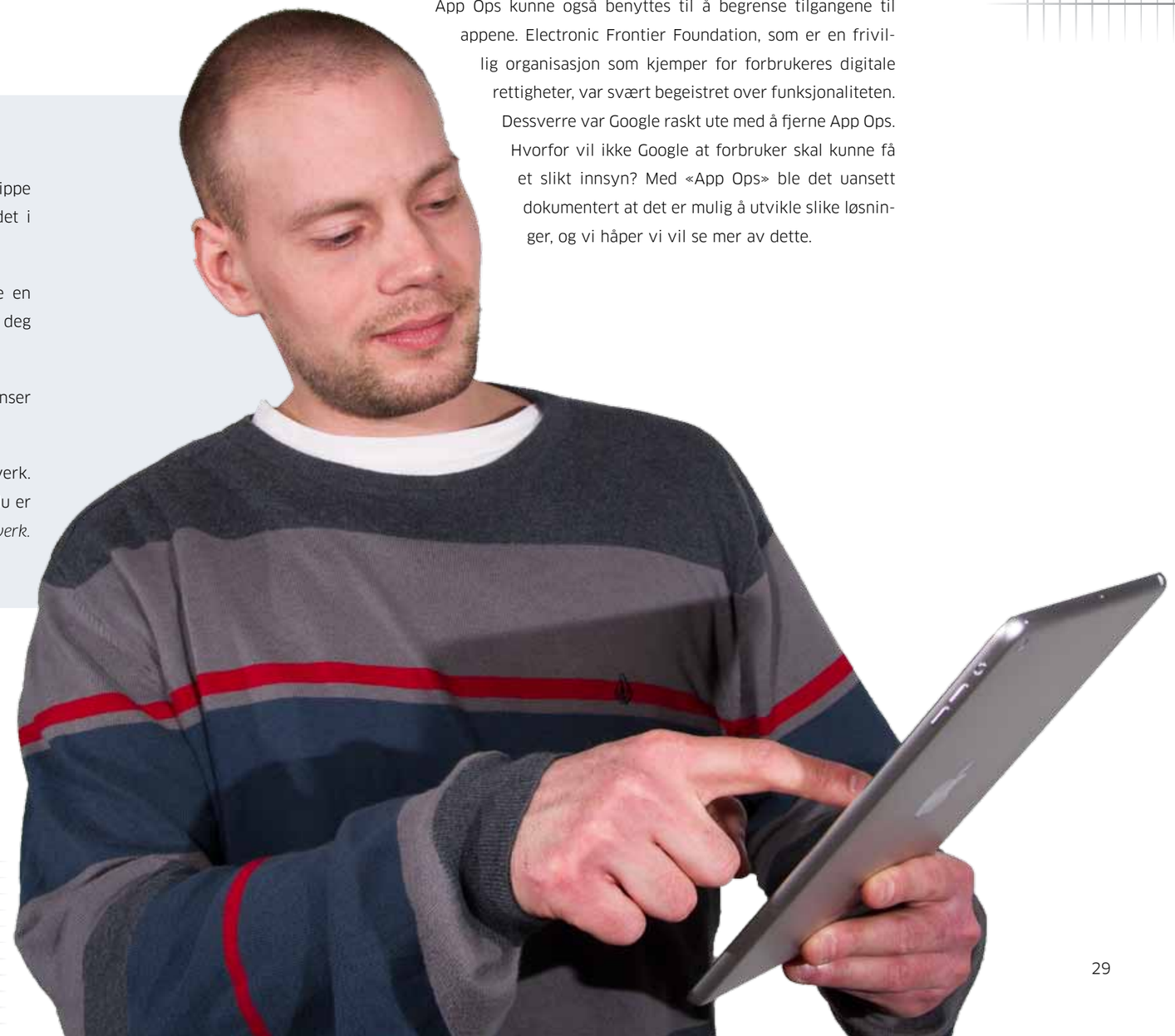
Privatpersoner kan reservere seg mot telefonsalg. Vi kan også reservere oss mot å motta uadressert reklame i postkassen. Som forbruker er det ønskelig også å kunne reservere seg mot å kunne bli sporet på nett.

Sporing på nett kan skje på mange måter og bruk av cookies/informasjonskapsler er en av metodene. Når man besøker nettsider, mottas disse små tekstfilene. De sender informasjon tilbake til nettsiden, slik at den gjenkjenner innstillinger og preferanser når nettsiden besøkes. Cookies benyttes til flere formål, deriblant til sporing. I bloggen til SINTEF eksemplifiseres sporing via cookies slik:

- Du besøker nettstedet *ganskevanligside.com*
- *ganskevanligside.com* laster inn innhold fra andre nettadresser (tredjeparter), f.eks. et knippe reklamebannere fra *reklamenettverk.com*, slik at når dette vises i nettleseren sin er det i praksis du som besøker tredjepartssidene.
- Første gang du besøker *ganskevanligside.com*, vil *reklamenettverk.com* gjerne plassere en cookie på datamaskinen din. Cookien inneholder f.eks. et unikt nummer som identifiserer deg (anonymt) for *reklamenettverk.com*, f.eks. #923489423897
- Deretter besøker du nettstedet *annenvanligside.no*, som tilfeldigvis også viser noen annonser fra *reklamenettverk.com*
- Siden du allerede har en cookie fra *reklamenettverk.com* på maskinen din, vil reklamenettverk.com nå kunne vite at du har besøkt både *ganskevanligside.com* og *annenvanligside.no* – du er jo personen med ID #923489423897 begge steder fordi du i praksis besøker *reklamenettverk.com* direkte gjennom nettleseren din i begge tilfeller.

Et steg i riktig retning er innføring av den nye Cookie-bestemmelsen i ekomdirektivet[19]. Bestemmelsen medfører at ansvarlige for nettsider må informere brukerne om cookie-bruk via en informasjonsside. Samtykke til bruk av cookies gir brukeren ved ikke å skru av for cookies i nettleseren. Bakgrunnen for lovendringen er at en rekke annonsører bruker informasjonskapsler for å spore forbruker rundt på nettet. Ved å kartlegge sidene du besøker kan de servere annonser som stemmer bedre overens med forbrukers interesser. Bestemmelsen har fått kritikk for å være upraktisk og at det medfører en fullstendig unødvendig utgift for bedrifter. Dessuten er det en umulig oppgave å påse at bedrifter etterlever informasjonspåbudet.

En god løsning som dessverre fikk kort levetid, var «App Ops» som ble lansert i Android 4.3. Hensikten med verktøyet var å gi forbrukere mulighet til se hvordan nedlastede apper forsøker å få tilgang til personverntruende kilder som eksempelvis lokasjon, kalender, kontaktliste osv. i telefonen. App Ops kunne også benyttes til å begrense tilgangene til appene. Electronic Frontier Foundation, som er en frivillig organisasjon som kjemper for forbrukeres digitale rettigheter, var svært begeistret over funksjonaliteten. Dessverre var Google raskt ute med å fjerne App Ops. Hvorfor vil ikke Google at forbruker skal kunne få et slikt innsyn? Med «App Ops» ble det uansett dokumentert at det er mulig å utvikle slike løsninger, og vi håper vi vil se mer av dette.



[19] Ekomloven § 2-7 bokstav b

8 | PROBLEMATIKK TILKNYTTET BRANSJENS SELVREGULERING

Betalingstjenesteområdet er i stor grad selvregulert. Kortselskapene Visa og MasterCard har utarbeidet regelverk som kortinnløsere selv forvalter. Utfordringer oppstår når bransjen som forvalter regelverket ikke etterkommer egne regler.

Under følger noen eksempler.

- Kortselskapene stiller krav til at en kortterminal må gjennom flere tunge sertifiseringer for å bli godkjent for det norske markedet, men er brukerstedet attraktivt nok, gir kortinnløser samtidig dispensasjoner og fritak fra dette. Når en løsning ikke er sertifisert, må den anses å være usikker. Eksempelvis kan sensitiv kortinformasjon komme på avveie gjennom hacking eller skimming. Sikre løsninger tar lenger tid å utvikle og de er dyrere å produsere. En annen konsekvens blir da at det ikke blir lønnsomt å satse på sikkerhet i produktutviklingen. Det bør heller ikke være slik at et norsk brukersted bare kan velge en utenlandsk kortinnløser, som velger å ikke følge gjeldende krav.

- Kortselskapene anbefaler sterkt at alle nettbutikker skal benytte sikkerhetsløsningen 3D Secure. Da dette kun er best practice, er det mange brukersteder som får fritak fra dette. I tillegg til sikkerhetstrusselen så kommer man inn i en ond sirkel. Om et brukersted får fritak, så ønsker ofte konkurrenten det samme. Det er primært fokuset på konverteringsrate som gjør at brukersteder ønsker fritak for 3D Secure, da de mener potensielle kjøpere faller fra ved autentisering. Det skal også understrekes at det ikke er 3D Secure som er problemet, men den lite brukervennlige autentiseringsløsningen Bank ID som mange kortutstedere har valgt. Secure Pay som er et europeisk forum for sikkerhet i betalinger består av tilsyn og overvåkingsorganer. I Seventh SEPA Progress Report skriver Secure Pay sine anbefalinger beste praksis når det gjelder sikkerhet i betalingstjenester på internett der betaling med kredittkort benyttes: «Brukersteder bør støtte sterk autentisering hos kortutsteder. Alle betalingsløsninger bør motivere til sterk autentisering ved å overføre ansvaret fra brukerstedet til utsteder[20]».

- Kortinnløserne og kortselskapene vedtok at innen 1. januar 2011 skulle alle kortterminaler være byttet ut med terminaler som leser chip i stedet for magnetstripe.[21] Her er Visa og MasterCard sine regler helt klare. Terminalene i butikk har blitt byttet, men i selvbetjente miljøer som typisk parkering finnes det ca. 1500 terminaler som fortsatt leser magnetstripe. På Flytoget er det også et høyt volum magnetstripetransaksjoner. Brukerstedene som eier disse ble i mange år før 2011 informert om kravet om bytte, men fortsatt er det mange som får lov til å benytte magnetstripelesere. Dette er terminaler som står i ubemannende miljøer, og man må anse at sjansen for å bli utsatt for svindel er stor. Om ikke disse løsningen raskt blir byttet ut, bør det som et minimum installeres anti-skimmings utstyr.

- Kortselskapene stiller krav til at brukersted skal være PCI sertifisert om brukerstedet skal lagre sensitiv kortinformasjon. Benytter brukerstedet moderne betalingsløsninger levert av en sertifisert sam-

[20] http://www.ecb.europa.eu/pub/pdf/other/recommendationsforthesecurityofinternetpaymentsen.pdf

[21] https://www.teller.no/Sikkerhet/EMV1/

arbeidspartner som eksempelvis Nets eller DIBS, er det få gode grunner til å lagre slike data. Før var det mange brukersteder som hadde egne systemer for å håndtere betaling på nett, fysiske brukersteder hentet ut data via magnetstripelesere for å tilby kunde elektronisk kvittering, kortnummer ble lagret i forbindelse med abonnementsbetalinger osv. Dette er ikke lenger tillatt uten å gjennomgå PCI DSS sertifisering og som nevnt har teknologien til leverandørene kommet så langt at slik lagring har blitt unødvendig. Allikevel er det selskaper som fortsatt lagrer kortinformasjon uten å være PCI sertifisert. Det er ikke slik at dette er beste praksis fra kortselskapene, men det er et krav at de skal gjennom en PCI sertifisering. I SEPA Progress Report skriver Secure Pay:

«Det oppfordres til realtidsovervåking og kontroll, som inkluderer sjekk mot svartelister og sperrelister, samt kontroll av unormal oppførsel. Den som tilbyr tjenesten, Payment ServiceProvider (PSP), skal oppfordre brukersteder til ikke å oppbevare kortdata, alternativt påse at de blir tilstrekkelig beskyttet. Kortselskapenes egne krav om å beskytte kortdata, de såkalte Payment Card Industry-kravene (PCI), vil også gjelde her. PSP skal tilby en sikker kommunikasjonskanal til kunden, som inkluderer å informere kunden om prosedyren for å rapportere mistenkelige hendelser eller belastninger som ikke er autorisert».

Konsekvensene av at kortinnløsere aksepterer løsninger som ikke er sikre, er ikke bare at forbruker kan bli utsatt for svindel. Usikre løsninger gjør også at forbruker må betale mer for varene fordi tap ved svindel må dekkes inn, samt at brukersted må betale langt mer i provisjon til kortinnløser når transaksjonene ikke er merket som 3D Secure eller Chip & PIN.

Det er også viktig at kravene til sikkerhet blir overholdt for å sikre like konkurransevilkår blant aktørene som tilbyr teknologi. Utviklingen går i feil retning når aktører som leverer sikre og sertifiserte løsninger ikke ønsker å satse i det norske markedet fordi de ikke kan konkurrere mot aktører som selger usertifiserte løsninger.

Betalingstjenesteområdet er altså i stor grad selvregulert. Når vi ser kortinnløsere som skal forvalte kortselskapenes regelverk igjen og igjen gir fritak og dispensasjoner fra sikkerhetskravene, så er det mye som tyder på det er behov for mer uavhengig tilsyn. Med mer nasjonal styring vil det også bli langt enklere å plassere ansvaret mellom aktørene enn i dag.

9 | SVINDEL

I følge Norges Banks «årsrapport om betalingssystem»[22] var det «lite» svindel også i 2012. I underkant av 0,02 prosent av all omsetning med kort er svindel. i 2012 utgjorde dette litt over 135 millioner kroner.

Selv om det uttales at svindeltallene er lave, er det viktig å huske at trusselbildet endrer seg hele tiden. Tapene er fordelt på følgende områder:

Svindeltype betalingskort	2011	2012
Misbruk av kortinformasjon, kort ikke til stede (internetthandel)	24 190	35 701
Stjålet kortinformasjon (inkludert skimming), misbrukt med falske kort i Norge	468	2 308
Stjålet kortinformasjon (inkludert skimming), misbrukt med falske kort utenfor Norge	57 340	55 869
Originalkort tapt eller stjålet, misbrukt med PIN i Norge	32 224	28 128
Originalkort tapt eller stjålet, misbrukt med PIN utenfor Norge	7 008	8 544
Originalkort tapt eller stjålet, misbrukt uten PIN	4 488	4 603
TOTALT	**125 718**	**135 153**

Kilde: Finanstilsynet

[22] http://www.norges-bank.no/pages/94894/Betalingssystem_2012_o.pdf

Svindeltype betalingskort	2011	2012
Angrep ved bruk av ondartet programkode på kundens PC (trojaner)	664	5 064
Angrep som utnytter sårbarheter i nettbankapplikasjon (hacking)	0	0
Tapt/stjålet sikkerhetsmekanismer	3 321	3 367
TOTALT	3 985	8 431

Kilde: Finanstilsynet

Det er usikkert hvor stor andel av svindelen som faktisk blir innrapportert av kortinnløsere/utstedere. Det er mulig at en del svindel blir tapsført uten at dette blir meldt videre. Svindel hvor brukersted står bak er heller ikke med i tallene. Det har også vært vanskelig å få oversikt over antall kortholdere som opplever svindel. Svindelstatistikken viser at det er 20 000 nordmenn som opplever svindel i løpet av et år, mens undersøkelsen Forbrukerrådet utførte i 2012 viste at det var 130 000 nordmenn som hadde opplevd kortsvindel det siste året. Avviket skyldes trolig mangelfull rapportering fra kortinnløser og kortutstedere i kombinasjon med at Finanstilsynet/FNO benytter et grunnlag hvor en del type svindel ikke er inkludert i statistikken.

Forbrukerrådet ønsker mer åpenhet om hvor kortmisbruk forekommer for å identifisere brukersteder som ikke tar betalingssikkerhet på alvor. Dette for å bidra til en mer rettferdig vurdering av forbrukertvister.

10 | MOBILHANDEL

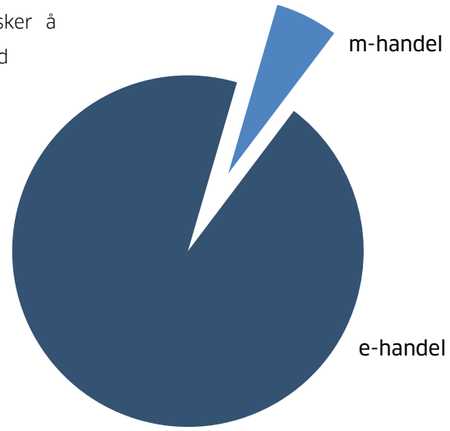
Selv om mobiltelefon som betalingsplattform er den raskest økende betalingsmetoden i Norge, utgjør det en liten andel sammenlignet med andre betalingsmetoder. Mobilbetaling kan innebære flere betalingsmetoder.

Eksempelvis betaling med NFC i fysisk butikk, QR-koder, via apper, overtaksert SMS eller som ordinært kjøp i nettbutikk via webleseren i telefonen. Dette er ny teknologi og det skaper definitivt utfordringer hva gjelder sikkerheten. Her er det ekstremt viktig at næringen er godt forberedt og har en proaktiv tilnærming.

10.1 | Mobilbetaling i e-handelen

I det følgende avsnittet omhandler vi e-handel hvor forbruker handler i en browser fra nettbrett eller smarttelefon.

En av hovedutfordringene for nettbutikkene som ønsker å selge via nettbrett og smarttelefoner, er at 3D Secure med autentisering med BankID ikke fungerer om man ikke benytter bestemte banker og teleoperatører. Brukersteder melder om opp til 80 prosent avbrutte kjøp ved check-out når autentisering med Bank ID skal gjennomføres. Uavhengig om betalingen for en vare gjennomføres fra en PC, smarttelefon eller nettbrett, så skal forbruker gjennom en autentisering. Som følge av denne problematikken er det mange brukersteder som søker sin kortinnløser om fritak fra å benytte 3D Secure. Når brukersted ikke benytter 3D Secure, så er det brukerstedet selv som må dekke tapene og ikke kortutstende bank. Tapskostnadene er det igjen forbrukerne som må dekke via høyere enhetspriser.



Problematikken relatert til Bank ID har gjort at fakturaleverandørene, og da primært Klarna, har fått et godt grep om mobilmarkedet. Ved betaling med faktura fungerer sikkerhetsmekanismene på samme måte uansett om betaling gjøres fra PC, brett eller smarttelefon. Det samme gjelder også PayPal som heller ikke krever noen autentisering med Bank ID.

E-handel via mobile enheter er i sterk vekst. Det er flere og flere nettbutikker som har bygget støtte for responsivt design. Med det menes design som tilpasser seg avhengig av device forbruker sitter med. Ved intervjuer av noen av de ledende nettbutikkene i Norge, forteller disse at 50 prosent av trafikken på nettstedene deres kommer fra brukere som bruker brett eller mobil, og omsetningen via samme kanaler står for 25 prosent.

10.2 | **Betaling via app**

De fleste appene som benytter kort som betalingsform finner vi på området transport og reiseliv. NSB og Ruter er de to som blir aller mest brukt. Apper hvor kjøper blir belastet over mobilregningen selger stort sett digitale innholdstjenester, selv om teleoperatørene forsøker å komme inn som et betalingsmiddel også innenfor andre varegrupper.

Når en app benytter kortbetaling, trenger brukerstedet følgelig en avtale med en kortinnløser. Betaling med kort i en app blir betraktet som et ordinært netthandelsbrukersted fra kortinnløsers side. Som nevnt skaper betaling i mobile devicer utfordringer fordi 3D Secure med Bank ID ikke fungerer for de fleste av forbrukerne. Dette kompliserer bestemmelsen av sikkerhetsnivået som brukersted skal benytte. Når brukersted får fritak for å kjøre 3D Secure, finnes det guidelines fra kortselskapene om hvordan forsøke å hindre svindel. Det har vært vanskelig å få nøyaktig svar på hvordan disse er utformet, og kortinnløserne håndterer dette på forskjellige måter.

For å sikre best mulig konverteringsrate er det vanlig ved mobilbetaling at brukersted lagrer kortnummeret til bruker når bruker oppretter profil i appen. Kortet skal da lagres hos en PCI DSS sertifisert part og i Norge benytter alle en PSP som innehar denne sertifiseringen. Fordelen er altså at kortholder slipper å ta frem kortet hver gang det handles i appen. I disse tilfellene bør det være påkrevd at kortholder taster inn sitt kontrollsiffer ved kjøp. Dette praktiseres i noen apper mens ikke i andre. Også her er det kortinnløserne som setter premissene for hvordan dette skal gjøres.

Som nevnt er dette et noe komplekst område som styres av kortbransjen selv som har noen guidelines som er førende. Det bør utarbeides en felles policy rundt sikkerhetsnivået som skal gjelde når brukersteder og leverandører har så sterkt fokus på å forenkle kjøpsprosessen.

10.3 | **App med betaling via mobilregningen**

Teleoperatørene forsøker også å bli en del av verdikjeden, og da med varer utover digitale innholdstjenester. Telenor har inngått avtale med Google som gjør at forbruker kan kjøpe apper og bli belastet via telefonregningen i Google Play. En utfordring her er at betaling via telefonregning ikke gir forbruker like god beskyttelse som når de handler med betalingskort. Mens de tradisjonelle betalingsformidlerne som banker og kredittkortselskaper må utforme sine vilkår i tråd med finansavtaleloven, gjør ikke teleoperatørene det sammen. Forbrukerombudet sier rett ut at teleoperatørene bryter loven[23].

10.4 | **Nettbank app**

Nettbank-apper har i løpet av kort tid rukket å bli svært populære. De er brukervennlige og enkelt tilgjengelig for forbruker. Som med andre løsninger bankene lanserer, må vi også her stole på at bankene har ivaretatt sikkerheten på en god måte. Løsningene er som oftest delt inn i to sikkerhetsnivåer.

[23] www.forbrukerombudet.no/2012/04/11042228.0

Eget passord er ofte tilstrekkelig for å kunne se saldo og overføre mellom egne konti. Dersom man skal gjennomføre regningsbetaling, må en også skrive inn engangskode i tillegg til passord. I Sverige har Datainspektionen (Datatilsynet) undersøkt sikkerheten i de svenske nettbank appene og uttrykker bekymring for dårlig vern av personopplysninger. Med bruk av riktig PIN og fødselsnummer kan personer hente ut informasjon om eksempelvis saldo, lån, transaksjoner osv. Etter gjennomgangen av Datainspektionen har både Nordea og Handelsbanken levert inn konkrete planer til nye sikkerhetsløsninger. Svenske myndigheter vurderer å forby Dansk Bank sin mobil app som for øvrig er den sammen appen som den norske filialen av Danske Bank benytter i Norge. Svenske myndigheter er de første i Norden til å granske disse banktjenestene. Datatilsynet i Norge vil se på rapportene til Datainspektionen før de bestemmer seg om de skal se nærmere på de norske mobilbank-appene.

På Forbrukerrådets betalingskonferanse i Trondheim, demonstrerte Einar Stangvik hvor enkelt man kan utføre et såkalt «man-in-the-middle angrep» i åpne nettverk som mange av oss benytter når vi logger oss i nettbanken. Ved å koble seg opp på den trådløse ruteren lurer han mobilen til forbruker til å tro at PC-en hans er den trådløse ruteren slik at all kommunikasjon mellom mobilen og internett foregår via Stangvik. Han får da kontroll over hva serverne og appene sier til hverandre. På denne måten kan hackeren både lese og endre data som går mellom nettet og mobilen. Stangvik mener de norske appene er sårbare overfor denne typen hacking. Men denne typen hacking kan hacker stanse innholdet serveren forsøker å sende appen og bytte dette ut med eget innhold som bruker da vil trykke på for å så bli sendt dit hacker ønsker. Det falske innholdet kan enkelt brukes for å svindle til seg sensitiv informasjon, eksempelvis for å logge seg inn på andres nettbanker. Det falske innholdet kan også inneholde ondsinnet programvare. Nå har flere av aktørene endret sine løsninger slik at serveren appen snakker med, faktisk tilhører appen. Blant annet var DnB raskt ute med å oppdatere sin app etter at Stangvik demonstrerte hvor enkelt det var både å legge inn falsk informasjon i appene og hvor enkelt det var å hente ut informasjon.

Tilfellene over tilsier at vi skal være kritisk til at sikkerheten er ivaretatt når de lanserer nye betalingstjenester. Finanstilsynet må spille en rolle når ny teknologi lanseres, slik Datadirektionen er i Sverige.

En utfordring med bankene er at det er lite åpenhet når det kommer til sikkerhet. Det kan i det lange løp virke fordummende overfor brukerne å ha en slik holdning da vi har sett hvor enkelt det har vært blant annet å hacke de norske nettbankene. Bankene burde tydeligere kommunisere sikkerhetsnivået i sine løsninger og la forbruker så ta et valg om de mener dette er troverdig og sikkert nok til å ta i bruk løsningene. Sikkerhetsmyndigheter og andre aktører viser derimot irritasjon over kritikere. Denne irritasjonen kunne kanskje vært unngått ved at de hadde vært litt mer åpne. Einar Stangvik mener på sin side at han ser det som langt mer nyttig å formane til skepsis og forsiktighet rundt å ta i bruk nye tjenester for tidlig, enn å proklamere «all is well».

11 | KONTAKTLØS BETALING

Norske banker har gjennomført pilotprosjekter hvor betalingskortet har innebygget RFID funksjonalitet, dvs. kort med radiosender. RFID er en godt utprøvd teknologi i andre sammenhenger enn betaling, som blant annet i adgangskort, heiskort, reisekort osv.

Når kortet holdes inntil terminalen, overføres betalingsinformasjonen mellom betalingskort og terminal. Kortholder kan betale småkjøp på henholdsvis 200 kroner med MasterCard PayPass og 175 kroner med Visa PayWave uten bruk av PIN. Beløpsgrensen for bruk av PIN forventes å øke til 200,- også på Visa PayWave i 2014. Overskrider beløpet beløpsgrensen, må kortholder betale som i dag ved å stikke kortet inn i terminalen og autentisere seg med PIN.

Parallelt med dette pågår det pilotprosjekter med NFC. Dette er tilsvarende funksjonalitet som RFID, men benyttes i smarttelefoner. I et samspill mellom NFC og SIM-kort med en betalingsapplikasjon, kan en bankterminal som kan lese RFID også lese NFC-signaler og dermed gjennomføre betalingstransaksjoner. Her gjelder samme beløpsgrenser, men kortholder taster ikke PIN om beløpet overskrider det PIN-frie beløpet, men taster inn en kode på telefonen som de automatisk mottar.

RFID og NFC er ingen ny teknologi og det er flere årsaker til at løsningene ikke har blitt lansert bredt ut i Norge enda. Fra brukerstedssiden så kreves det investeringer i nye bankterminaler og de må også betale langt mer i brukerstedsprovisjon fordi bankene ikke har valgt å bygge støtte for kontaktløs betaling med BankAxept.

Historien har vist hvor vanskelig det er å introdusere nye betalingsløsninger. Skal nye betalingsløsninger få gjennomslag må brukerne oppleve at disse er mer effektive enn eksisterende løsninger. Alternativt må det tilbys et økonomisk insentiv. Det er tvilsomt at selling pointene til kortinnløserne er tilstrekkelig til at produktet vil ta syv mil steget. De spiller på at produktet er mer hygienisk enn kontanter (kontaktløs betaling konkurrerer strengt tatt ikke mot kontanter) og at brukersted øker sin kundelojalitet ved å tilby en innovativ måte å betale på.

I Dagens IT kunne vi 10.desember 2012 lese om Telenor sjef Jan Fredrik Baksaas som formante til samarbeid og dugnad mellom sektorer og aktører for å få NFC ut til forbrukerne. Han uttalte at momentet rundt NFC og kontaktløs betaling med mobilen er så stort at det innen to år vil bli vanlig for de fleste av oss. Disse utsagnene går inn i rekken av utallige entusiastiske prognoser som involverte parter i NFC kjeden har kommet med. Man kan stille spørsmålet om NFC begynner å bli en utdatert teknologi og det er tross alt ingen forbrukere som roper på kontaktløs betaling når dagens betalingsløsninger fungerer svært godt. At Apple ikke har installert NFC i iPhone og dermed har vist NFC fingeren, bidrar neppe heller til at Baksaas' profeti vil gå i oppfyllelse. Kontaktløs betaling vil nok heller bli en realitet når teknologien fordrer mindre utskifting av infrastruktur på brukerstedssiden, forbruker får et skikkelig insentiv til å skifte handlemønster og løsningen tilfører brukersted større verdi enn kun selve betalingstransaksjonen. Dette kan det virke som om mCASH har forstått og deres løsning blir nærmere beskrevet under. Deres kontaktløse løsning er ikke basert på NFC med de åpenbare begrensningene NFC gir, men bruker QR-koder som støttes av alle smarttelefoner.

Sikkerhetsaspektet ved bruk av NFC betaling hører vi lite til. Vi kan riktignok lese at forbrukers rettigheter er de samme som med øvrige betaling utført med chip & PIN, men det er ikke her utfordringen rundt sikkerheten primært ligger. Utfordringen ligger i at NFC teknologien er en velegnet inngang til mobile enheter for kriminelle.

Spørsmålet er når kriminelle for alvor begynner å innse hvilken gavepakke NFC kan være for dem. Om noe så enkelt som å bytte ut en NFC-lapp eller plassere en lapp i nærheten av en «sunn» NFC leser kan gi kriminelle full tilgang til telefonen din, er det bare kreativiteten som setter grenser for hva dette kan brukes til.

Det er vanskelig å få full oversikt over betalingsløsninger basert på kontaktløs teknologi som er planlagt lansert, men følgende løsninger er mye omtalt i media:

VALYOU

Telenor og DnB har etablert selskapet TSM Nordic AS med det hovedmål å skape et åpent økosystem for kontaktløse tjenester via mobilen. Selskapet

har ambisjoner om å utvide selskapets virksomhet internasjonalt og i Norge var siste kommuniserte lanseringstidspunkt høsten 2013. Som med alle andre løsninger som baserer seg på NFC teknologi er det en rekke brikker som må være på plass for at forbruker skal kunne ha nytte av løsningen. Det stilles krav til type mobilabonnement, bankforbindelse, type telefon og selvsagt at betalingsterminalen støtter betaling med NFC.

Hvor attraktivt produktet vil bli er vanskelig å si, og med de forutsetningene som nevnt over er det heller ikke et særlig høyt antall brukere per nå som i det hele tatt kan ta løsningen i bruk.

Tap2Pay

Dette er et produkt som minner mye om VALYOU, men forskjellen er at Tap2Pay er knyttet opp mot et MasterCard og ikke et Visa-kort.

Fellesnevnerne ved de to ovennevnte løsningene er at vi i årevis har hørt om at løsningene forventes satt i drift innen kort tid og troverdigheten begynner nå å bli rimelig tynn.

mCASH

Dette er en app som forventes lansert i tidlig i 2014. Appen er koblet opp mot en sentral server som er koblet til banker, kortselskaper og butikker. Koblingen til butikkene skjer over internett og gjennom kassen i butikken. Når forbrukeren skal betale for varer i kassen, skanner han en mCASH QR-kode og mottar straks en betalingsforespørsel. Denne inneholder informasjon fra kassen om hva kunde skal betale, akkurat som den man normalt får i betalingsterminalen. Videre bekrefter kunden på mobilen med sin PIN-kode og betalingen behandles deretter av kundens bank. Fordeler skal være at det går raskere enn å betale med kort, og du kan pakke varene i posen mens du venter fremfor å stå ved betalingsterminalen med kortet. Løsningen skal kunne benyttes til både betaling mellom personer, i butikk og på nett. På internett slipper man å taste inn kortnummer og bekrefte med Bank-ID, og det skal føre til en dramatisk forbedring av brukeropplevelsen i følge mCASH. En fordel skal også være at applikasjonen kan knytte mobilen til både betalingskort og bankkonto og mCASH belaster den valgte kontoen.

En av hovedgrunnene til at mCASH mener at de vil lykkes, er at løsningen ikke innebærer dyre investeringer eller økning i brukerstedsprovisjoner. Det vil tvert i mot bli billigere å betale med mCASH.

Det «skumle» med løsningen er at den fanger opp svært mye personopplysninger. Den fanger ikke bare opp hvor forbruker handler, men også hva forbruker handler. På Forbrukerrådets betalingskonferanse i november 2013 forklarte gründer Daniel Döderlein mulighetene dette gir brukerstedene som får tilgang til denne informasjonen. Han understreket at forbruker vil få et tydelig valg om de ønsker at informasjonen skal kunne benyttes av butikkene, og det skal gjøres enkelt å slette tidligere gitt samtykke.

12 | UTFORDRINGER MED AT MYE SAMLES I ÉN ENHET

Finanstilsynet er blant flere som har uttrykt bekymring over at det stadig kommer til flere bank- og betalingstjenester i mobilen som gjør at man samler alt i et risikopunkt i stedet for å spre det utover.

De er såpass bekymret at neste risiko- og sårbarhetsanalyse av foretakenes bruk av IT vil dreie seg om mobilitet. Rapporten skal være klar i mars 2014.

Datatilsynet støtter Finanstilsynet. Man gjør nå mye via mobilen som har en bitte liten skjerm der bruker kanskje ikke har den samme sikkerhetsprogramvaren som på en datamaskin sier de. De oppfordrer også Finanstilsynet til å etterprøve bankene når de forteller at disse appene er pålitelige og sikre.

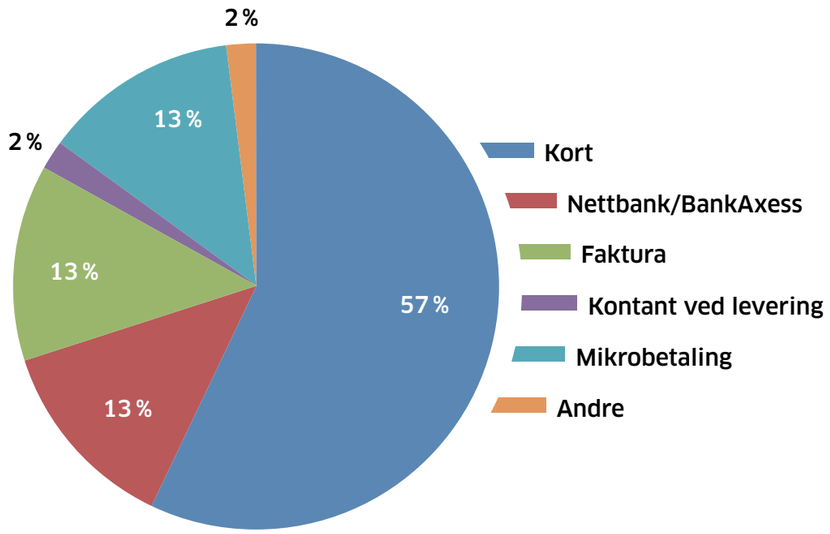
13 | HVORDAN BETALER VI PÅ NETT?

Betaling med betalingskortene Visa og MasterCard har siden starten på e-handelen vært de dominerende betalingsmetodene og slik er det fortsatt.

Postoppkrav var også i en periode utbredt, men har stort sett blitt erstattet med kortbetaling eller andre betalingsformer som gir nettbutikk mindre administrasjon med varehåndtering, samt garantert oppgjør fra finansiell samarbeidspartner.

Med tiden ar det blitt utviklet flere nye betalingsmetoder som mange nettbutikker nå tilbyr sine kunder. Undersøkelser viser at en av hovedårsakene til at forbrukere avbryter sine kjøp, er at nettbutikken ikke tilbyr ønsket betalingsform. Betalingsformens kostnad for brukersted innvirker også på hvilke betalingsformer brukerstedene ønsker å tilby til sine kunder.

Slik sier forbrukerne i følge DIBS e-handelsindeks at de ønsker å betale på nett:



Kortbetaling: Visa og MasterCard dominerer. Diners og Amex tilbys av en del brukersteder, primært innen reise og underholdning. Å betale med kort oppfattes som trygt og det er enkelt.

For forbruker vil den tryggeste betalingsformen være å betale med kredittkort fremfor å benytte debetkort tilknyttet personlig bankkonto. Dette fordi ved kredittkortkjøp, trekkes ikke kjøpesummen direkte fra konto, men kredittkortselskapet betaler nettbutikken. Forbruker får så en faktura slik at kortholder ikke har noe med oppgjøret til nettbutikk å gjøre. Når forbruker mottar faktura fra kredittkortselskapet, kan forbruker dobbeltsjekke at alt er korrekt. Om beløpet ikke er korrekt eller om forbruker er svindlet, står man tryggere ettersom pengene ikke har blitt trukket fra konto.

Visa og MasterCard sine regler for tilbakeføring ved svindel, er dog uavhengig om kortet er debet- eller kredittkort, men forskjellen er at paragraf 54b i finansavtaleloven kun gjelder ved kredittkjøp.

Nettbank: Selv om en del av spurte forbrukere responderer at de ønsker å betale via nettbank, er det et ikke så mange nettbutikker som tilbyr denne betalingsformen. Unntaket er mindre nettbutikker som ønsker å tilby en betalingsform med lave kostnader.

BankAxess: BankAxess er en norsk betalingstjeneste som alle banker i Finans Norge, eller har avtale med Finans Norge har anledning til å tilby. I likhet med BankAxept er BankAxess en samordnet tjeneste som gjør det mulig for en kjøper å godkjenne belastning av sin bankkonto til fordel for en selger med konto i annen bank. Mens BankAxept-kort bare kan benyttes for å godkjenne en umiddelbar belastning, kan BankAxess benyttes for å godkjenne en belastning som skal gjennomføres på et senere tidspunkt, altså i det øyeblikk varene sendes fra nettbutikk.

Betalingsformen har hatt en beskjeden vekst. Omsetning via BankAxess utgjorde i 2012 534 millioner kroner mot 478 millioner i 2011. Selv om nettbutikk kan tilby lavere priser til kunder som handler med BankAxess, så finnes det ikke noe godt insitament for forbruker å velge denne betalingsformen. Betalingstjenesten er tungvinn å komme i gang med for bruker og tjenesten er lite markedsført. Bankene tjener mer på betalinger foretatt med Visa- eller MasterCard kort enn med BankAxess. Løsningen vil trolig i løpet av 2014 enten bli faset ut eller så vil løsningen rustes opp.

Faktura: Online betaling med faktura og garantert oppgjør er en relativt ny betalingsform som har fått stor utbredelse blant de norske nettbutikkene. Ved betaling med faktura gjøres det en online kredittsjekk basert på forbrukers fødselsnummer, og det skjer like raskt som autorisasjon med kort. Årsaker til at mange forbrukere ønsker å betale med faktura er at de får mulighet til å se varene og dermed forsikre seg om at de ikke betaler for noe de ikke har bestilt og ingen autentisering med Bank ID er nødvendig.

Delbetaling/kontokunde er en tjeneste som gir fakturaleverandør gode inntekter. Ved avtale om delbetaling er det viktig at forbruker blir opplyst om hva den totale kostnaden vil bli. Avhengig av fakturaleverandøren, kan forbruker enten velge en fast avdragsordning eller de kan velge en såkalt «minimum to pay» løsning. Det kan stilles spørsmål om det skal være tillatt å tilby forbruker delbetaling helt uavhengig av kjøpesummen. Det viser seg at mange forbrukere velger å dele opp kjøpesummen til tross for at varen koster lite og totalprisen blir høy. Koster for eksempel varen NOK 200,- og man velger å betale over seks avdrag, utgjør fakturagebyrene NOK 270,-. I tillegg tilkommer renter som ofte ligger på rundt 22 prosent._

Microbetaling: Mange forbrukere svarer at de ønsker å benytte microbetaling, og da er det primært PayPal (eid av eBay) som blir benyttet. PayPal er en amerikansk betalingstjeneste for netthandel og er således et godt eksempel på en virtuell betalingstjeneste uten noen form for norsk regulering. En av fordelene med PayPal er at bruker slipper å taste inn betalingsopplysningene hver gang man handler på nett. For å komme i gang med PayPal må forbruker opprette en konto hvor man kan velge å fylle opp kontoen med x antall kroner og/eller tilknytte et kredittkort til kontoen.

PayPal opererer med det de kaller PayPal kjøperbeskyttelse. Kjøperbeskyttelsen gjelder så fremt man har kjøpt varer som ikke strider mot brukeravtalene til PayPal og eBay (eksempelvis immaterielle varer som digitale varer/tjenester, fast eiendom, virksomheter etc.). Videre skal det gjelde en fysisk vare som sendes med post/leveringsfirma og hele beløpet for varen skal være betalt med én betaling. Oppstår det tvist skal denne tvisten opprettes innen 45 dager etter kjøpsdatoen og om denne ikke lar seg løse innen 20 dager etter opprettelse må det eskaleres et krav hvor så PayPal så avgjør saken. Overholdes ikke tidsfristene vil ikke PayPal bistå forbruker.

14 | HVA KOSTER BETALINGSTJENESTENE?

I Norge er det virksom konkurranse på kortinnløsersiden. Det har blitt mange innløsere i et lite marked. Mens det tidligere fantes noen forskjeller, har nå kortinnløserne blitt veldig like.

Viktigste konkurranseparameter er definitivt pris og oppgjørsfrekvens, noe som kommer forbrukerne til gode. Brukerstedsprovisjon er noe hvert enkelt brukersted forhandler med sin innløser om. For mindre brukersteder ligger nå standardprovisjonen for Visa og MasterCard transaksjoner på rundt 1,99 prosent pluss NOK 90,- per måned om omsetningen ikke når et visst nivå. Store brukersteder betaler ned mot 1 prosent og under dette også.

Interchange

En viktig parameter som påvirker brukerstedsprovisjonen er interchange. Interchange er et formidlingsgebyr som kortinnløser betaler til kortutsteder. Den nasjonale interchangen fastsettes av medlemsorganisasjonen i Visa Europe Norge som består av kortinnløsere og kortutstedere. Interchangesatsen varierer ut i fra type kort (debet- kredittkort), type sikkerhet i løsningen, samt bransje. Det er egne satser for kjøp foretatt på utenlandske brukersteder.

I forbindelse med revisjon av betalingstjenestedirektivet, har EU-kommisjonen fremmet flere forslag til reguleringer av betalingsformidling. Når det gjelder interchange er det foreslått å sette disse til 0,2 prosent på debetkorttransaksjoner og 0,3 prosent på kredittkorttransaksjoner for grenseoverskridende handel uavhengig om betaling utføres i fysisk butikk eller på nett. De samme satsene skal være gjeldende også for nasjonale korttransaksjoner med Visa og MasterCard, men først gjeldende to år etter forordningens ikrafttredelse. Et annet utkast til forordning er at det skal være forbud mot automatiske mekanismer som begrenser kortholders valg av korttype. Dette betyr at prioriteringsregelen som i dag finnes i alle betalingsterminaler står for fall og kortholder skal selv kunne velge betalingsmetode i kjøpsøyeblikket. Følgende av dette vil bli dyrere enhetspriser når butikk vil måtte betale mer i brukerstedsprovisjon.

I fysisk handel benyttes primært BankAxept og ikke Visa eller MasterCard. BankAxept er en kostnadseffektiv betalingsmetode for alle parter, og brukersted betaler i snitt et transaksjonsgebyr på mellom 10 og 20 øre mot i rundt 2 prosent ved bruk av Visa og MasterCard. Tiden vil vise om BankAxept vil leve videre eller om dette blir faset ut. Finland har gjort dette med sine nasjonale kort til fordel for de internasjonale kortene. Disse er langt dyrere å benytte for bruker og butikk. De som vil tjene på å fase ut BankAxept vil være kortutstedere og kortinnløserne.

På betalingsformidlingskonferansen Finans Norge avholdt i oktober 2013, presenterte Eldar Skjetne fra SpareBank 1 Gruppen de videre planene for BankAxept. Bankene har etablert NyBax som har til hensikt å revitalisere BankAxept både hva gjelder forretningsmodell og funksjonalitet, slik at tjenesten ikke taper i konkurranse med andre kort grunnet manglende funksjonalitet eller økonomisk insentiv for bankene til å fortsette å satse på produktet. Utfordringen her vil være om bankene vil forplikte seg her når de tjener langt mer på transaksjoner foretatt med Visa og MasterCard.

Amex og Diners har ingen interchange siden dette er lukkede systemer hvor kortselskapene fungerer som både innløser og utsteder.

Surcharging

Viderebelastning av brukerstedsprovisjon over på kortholder, såkalt surcharging, er et tema som stadig er oppe til diskusjon. Slik surcharging var tidligere ikke tillatt, men er nå lovfestet i finansavtaleloven § 39b. I loven heter det blant annet «Dersom en betalingsmottaker krever gebyr eller gir rabatt for bruk av et bestemt betalingsinstrument, skal betaleren opplyses om dette før en betalingstransaksjon iverksettes. Institusjonen kan ikke hindre betalingsmottakeren i å kreve gebyr eller gi rabatt som nevnt». Surcharging har alltid blitt praktisert men da innbakt i varens totalpris. Prisdiskriminering basert på om kunde betaler med kontanter eller kort/korttype har ikke blitt praktisert i Norge. Dette gjøres blant annet i Danmark, hvor brukerstedsprovisjonen butikk må betale til sin innløser viderebelastes kortholder ved bruk av internasjonale kort. Fordelen ved å surcharge slik det gjøres i Danmark, er at man får frem kostnadene ved kortbetaling og man unngår at de som betaler kontant eller med Dankort må dekke den høye brukerstedsprovisjonen

som øvrige kort genererer. Man får følgelig også konkurranse på betalingstjenestene. Ved å synliggjøre ekstrakostnadene kan forbruker velge betalingsmiddel ut i fra pris og evt. andre faktorer.

Ulempen ved surcharging er at prisbildet kan bli uoversiktlig for forbruker. Ulike priser basert på forbrukers betalingsmetode blir også komplisert da opplysningsplikten i finansavtaleloven § 39b skal overholdes. Det er videre naivt å tro at enhetsprisene kommer til å gå ned om brukerstedsprovisjonen bli skilt ut. Trolig vil vi heller oppleve at prisene blir de samme, men at brukerstedsprovisjonen vil bli lagt på.

BankAxess

Ved denne betalingsformen betaler brukersted et månedsgebyr og en fast kronesats til banken de inngår avtale med. Også her er varierer satsen ut fra volum, og kan typisk ligge på 300,- per måned og NOK 1,50,- til NOK 3,- per transaksjon.

Faktura

Som de øvrige betalingsformene, settes også her satsene ut fra volum og prisingen er noe kompleks, samt at den varierer fra selskap til selskap. Man kan si at fakturakjøp/fakturafinansiering prises på noen lunde samme måte og med samme satser som ved Visa og MasterCard. Brukersted mottar altså ca. 98 prosent tilbake av salgssummen. Brukersted legger som oftest på et fakturagebyr som dekker inn deres kostnader eller baker kostnaden inn i vareprisen.

Ved kontokjøp/delbetaling betaler sjelden brukersted provisjon for tjenesten, da dette er en særs lønnsom løsninger for fakturaleverandør.

PayPal

Brukersted betalinger ingen faste kostnader men betaler 2,80,- per transaksjon pluss en prosentsats som varierer mellom 1,9 til 3,4 prosent. PayPal belaster ikke forbruker ved kjøp så fremt kjøpesummen er i norske kroner. Ved utenlandsk valuta legges det på et valutakonverteringsgebyr.

PSP kostnader

Alle nettbutikker benytter en Payments Service provider som tilbyr teknologien som håndterer de forskjellige betalingsformene på en sikker måte. Ofte betales en månedskostnad på NOK 600,- pluss et transaksjonsgebyr som varierer fra NOK 0,50,- til NOK 2,50,-.

15 | BETALINGSTJENESTER I FYSISK VAREHANDEL I NORGE

Innen fysisk varehandel har det ikke skjedd like store endringer som vi har sett i den digitale verden. Det har vært gjennomført et omfattende skifte av betalingsterminaler som følge av innføringen av chip, og en del av de nye terminalene har også støtte for NFC og RFID.

På samme måte som vi ser innen e-handelen, forsøker også fysisk butikk å benytte den informasjonen de innehar om oss for å opprette en-til-en dialog. Kjøper man varer på eksempelvis Maxbo eller G-sport, kan forbruker få rabatter i bytte mot kontaktopplysninger, som benyttes for å sende nyhetsbrev og tilbud. Kundelojalitetsprogrammer er et virkemiddel som flere og flere aktører innen varehandelen tar i bruk. En betalingsløsning fysisk varehandel ønsker seg, er en løsning hvor betalingen går gjennom de kjente og godkjente nettverkene (eller aller helst på finansiering), men at løsningen også åpner opp for at butikk kan gjøre datafangst om forbruker som importeres i CRM løsningen.

En trend blant flere bransjer i varehandelen er at marginene stadig blir mindre og mindre. Resultater av dette er blant annet økt fokus på betaling med finansiering som gir gode inntekter, samt salg av tilleggstjenester som vareforsikringer.

Betalingsløsningene som tradisjonell varehandel benytter i dag ses på som ryddige og oversiktlige, og svindelen her er lav. Det har historisk sett vært noen utfordringer med aktører som har leid ut betalingsterminaler og så rutet alle oppgjør inn på egen konto. Dette er historie og det er tatt grep for å sikre at dette ikke skjer igjen.

Betaling med mobil ved bruk av NFC eller QR-koder er på vei og en del brukersteder har også testet ut forskjellige løsninger med vekslende erfaringer. Hovedhensikten med innføringen av kontaktløs betaling er for mange butikker at betalingen da kan gjennomføres raskere enn normal betaling i bankterminal med bruk av chip og PIN.

15.1 | Kortbetaling i vareautomater

I takt med økt kortbruk og mindre kontanter blant forbrukerne, øker antall betalingsterminaler i selvbetjente vareautomater. Kortbetaling i vareautomater er relativt nytt og det bærer det også preg av. Det er ofte andre leverandører enn Point og Nets som leverer kortterminaler innen vending. Dette fordi det stilles andre krav til betalingsterminalens størrelse og virkemåte enn hva disse primært leverer. Innen vending er heller ikke PIN-PAD påkrevd om varen koster mindre enn 15 euro. Kravene til sertifiseringer og godkjenninger er dog de samme som gjelder for terminaler hvor det er ekspedient til stede. Ved bruk av Point og Nets så fungerer alt i henhold gjeldende regelverk. Situasjonen er litt annen når det gjelder de rendyrkede vending-terminalene. Hovedleverandøren av terminaler innen vending i Norge, benytter terminaler som ikke oppfyller kortselskapenes krav til sertifiseringer.

Hvordan kan det da ha seg at brukersteder kan få avtale med kortinnløsere som forvalter regelverket til de internasjonale kortselskapene uten at terminalen oppfyller gjeldende krav? Dette er litt uklart, men det antas at kortinnløsers vurderinger av sikkerhet opp mot inntjening på kortprovisjon gjør at brukersteder får fritak. Problemet med at det gis fritak for nye løsninger som utplasseres, er at sikkerhet blir en konkurransehemmende faktor. Sertifiseringene er svært dyre, det stilles høye krav til software og det skal også inn fysiske komponenter for at løsningen skal kunne bli sertifisert. Pris vil som oftest være det viktigste kriteriet for valg av betalingsterminal. Når brukersted mottar de samme betingelsene fra sin kortinnløser uavhengig om løsning er sertifisert eller ikke, så velger ofte brukersted den rimeligste løsningen. Sertifiseringene skal blant annet sikre at det er mer eller mindre umulig å hente ut sensitiv kortinformasjon fra terminalen som senere kan misbrukes av kriminelle.

Obligatoriske sertifiseringer

- EMV Level 1
- EMV Level 2
- PCI PTS 3.1 eller senere
- PCI PA-DSS 2.0 eller senere
- Visa ADVT
- MasterCard TQM
- MasterCard TIP
- PNC E2ECE for UPT komponenter
- CE

15.2 | Kortbetaling innen parkering

Brukerstedene ble varslet om EMV kravene tilbake i 2008. De har altså fått god tid på seg til å bytte ut sine terminaler, og etter 1. januar 2011 ble det ikke lenger tillatt å benytte ikke-godkjent terminal. Varehandelen har tatt dette til følge og i dag finnes det i butikkene ingen terminaler som ikke er godkjent, og det er heller ikke teknisk mulig å benytte noen annet enn terminaler som er godkjent.

I selvbetjente miljøer er det ikke slik. Det finnes fortsatt mange hundre terminaler som ikke er byttet ut enda og som dermed er sårbare for svindel. Det er jo nettopp i selvbetjente miljøer at sikkerheten burde være på topp. Disse terminalene finnes primært innenfor parkering og bomanlegg. En av årsakene til at disse ikke har byttet ut løsningene sine, har vært at deres leverandør ikke har hatt noen godkjent betalingsløsning som støtter EMV kravene. Det kan kanskje stemme til en viss grad, men det er en rekke selskaper som har byttet ut sine løsninger, og dette er selskaper som benytter de samme leverandørene som de som ikke har byttet ut sine enda.

REFERANSER

Finanstilsynets «Risiko- og sårbarhetsanalyse 2012»

Artikkel 29-Gruppen: Udtalelse nr. 02/2013 om apps i intelligente enheder

DIBS e-handelsindeks 2012/2013

Norges Banks årsrapport om betalingssystem

Datatilsynets rapport, «Hva vet appen om deg?»

Datatilsynets rapport, «Big Data - personvernprinsipper under press»

Datatilsynets rapport, «Internettsveip 2013»

ORDLISTE

3D Secure: Kortselskapenes tekniske standard for å identifisere og beskytte kjøpere og selgere når kortbetalinger utføres via internett. 3D Secure beskrives nærmere under.

Artikkel 29: EU-kommisjonens rådgivende organ i personvernspørsmål.

Autorisasjon: Kontroll mot kortutstedende bank om det finnes dekning på kortet, om det er sperret med mer i forbindelse med en korttransaksjon.

BankAxept: Åpent betalingssystem hvor alle banker i Norge kan tilslutte seg nettverket gjennom Finans Norge. BankAxept har en markedsandel på 88,2 prosent. Kortet kan ikke benyttes til netthandel som gjør at markedsandelene går noe ned år for år.

Brukerstedsprovisjon: Prosentvis avgift som brukersted betaler til sin kortinnløser.

Chargeback: Korttransaksjon som er gjenstand for reklamasjon i henhold til kortselskapenes regelverk.

CVC2/CVV2: Henholdsvis MasterCards og Visas betegnelse på sikkerhetskoden trykket på baksiden av kortet.

EMV: Samarbeid mellom Europay, MasterCard og Visa der målet er å øke sikkerheten gjennom å følge en omforent standard for kommunikasjon mellom betalingsterminaler og kort basert på chipteknologi. De samme reglene gjelder nå også for Amex, Discover Card og Diners Club. I henhold til kortselskapenes regelverk er det ikke tillatt å benytte en ikke-godkjent betalingsterminal etter 1. januar 2011.

IMEI-nummer: Telefonens unike identitet.

Interchange: Et såkalt formidlingsgebyr som kortutstedende bank mottar per transaksjon. Interchangegbyret varier i størrelse ut i fra bransje, sikkerhetsløsningen som benyttes samt korttype. Et kredittkort har ofte en høyere interchange fordi kortutsteder har en kredittrisiko. Videre er det forskjell på nasjonale og internasjonale satser.

IP-adresse: Unik identifikator som tildeles en PC.

Kortinnløser: En kortinnløser er brukerstedets finansielle samarbeidspartner. De samler inn korttransaksjoner, utbetaler oppgjør samt videresender korttransaksjoner til kortutsteder. De norske kortinnløsere eller innløsere som har etablert kontor i Norge er Teller, Elavon, Nordea, Handelsbanken og Swedbank.

Kortselskap: Betegnelse på Visa, MasterCard, Diners, Amex og eventuelt andre kortmerker som utsteder og bedømmer oppfyllelsen av regelverket for håndteringen av kort.

Kortutseder: Bank eller annen finansiell institusjon som utsteder kort. Kortutstedere responderer på autorisasjoner og trekker kortholder.

NFC: Near Field Communication tilsvarer RFID men NFC benyttes i smarttelefoner.

PCI DSS standarden: De internasjonale kortselskapene har satt opp noen sikkerhetsstandarder som gjelder i forbindelse med alle kortbetalinger. PCC DSS står for Payment Card Industri-Data Security Standard. PCC DSS er regler for hvordan sensitive kortinformasjon skal håndteres.

Prioriteringsregelen: I de norske terminalene er det en prioriteringsregel som gjør at terminalen prioriterer BankAxept delen i kort som er co-branded med andre betalingskort som eksempelvis Visa eller MasterCard.

PSP (Payments Service Provider): En PSP er den tekniske leverandøren av teknologien som muliggjør sikker betaling og fungerer som bindeleddet mellom nettbutikk/kortholder og kortinnløser/kortutsteder/fakturaleverandør etc. En PSP fungerer litt som en kortterminal gjør i den fysiske handelen. I Norge er det fire dominerende PSP'er. Dette er NetAxept (Nets), PayEx og DIBS. Svenske Klarna har også etablert seg i Norge og har i løpet av kort tid blitt en betydelig aktør.

RFID: Radio Frequenzy Identification hvor en radiosender er implementert I betalingskortet. Kortet kan benyttes for betaling i bankterminaler som støtter kontaktløs betaling.

SEPA: Single Euro Payments Area er et felles europeisk betalingsområde som dreier seg om harmonisering av euro-betalinger.

Skimming: Uautorisert kopiering av betalingskort. Gjøres typisk ved at svindlere monterer en kortleser i en betalingsterminal som kopierer kortinformasjonen og som så igjen brukes til å produsere falske kort.

Layout: Atle Hansen | www.drage-design.no