Finanstilsynet
Postboks 1187 Sentrum
0107 Oslo

Dato: 10.09.2015
Vår ref.: 15-1041
Deres ref.: 15/5816

Høring – forslag til nytt regelverk på området for betalingstjenester og finansforetakenes bruk av informasjons- og kommunikasjonsteknologi (IKT)

Det vises til Finanstilsynets brev av 16. juni 2015 med forslag til endringer i IKT-forskriften samt til nytt regelverk på betalingsformidlingsområdet. Høringsfristen er 1. september 2015. Pga intern saksbehandling har Finans Norge bedt om og fått innvilget utsettelse til 10. september 2015.

Finans Norges hovedmerknader:

- Finans Norge kan ikke slutte seg til forslaget til endring i IKT-forskriften som innebærer at foretaks styre skal behandle *alle* avtaler om utkontraktering og endring i slike avtaler.
- Det bør ikke være krav om styrebehandling så fremt anskaffelsen eller endringen i denne ligger innenfor styrefastsatte retningslinjer for anskaffelser uten styrebehandling. Finans Norge mener at forslaget til forskrift på området for betalingstjenester ikke i tilstrekkelig grad gjenspeiler hvordan systemer for betalingstjenester reelt sett er innrettet. Vi synes ikke at forkriftsutkastet implementerer EBAs retningslinjer om sikkerhet for nettbaserte betalinger på en hensiktsmessig måte. Finans Norge mener forskriftens virkeområde må være sammenfallende med EBA's retningslinjer.

1.1 Om forslaget til endring i regelverket om utkontraktering

Forskrift 21.05.2003 om bruk av informasjons- og kommunikasjonsteknologi gjelder alle foretak underlagt tilsyn av Finanstilsynet. Forskriften omfatter IKT-systemer som er av betydning for foretakets virksomhet. For eksterne brukere av foretakets IKT-systemer skal det foreligge avtaler som sikrer at forskriftens krav til sikkerhet og dokumentasjon ivaretas.

Gjeldende forskrift § 12 setter krav ved utkontraktering av foretakenes IKT-systemer. Bestemmelsen forankrer foretakets fulle ansvar for utkontraktert virksomhet og oppstiller krav til utkontrakteringsavtalene, herunder for å sikre Finanstilsynet tilgang ved inspeksjon.

Bestemmelsen oppstiller imidlertid ingen kvantitative/ kvalitative begrensninger i utkontrakteringsretten. En slik begrensning følger imidlertid nå av finansieringsvirksomhetsloven § 2-17 a) som etter endring i 2014 setter et forbud mot utkontraktering av kjerneoppgaver. Ved en samtidig endring i tilsynsloven § 4b ble det også innført en meldeplikt til Finanstilsynet ved inngåelse av avtale om utkontraktering av virksomhet, ved senere endring av slik avtale og ved bytte av oppdragstaker. Meldingen skal gis minst 60 dager før iverksettelsen av avtalen, avtaleendringen eller byttet av oppdragstaker. Ved forskrift 05.06.2015 er det gitt noen mindre unntak fra denne meldeplikten.

1.2 Krav om styrebehandling ved utkontraktering

Verken ovennevnte lovhjemler eller forskrifter inneholder nærmere krav til foretakets saksbehandling før det inngås avtaler om utkontraktering, som i dag følger av de vanlige selskapsrettslige reglene om kompetansefordelingen mellom styret og daglig leder/administrasjonen.

Finanstilsynet foreslår at utkontraktering av IKT-virksomhet eller endring av denne skal behandles av foretakets styre, jf. forslaget til ny § 12 i IKT-forskriften.

I høringsnotatet vises det til at IKT-systemer er blitt en sentral og vesentlig del av særlig bankenes virksomhet, men også generelt for andre institusjoner under tilsyn. Tilsynsvirksomheten har vist til at IT-prosjekter, som etter Finanstilsynets syn har vesentlig betydning for institusjonens virksomhet og risiko, er gjennomført uten medvirkning fra institusjonenes styre eller øverste ledelse.

Det foreslås at styret skal forelegges planer for utkontrakteringen med risikovurdering, og en beskrivelse av hvordan foretakets ansvar for den utkontrakterte virksomheten skal følges opp. Styrets behandling skal sikre at beslutninger om utkontraktering av viktig virksomhet er forankret i foretakets øverste ledelse.

1.3 Finans Norges syn

Finans Norge anser at dersom foretakets styre allerede har vedtatt retningslinjer eller policy for utkontraktering, må det være tilstrekkelig at styret får eventuelle nye avtaler eller endringer i eksisterende til orientering, ikke beslutning, dersom anskaffelsen eller endringen ligger innenfor allerede vedtatte retningslinjer.

Det må uansett innarbeides et vesentlighetskrav for saker som skal forelegges styret. Slik forslaget nå fremstår, må enhver endring, stor eller liten, styrebehandles, noe som vil medføre byråkratisering og ekstraarbeid i virksomheter med mange IKT-avtaler. De samme avtaler skal meldes til Finanstilsynet 60 dager før iverksettelse av avtalen. Dette forsinker prosessen. Dersom en sak som i utgangspunktet skal meldes, først må styrebehandles, vil det forsinke anskaffelsesprosessen ytterligere.

For mindre vesentlige endringer og anskaffelser bør styret ikke involveres. Det er mulig at dette følger av at IKT-forskriften gjelder systemer av betydning for foretaket. På den annen side viser høringsnotatet til bestemmelsene i blant annet finanstilsynslovens § 4 c) om meldeplikt, hvor det ikke er satt noe vilkår om betydelig eller vesentlig. Det vil derfor gjøre bestemmelsen klarere dersom ordet betydelig/vesentlig legges til i forskriftens tekst.

Omnummerering av bestemmelsene i IKT-forskriften:
Forslaget innebærer at § 12 blir til § 11. Finans Norge ser at det er logisk siden § 10 foreslås opphevet. Imidlertid er § 12 innarbeidet i annet lovverk og ikke minst avtaleverk slik at en omnummerering vil måtte medføre mange endringer både i avtaler og offentlig regelverk.

Et alternativ for sikre mindre krav til etterfølgende regelverk- og avtalerevidering er å beholde § 10 som en tom bestemmelse.

2.1 Om forslag til ny forskrift om system- og sikkerhetskrav for betalingstjenester
I ny forskrift om systemer for betalingstjenester foreslås at foretak som tilbyr elektroniske betalingstjenester, skal gjennomføre løpende risiko- og sårbarhetsanalyser. I tillegg foreslås det enkelte minimumskrav til sikkerhet, herunder påloggingsmekanismer, krav til kryptering og betryggende utlevering av identitetskjennetegn. Finanstilsynet mener at den nye forskriften særlig vil ha betydning for nye betalingstjenester og/eller nye tjenesteleverandører.

Finanstilsynet opplyser at kravene er i samsvar med prinsippene som ligger til grunn for den omforente europeiske standarden (SecuRe Pay). Basert på SecuRe Pay, har EBA fastsatt retningslinjer for sikkerhet for internett-betalinger, som vil bli gjort gjeldende fra 1. august 2015.

Forskriftsforslaget retter seg mot foretak som har tillatelse til å tilby betalingstjenester. Dette kan være foretak med norsk konsesjon, eller foretak som driver virksomhet her i riket basert på tilsvarende tillatelse i annen EØS-stat i samsvar med EU-retten. Finanstilsynet legger til grunn at kravene som foreslås, vil omfatte de nevnte norske foretak samt foretak som driver virksomhet i Norge som filial, i samsvar med "general good"- læren.

IKT-forskriftens § 3 inneholder krav om årlig risikovurdering. Det fremlagte forslag til forskrift gjelder kun for betalingssystemer, og går lengre enn IKT-forskriften ved at det kreves løpende risikovurderinger.

2.2 Finans Norges syn

Virkeområdet for IKT-forskriften omfatter også "Systemer for betalingstjenester". Finans Norge oppfatter gjeldende IKT-forskrift § 12, tredje ledd slik at betalingsforetak i formalisert samarbeid med andre kan sikre seg nødvendig og tilstrekkelig kompetanse til å forvalte utkontrakteringsavtaler.

Betalingssystemlovens (bsl) definisjon av "systemer for betalingstjenester" peker ikke på et bestemt foretak. Inngrepshjemmelen etter bsl § 3-3, andre ledd, retter seg mot "den institusjon som driver systemet". Det normale er at grunnlaget for det enkelte foretaks tilbud av betalingstjenester består av et sett av avtaler mellom tilbyderne. Grunnlaget for tilbudet forvaltes av en part som er utpekt i avtalene mellom tilbyderne. I mange tilfeller vil den utpekte part også være ansvarlig for å etablere sentrale felles komponenter som er nødvendige for å kunne oppfylle den funksjonalitet som betalingstjenesten skal inneholde, såkalte FOI-er. For å få gjennomført en betaling som faller inn under "systemer for betalingstjenester", vil det dermed normalt være minst tre aktører involvert – betalers bank, betalingsmottakers bank og den part disse foretak har utpekt til å forvalte avtalene og eventuelle felles operasjonelle komponenter. Dersom foretaket partene har utpekt ikke er et foretak under tilsyn, oppfatter vi at Finanstilsynet likevel har et indirekte tilsyn, jf IKT-forskriftens § 12, andre ledd.

Forslag til ny forskrift om systemer for betalingstjenester retter seg mot foretak som har konsesjon til å tilby betalingstjenester, men ikke mot "Systemer for betalingstjenester". Finans Norge mener derfor at forslaget til ny forskrift ikke i tilstrekkelig grad gjenspeiler hvordan systemer for betalingstjenester reelt sett er innrettet. Betalers bank vil være ansvarlig overfor sin kunde for et betalingsoppdrag inntil det har kommer frem til mottagers bank med angivelse av kreditkontonummer, jfr. Finansavtaleloven § 40,1.ledd. Det enkelte foretak skal ha direkte styring og kontroll på gjennomføringen av sin del av transaksjonsforløpet, samt gjennom avtaler og oppfølging sikre seg kontroll av virksomheten i øvrige aktører og fellesinstitusjoner som inngår i systemet. Tilsvarende vil en fellesinstitusjons oppfølging av deltagerne i systemet skje på grunnlag av avtaler mellom fellesinstitusjonen og deltagerne. Melding til Finanstilsynet etter bsl § 3-2 skal innholde disse avtalene.

Finans Norge mener at ny forskrift med hjemmel i bsl § 3-3 bedre må tilpasses hvordan grunnlaget for det enkelte foretaks tilbud av betalingstjenester er organisert. Etter vårt syn

bør også en ny forskrift, i likhet med IKT-forskriften, gi åpning for at foretaket gjennom et formalisert samarbeid med andre, kan besitte tilstrekkelig kompetanse til å forvalte utkontrakteringsavtaler. Det er likevel foretakene med konsesjon som er ansvarlig for at systemet for betalingstjenesten innrettes i tråd med offentlige krav.

Finanstilsynet opplyser at forslaget til ny forskrift også vil ivareta retningslinjer for internettbetalinger som EBA har utarbeidet og som ble gjort gjeldende fra 01.08.2015. Dekningsområdet for EBAs retningslinjer er imidlertid ikke sammenfallende med bsl sin definisjon av systemer for betalingstjenester. Definisjonen i bsl vil inkludere flere typer betalingstjenester enn EBAs retningslinjer. Eksempelvis vil betalinger via telefon (Telegiro) og mobilbetalinger som ikke er basert på browser-teknologi, ikke være omfattet av EBAs retningslinjer, men vi oppfatter at slike tjenester vil omfattes av Finanstilsynets forslag til ny forskrift. Finans Norge mener forskriften bør endres slik at dekningsområdet er sammenfallende med EBAs retningslinjer, slik at begrepet ”telenett” tas ut og forskriften dermed kun omhandler betalingstjenester tilgjengelig over internett.

Finans Norge tar til orde for en klargjøring av forslaget til ”*løpende* risiko- og sårbarhetsanalyser” i forskriftsutkastets § 2. EBAs retningslinjer (punkt 4) krever at ROS-analyser skal foretas periodisk og ved større endringer eller hendelser. Disse retningslinjene kan vi slutte oss til. IKT-forskriftens § 3 vil etter det vi forstår gjelde parallelt, slik at den årlige vurderingen da uansett må gjennomføres. Foretakets løpende sikkerhetsovervåking er foreslått regulert i forskriftsutkastets § 3 siste setning.

I følge forslaget til § 3, første ledd, andre punktum, skal foretaket følge gjeldende nasjonale og internasjonale standarder for å sikre konfidensialitet, integritet og tilgjengelighet. Det finnes en rekke ”standarder” på området og på ulike nivåer. Det er ikke alltid samsvar mellom standardene. Det er uklart hvilke standarder foretakene vil være pålagt å følge. Finans Norge kan heller ikke se at det kan være riktig å peke på en spesifikk standard. Vi forslår at setningen utgår.

For foretak som tilbyr samordnede betalingstjenester i samarbeid med andre foretak vil det ikke være mulig alene å beskytte tjenesten i sin helhet (ende til ende), jf forslagets § 3 andre ledd. Vi vil i denne sammenheng vise til EBAs retningslinjer punkt 11.2 der det er oppført at foretaket ”should *ensure* that …. end-to-end encryption is applied beetween the communicating parties…”. Etter EBAs retningslinjer bør således foretaket *forsikre* seg om at tjenesten beskyttes ende til ende. Vi foreslår at en slik formulering også benyttes i forskriften.

På side 6 i høringsnotatet under ”Krav til betalingsløsninger betjent av kunde” i 4. avsnitt omtales krav til foretaket om overvåkning og *måling* av trafikk. Dette kravet finner vi igjen i forskriftsutkastets § 3*: ”*Foretaket skal overvåke og *måle* trafikk for betalingstjenester for å

kunne avdekke og hindre uautorisert bruk.” At foretaket skal overvåke trafikken er vi enige i, men vi er usikre på hva som ligger i begrepet ”måle”.

Finans Norge antar at forslaget til bestemmelse i § 3, tredje ledd om sikker påloggingsmekanisme retter seg mot kundens betalingstjenesteleverandør og da ved kundens pålogging til tjenesteleverandørens egne tjenester, som for eksempel nettbank. Vi er likevel usikre på dette og viser til høringsnotatets antydning om at nettbutikker som ikke har 2-faktor identifisering vil måtte tilpasse seg indirekte som følge av krav til foretakene som omfattes av forslaget. Først når EBAs retningslinjer blir en realitet for netthandel gjennom hele Europa kan betalingstilbyderen imøtekomme et slikt krav også for grensekryssende transaksjoner innen EØS. Fortsatt vil det imidlertid kunne operere betydelige netthandelsbutikker utenfor Europa som ikke vil ha tilpasset seg 2-faktor identifisering. Finans Norge kan vanskelig se hvordan en utsteder av kort i internasjonale (globale) kortordninger skal kunne forsikre seg om at utstedte kort bare kan anvendes i nettbutikker som har systemer som sikrer en 2-faktor identifisering.

I høringsnotatet peker Finanstilsynet på at tilbydere som bare har betalingskort med magnetstripe må heve sitt sikkerhetsnivå. Vi er usikre på om Finanstilsynet med dette mener at utstedere av kort som bare har magnetstripe må endre kortteknologi. Vi er også usikre på om dette kravet innebærer at foretak som er innløsere for brukersteder i Norge ikke lengre vil kunne innløse transaksjoner fra kort som bare har magnetstripe.

Begrepene ”påloggingsmekanisme” og ”identitetskjennetegn” i utkastets § 3 er ikke definert. Finans Norge antar at det med ”identitetskjennetegn” menes sikkerhetsmekanismer (”security credentials”) som kunden skal benytte, men det er ikke åpenbart av tekstforslaget. Vi foreslår at begrepene defineres.

Avslutningsvis vil Finans Norge få knytte noen kommentarer til den generelle teksten i høringsnotatet:

- På side 5 uttaler Finanstilsynet: ”Det har imidlertid vist seg, blant annet gjennom erfaring fra tilsynsvirksomheten, at det ikke i tilstrekkelig grad er etablert kontroll med etterlevelse av selvreguleringen (Blåboka)”. Finans Norge stiller seg noe spørrende til denne uttalelsen. Mener Finanstilsynet at bankene selv ikke har gode nok oppfølgings- og kontrollrutiner for sin egen deltagelse i betalingstjenester som faller inn under ”Blåboka”? Eller er det Finanstilsynets oppfatning at fellesinstitusjoner som forvalter selvreguleringen (som Finans Norge og BSK) ikke har etablert tilstrekkelige systemer og rutiner som sikrer at deltagerne etterlever nedfelte krav i næringens eget regelverk?

  Næringens felles regler inneholder ikke bestemmelser som gir Finans Norge eller BSK

hjemler til å foreta tilsyn hos bankene. Manglende etterlevelse av avtaler og regelverk avdekkes ved at "banken i den andre enden" opplever forringelse i den kvalitet denne kan levere til sine kunder. Manglende etterlevelse av standarder avdekkes i utvekslingen mellom bankene. Transaksjoner som ikke er i henhold til standarder avvises. En bank kan også oppleve tap/misbruk som følge av at en annen bank ikke følger sikkerhetskrav. Brudd på sikkerhetskrav følges straks opp av BSK.

Det er Finans Norges oppfatning at samfunnet generelt opplever at betalingstjenestene som faller inn under "Blåboka" gjennomgående er av god kvalitet, har høy operasjonell stabilitet og er sikre i bruk. Vi vil tro at også Finanstilsynets IKT-forskrift har vært medvirkende til foretakenes fokus på operasjonell stabilitet. Vi reiser heller ikke innvendinger til at Finanstilsynet på en hensiktsmessig måte implementerer EBAs retningslinjer i Norge.

- På side 6 i høringsnotatet slår Finanstilsynet fast at "Foretaket skal også sikre at mobile betalingsløsninger skal ha minst tilsvarende sikkerhet som for tradisjonelle nettbaserte løsninger". En slik bestemmelse finner vi ikke igjen i forskriftsutkastets tekst. Finans Norge ønsker å påpeke at mobile betalingstjenester har et tjenesteinnhold som kan være begrenset sammenlignet med nettbank. Det er derfor etter vårt syn neppe hensiktsmessig å kreve at mobile betalingstjenester skal ha minst samme sikkerhet som tradisjonelle nettbaserte løsninger. Den ROS-analyse som foretaket skal gjennomføre ved innføring av nye tjenester, og de risikoreduserende tiltak foretaket gjennomfører som følge av ROS-analysen, bør etter Finans Norges vurdering være avgjørende for hvilket teknisk sikkerhetsnivå nye løsninger skal ligge på, uavhengig av om de er mobile eller nettbaserte.

Med vennlig hilsen
Finans Norge

Tor Johan Bjerkedal
Fagdirektør

Anne Ystenes
Seniorrådgiver