FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Styret i Vipps AS
Postboks 9236 Grønland
0134 OSLO

VÅR REFERANSE	DERES REFERANSE	UNNTATT OFFENTLIGHET	DATO
18/8139		Offl. § 13 1. ledd, jf. fvl. § 13 1. ledd nr. 2 Merkede avsnitt er unntatt offentlighet	24.07.2019

Merknader - endelig rapport

Finanstilsynet gjennomførte stedlig tilsyn i Vipps AS 8. og 9. oktober 2018 (på det tidspunktet VBB AS). Tilsynet hadde som formål å vurdere hvordan Vipps AS administrerer, utvikler, forvalter, drifter og sikrer betalingstjenesten Vipps, med spesiell oppmerksomhet rettet mot funksjonaliteten i Vipps, drift av IKT-systemene som understøtter Vipps og styring og kontroll av risikoen for hvitvasking og terrorfinansiering ved bruk av Vipps.

Til grunn for disse merknadene ligger Finanstilsynets foreløpige rapport datert 5. februar 2019 og styrets kommentarer til rapporten i brev av 3. mai 2019.

Finanstilsynet har følgende merknader etter det stedlige tilsynet:

Forhold knyttet til styring og kontroll med opplysningsplikt og kundens valg ved ny funksjonalitet.

Kundens valg ved ny funksjonalitet i Vipps

Finanstilsynet påpekte i foreløpig rapport at Vipps må informere kundene tydeligere om ny funksjonalitet i tjenesten, kvalitetssikre informasjonen til kundene om tjenesten, gi kunden valget om den vil ta ny funksjonalitet i bruk eller ikke, og sikre at det er mulig for kunden å skru av ny funksjonalitet. Finanstilsynet har fra styrets svar merket seg at foretaket gjør en vurdering før lansering av ny funksjonalitet, om foretaket skal kreve kundens aktive samtykke for å ta i bruk den nye funksjonaliteten eller kunden skal gis mulighet for å slå av funksjonaliteten. Finanstilsynet fastholder at funksjonalitet som påvirker kundens betalinger som hovedregel skal kreve kundens aktive samtykke før den tas i bruk.

Beløpsgrense

Finanstilsynet stilte i foreløpig rapport spørsmål ved Vipps beløpsgrense for venne-betalinger. Finanstilsynet har merket seg foretakets redegjørelse for beløpsgrenser for vennebetalinger og tar dette til etterretning.

Forhold knyttet til styring og kontroll med drift og beredskap.

Redundans

FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

Telefon 22 93 98 00
Telefaks 22 63 02 26

post@finanstilsynet.no
www.finanstilsynet.no

Saksbehandler
Åshild Johnsen
Dir. tlf 22 93 97 02

Finanstilsynet ba i foreløpig rapport foretaket redegjøre for valgt kontinuitetsløsning for Vipps og hvordan risikoen ved denne er vurdert. Finanstilsynet har merket seg foretakets beskrivelse av valgt driftsløsning som består av en aktiv installasjon og en passiv installasjon. Hver av disse har innebygget redundans og er lokalisert i to ulike geografiske regioner. Finanstilsynet tar dette til etterretning.

Vipps' avhengighet av driftsstabilitet hos andre leverandører
Finanstilsynet anbefalte i foreløpig rapport at Vipps kartlegger og dokumenterer hvilke konsekvenser ulike avbruddsscenarier hos ulike leverandører har for tjenestene og hvilke innebygde reserveløsninger som finnes. Finanstilsynet tar til etterretning Vipps sin vurdering av at Vipps venne-betaling med straks-betaling fra konto og betaling med kort ikke er likeverdige alternativer pga. tidsforskjellen for når pengene er tilgjengelige på mottakers konto. Finanstilsynet har merket seg Vipps' beskrivelse av pågående aktiviteter for å minimere påvirkningen på Vipps ved driftsavbrudd hos leverandørene, og tar dette til etterretning.

Avstemming av beredskapsplaner- og tester med leverandørene
Finanstilsynet anbefalte i foreløpig rapport foretaket å avstemme beredskapsplanen for Vipps med beredskapsplanene for de viktigste leverandørene og vurdere å gjennomføre felles beredskapstester med leverandørene. Finanstilsynet har merket seg foretakets redegjørelse for oppdatering av beredskapsplan og for gjennomførte og planlagte øvelser sammen med leverandører. Finanstilsynet tar dette til etterretning.

Forhold knyttet til styring og kontroll av applikasjons- og driftssikkerhet.

Tilgangsstyring
Finanstilsynet påpekte i foreløpig rapport at dokumentasjonen av foretakets rutiner for tilgangsstyring var inkonsistente og uferdige. Av styrets svar fremkommer det at foretaket har implementert rammeverket for tilgangsstyring som ble presentert på møtet, men at det gjenstår å ferdigstille standarder og detaljerte rutiner, og å etablere kontrollmekanismer for bruk av disse. Finanstilsynet forventer at standarder og rutiner for tilgangsstyring ferdigstilles senest 1. oktober 2019 og ber om en bekreftelse når arbeidet er sluttført.

Beskyttelse av data
Finanstilsynet ba i foreløpig rapport foretaket regelmessig vurdere nivået på kryptering av data målt mot tilgangene for ansatte hos driftsleverandøren. Finanstilsynet har fra styrets svar notert seg at foretaket vurderer nivået på kryptering av data som tilfredsstillende og at beskyttelse av data er gjenstand for foretakets kvartalsvis risikovurdering. Finanstilsynet tar dette til etterretning.

Sikkerhet i design- og applikasjonsutvikling

[redacted]

Av styrets svar har Finanstilsynet merket seg tiltak foretaket har iverksatt for å styrke sikkerhetsarbeidet i de ulike fasene av systemutviklingen. Blant annet er bruken av ulike typer sikkerhetstester både før og etter implementering utvidet. Finanstilsynet forventer at foretaket opprettholder høy oppmerksomhet og ressursbruk på dette området.

Forhold knyttet til styring og kontroll av risikoen for hvitvasking og terrorfinansiering.

AML-risikoanalyse
Finanstilsynet har merket seg at AML-risikoanalysen ble behandlet på styremøte i november 2018 og har notert seg at foretaket har utvidet risikoanalysen med beskrivelse av hvilke forhold som utløser forsterkede kundetiltak. Finanstilsynet tar dette til etterretning.

Stillingsinstruks for hvitvaskingsansvarlig
Finanstilsynet har merket seg og tar til etterretning at rollebeskrivelsen for hvitvaskingsansvarlig er etablert og godkjent av styret.

AML-rapportering til styret
Finanstilsynet har merket seg og tar til etterretning at foretaket fra Q1 2019 har inkludert rapportering på AML i den kvartalsvise rapporteringen til styret.

Kundetiltak
Finanstilsynet påpekte i foreløpig rapport at verken for Vipps' sluttbrukere eller brukersteder innhentes og vurderes "nødvendige opplysninger om kundeforholdets formål og tilsiktede art" i henhold til krav i hvitvaskingsloven. I styrets tilsvar vurderer foretaket at dagens bruksmuligheter i Vipps innebærer at sluttbrukers valg av tjenester i Vipps i seg selv er tilstrekkelig beskrivende for "kundeforholdets formål og tilsiktede art", og at dette vurderes fortløpende ved introduksjon av ny funksjonalitet. Hvitvaskingslovens § 12 (5) og § 13 (5) fastsetter et obligatorisk risikobasert kundetiltak for alle typer kunder som innebærer at "Rapporteringspliktige skal innhente og vurdere nødvendige opplysninger om kundeforholdets formål og tilsiktede art". Tiltaket innebærer at rapporteringspliktig foretak utfra sin risikobaserte analyse og vurdering skal innhente og vurdere nødvendige opplysninger om kunden. For kunder med lav risiko for hvitvasking og terrorfinansiering, som har et regelmessig og forutsigbart transaksjonsmønster, er det tilstrekkelig at formålet med kundeforholdet angis generelt, for eksempel "betalingsformidling". For kundeforhold med høy, eller forhøyet risiko for hvitvasking og terrorfinansiering, skal det innhentes og vurderes mer detaljerte opplysninger om kundeforholdet utfra en risikobasert vurdering. Finanstilsynet anser at kundeforholdets formål og art vil være selvforklarende for mange kunder som anvender tjenesten til enkle og lave pengeoverføringer. For andre kunder, og da særlig de som anvender tjenesten i næringsøyemed og/eller overfører mer betydelige summer, er foretaket i brudd med §§ 12(5) og 13(5). Hvis Vipps utvides med funksjonalitet, for eksempel å gjennomføre grensekryssende transaksjoner, vil det utløse krav om innhenting og vurdering av "nødvendige opplysninger om kundeforholdets formål og tilsiktede art" før sluttbruker tar slik funksjonalitet i bruk. Finanstilsynet forventer at foretaket innhenter og vurderer "nødvendige opplysninger om kundeforholdets formål

og tilsiktede art" for alle kundeforhold som ikke oppfyller lovpålagte krav. Dette arbeidet bør gis høy prioritet. Finanstilsynet ber om å bli informert om status for dette innen 1. oktober 2019.

ID-verifisering av resterende portefølje

Finanstilsynet har merket seg og tar til etterretning, at fra starten av Q2 2019 er alle sluttbrukere over 15 år ID-verifisert med BankID.

Screening mot PEP- og sanksjonslister

Finanstilsynet avdekket under tilsynet meget alvorlige brudd på kravene knyttet til frysbestemmelsene i sanksjons- og tiltaksforskriftene, ved at foretaket ikke kontrollerte kunder eller transaksjoner mot internasjonale sanksjonslister. Det forelå heller ikke systemer for å identifisere politisk eksponerte personer (PEPs). Finanstilsynet har fra styrets svar merket seg at screening av sluttbrukere mot PEP- og sanksjonslister ved kundeetablering og gjennom daglig screening av kundebasen, ble implementert i november 2018. Fra styrets svar har Finanstilsynet merket seg at screening av brukersteder og rolleinnehavere mot PEP- og sanksjonslister ved kundeetablering og gjennom daglig screening av bedriftskundebasen først vil være ferdig etablert ved utgangen av Q2 2019. Finanstilsynet legger til grunn at Vipps gjennomfører screening av brukersteder og rolleinnehavere mot PEP- og sanksjonslister ved kundeetablering og gjennom screening av bedriftskundebasen hver gang det gjøres endringer på sanksjonslistene. Finanstilsynet forventer at dette er på plass innen 30. juni 2019, og ber om foretakets bekreftelse når det er gjennomført.

Brudd på egne retningslinjer for oppgjørskonto

Finanstilsynet har merket seg at for brukersteder i Vipps må oppgjørskonto eies av den juridiske enheten som har inngått Vipps brukerstedsavtalen, men med unntak for enkeltmannsforetak som kan benytte privat bankkonto som oppgjørskonto. Finanstilsynet tar dette til etterretning.

Ressurser på AML-området

Finanstilsynet viste i foreløpig rapport til at styret bør vurdere om enheten skal tilføres ytterligere ressurser for etterlevelse av hvitvaskingsregelverket og tiltak mot terrorfinansiering, herunder finansielle sanksjoner og frysforpliktelser. Fra styrets svar har Finanstilsynet notert seg at foretaket fortløpende vurderer behovet for ressurser på AML-området, og i rekruttering til AML-oppgaver legger vekt på å sikre bred kompetanse. Med bakgrunn i Vipps' økende produkt- og kundeportefølje og planlagte internasjonale satsing, forventer Finanstilsynet en økt ressursinnsats for å følge opp regelverket med tiltak mot hvitvasking og terrorfinansiering.

Kopi av dette brevet bes sendt til ekstern og intern revisor.

For Finanstilsynet

Olav Johannessen
seksjonssjef

Åshild Johnsen
tilsynsrådgiver

Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.