



Styret i Vipps AS
Postboks 9236 Grønland
0134 OSLO

VÅR REFERANSE
21/808

DERES REFERANSE

DATO
20.10.2021

Tilsynsrapport

Finanstilsynet gjennomførte stedlig tilsyn i Vipps AS 17. – 18. mars 2021. Samtalene ble gjennomført på digital plattform som følge av smitteverntiltak. Tilsynet var ledd i Finanstilsynets risikobaserte tilsynsvirksomhet. Formålet med tilsynet var å vurdere foretakets styring og kontroll av virksomheten, herunder av samfunnsviktige/-kritiske funksjoner. Videre ble foretakets arbeid siden stedlig tilsyn i 2018 når det gjelder forebygging av hvitvasking og terrorfinansiering fulgt opp.

Til grunn for tilsynsrapporten ligger Finanstilsynets foreløpige tilsynsrapport datert 25. juni 2021 og foretakets kommentarer til denne i brev av 15. september 2021.

Finanstilsynet har følgende merknader etter tilsynet:

1 OVERORDNEDE FORHOLD

1.1 Forretningsmodell og strategiske valg

Finanstilsynet noterte i foreløpig tilsynsrapport at Vipps ser seg som en ledende aktør innen betaling og autentisering/signering. Foretaket har svært høy markedsdekning innenfor virksomhetsområdene Vipps lommebok, BankID og BankAxept i Norge. Ambisjonene om vekst og konsolidering i Norden innebærer et betydelig investeringsbehov i et marked preget av store internasjonale aktører. Inntekspotensialet skal utvides ved å gå internasjonalt og ved å legge til verdiøkende tjenester. Det er inngått en rekke samarbeidsavtaler, herunder for å understøtte den internasjonale satsingen, og foretaket har utkontraktert vesentlige forretningsystemer til eksterne leverandører. Foretaket har også etablert et datterforetak (Vipps Mobil AS) for å tilby "Norges enkleste mobilabonnement".

Finanstilsynet ba i foreløpig tilsynsrapport om styrets kommentar til planene om ekspansjon utenfor Norge samt en redegjørelse av status for de viktigste samarbeidsavtalene og for virksomheten i Vipps Mobil AS.

Styret viser i sitt svar til avtalen av 30. juni 2021 om å slå sammen lommeboken i Vipps med tilsvarende virksomhet i Danmark og Finland, og er av den oppfatning at en sammenslåing vil gi et sterkt fundament for å stå imot den stadig økende konkurransen fra internasjonale aktører. Med en samlet kundebase i Norden på over 11 millioner sluttbrukere vurderer styret at selskapet vil stå i en unik posisjon for å ta den ledende posisjonen for netthandel i Norden. Styret viser også til at samlet transaksjonsvolum vil skape grunnlag for betydelig lavere kostnader på blant annet transaksjoner i Norden. Finanstilsynet legger til grunn at målet om å ta den ledende posisjonen for netthandel også

innebærer en forventning om vesentlig økte inntekter for foretaket, og ser dette som en forutsetning for at foretaket skal lykkes på sikt.

Når det gjelder viktige samarbeidsavtaler, viser styret til at det ikke er endringer i hverken BankAxept deltakeravtalen eller distribusjonsavtalen med bankene, men at distribusjonsavtalene skal reforhandles innen utgangen av året. Intensjonen med samarbeidsavtalen som ble inngått med Visa høsten 2020 var å utvikle en felles internasjonal mobil lommebok med Vipps som leverandør og Visa som leverandør av infrastruktur. Finanstilsynet noterer fra styrets svar at utfordringer med å finne en felles forretningsmodell og avtalen om å slå sammen lommeboken i Vipps med tilsvarende virksomhet i Danmark og Finland, gjør at avtalen i større grad blir en avtale om infrastruktur. *Finanstilsynet ber om at foretaket informerer Finanstilsynet dersom det inngås nye samarbeidsavtaler.*

Virksomheten i Vipps Mobil AS ble lansert i oktober 2020, og er i etableringsfasen. Styret viser til at foretaket kommer til å vurdere utviklingen av kundemassen og markedet fortløpende, for å identifisere egnede tiltak for å oppnå ønsket markedsposisjon.

1.2 Økonomi og soliditet

Finanstilsynet viste i foreløpig tilsynsrapport til at foretakets forventede inntekter i 2020 ble lavere enn forventet som følge av koronapandemien og at flere forhold bidro til vesentlige ekstrakostnader. Stadige utsettelse av migreringen til ny driftsleverandør for BankID (prosjekt Fiducia) var, og er fortsatt, en årsak til store ekstrakostnader. Foretakets underskudd i 2020 ble likevel vesentlig lavere enn et år tidligere, og foretaket viste til at denne utviklingen skal fortsette ved å redusere konsulentkostnader samt å ha større oppmerksomhet fra ledelsen på at innovasjon og nye produkter og tjenester som utvikles har tilstrekkelig inntekspotensial.

Finanstilsynet ba i foreløpig rapport om styrets vurdering av foretakets kapitalbehov, jf. finansforetaksloven § 13-6 første ledd. Styret viser i tilsvaret til at det vurderer at foretakets soliditet er god og at kapital situasjonen er tilfredsstillende.

Finanstilsynet viste i foreløpig tilsynsrapport til at Finansdepartementets vedtak av 14. juni 2018 om tillatelse til sammenslåing av Vipps AS, BankAxept AS og BankID Norge AS inneholdt et vilkår om at foretaket skal beregne kravet til ansvarlig kapital etter den metode i finansforetaksforskriften § 14-4 som til enhver tid gir det høyeste beløpet. Finanstilsynet vurderte i foreløpig tilsynsrapport at endringen i beregningsmetode som foretaket gjennomførte per fjerde kvartal 2019 bryter med dette vilkåret. Endringen førte til at foretakets beregnede kapitalkrav ble redusert fra 29 millioner per andre kvartal 2019 til 13 millioner per utgangen av 2019. Finanstilsynets viste samtidig til at endringen ble kommunisert svært mangelfullt og først ved utløpet av fristen for rapporteringen.

Styret viser i sitt svar på foreløpig tilsynsrapport til at foretaket har hatt dialog, både på e-post og telefonisk, med Finanstilsynet i god tid før endringen, og at det var foretakets forståelse at Finanstilsynet hadde akseptert endringen. Styret viser for øvrig i sitt svar til at styrets vurdering er at foretaket har lagt til grunn det strengeste kravet i beregningen. Styret viser i den sammenheng til at beregningen av foretakets kapitalkrav etter tidligere anvendte metode har medført lavere kapitalkrav etter at foretaket har lagt til grunn myndighetenes føringer for hva som kan sies å være faste kostnader, gitt i forskrifter som ble vedtatt som koronatiltak for næringslivet.

Finanstilsynets syn er at dialogen foretaket viser til å ha hatt med Finanstilsynet om kapitalkrav i hovedsak har vært av rapporteringsteknisk karakter og om rettidig rapportering. Tilleggsmerknaden i foretakets e-post den 31. mars 2020 om at kapitalkravet per 31. desember 2019 var beregnet etter

ny metode kan på ingen måte ses som en anmodning om godkjenning av å anvende en ny beregningsmetode eller fravike fusjonsvilkåret av 14. juni 2018. Finanstilsynet opprettholder dermed vurderingen av at foretaket har brutt konsesjonsvilkåret for beregning av kapitalkravet. Det fremstår dermed uklart for Finanstilsynet i hvilken grad foretaket har overholdt minstekravet til kapitaldekning i perioden frem til ny kapital ble betalt inn i slutten av juni 2021. Finanstilsynet ser heller ikke at styrets henvisning til myndighetenes midlertidige koronatiltak om å få dekket faste kostnader har direkte relevans i saken. I tillegg til at myndighetstiltakene det vises til har et annet formål, ble forskriften også publisert etter at foretakets revisjonsutvalg behandlet saken om endring av beregningsmetode den 24. mars 2020.

Finanstilsynet vurderer det som kritikkverdig at foretaket ikke har etterlevd fusjonsvilkåret i Finansdepartementets vedtak av 14. juni 2018. *Finanstilsynet legger til grunn at foretaket retter seg etter kravet om å beregne kapitalkravet etter den metoden i finansforetaksforskriften § 14-4 som til enhver tid gir det høyeste beløp og ber om en bekreftelse på dette innen 15. november 2021.*

Finanstilsynet forventer for øvrig at styret påser at foretaket har en kapitalisering som til enhver tid som et minimum er i samsvar med lovens krav og at kapitaliseringen står i forhold til foretakets planlagte virksomhet fremover.

1.3 Organisering – hvitvaskingsansvarlig og uavhengig kontrollfunksjon for etterlevelse

Etter hvitvaskingsloven § 8 (5) skal det utpekes en person i ledelsen som skal ha et særskilt ansvar for å følge opp rutinene som er vedtatt for å sikre at virksomheten håndterer identifisert hvitvaskingsrisiko og for at plikter etter bestemmelser i eller i medhold av hvitvaskingsloven oppfylles. Hvitvaskingsansvarlig skal ha direkte rapporteringslinje til styret og øverste ledelse ved behov, og har ansvaret for at rutiner implementeres og etterlevs i virksomheten. Hvitvaskingsloven § 35 (2) har krav om at det utnevnes en etterlevelsesansvarlig for å påse at hvitvaskingsregelverket overholdes dersom en risikovurdering av virksomhetens omfang og art tilsier det. Finanstilsynets rundskriv 8/2019 utdyper i kapittel 3 forventninger til organisering og ansvarsfordeling. For finansforetak som har krav om en uavhengig kontrollfunksjon for etterlevelse (compliance), følger det av Finanstilsynets veileder til hvitvaskingsloven (rundskriv 8/2019) punkt 3.2.1 at hvitvaskingsansvarlig som utgangspunkt bør være plassert i førstelinje. Alternativt må foretaket ha en dokumentert, risikobasert begrunnelse for at dette ikke gjøres, herunder med vurderinger av risikoene som kan oppstå ved at andrelinjen følgelig vil kontrollere eget arbeid. Som betalingsforetak er Vipps unntatt fra kravet om uavhengige kontrollfunksjoner etter finansforetaksloven § 13-5 (2). Foretaket er imidlertid vurdert å ha et omfang og en art som i henhold til hvitvaskingsloven § 35 annet ledd bokstav a tilsier at det må utnevnes en etterlevelsesansvarlig.

Kontrollfunksjonen for etterlevelse bør organiseres på en slik måte at evnen til å utføre oppgavene på en objektiv og uavhengig måte ikke kan påvirkes av enhetene som skal overvåkes. Kontrollfunksjonen bør ha mulighet til å rapportere direkte til styret i tilfeller der styret ellers ikke får nødvendig informasjon om vesentlige risikoer via den alminnelige rapporteringen. Finanstilsynet forventer videre at funksjonen har tilstrekkelig kompetanse og ressurser, at leder for funksjonen er innplassert tilstrekkelig høyt i organisasjonshierarkiet og med tilstrekkelig formell og faktisk status internt i foretaket. Etter rundskrivets punkt 3.3 skal etterlevelsesansvarlig gjennomføre kontroller og vurderinger for å påse at virksomheten overholder hvitvaskingsregelverket og om tiltakene som iverksettes for å avhjelpe eventuelle mangler er effektive. Kontrollfunksjonen bør også bidra med råd og anbefalinger. Med bakgrunn i virksomhetens art og omfang forventer Finanstilsynet at foretaket har etablert en uavhengig

kontrollfunksjon med ansvar for etterlevelse som strekker seg ut over hvitvaskingsområdet. Finanstilsynet forventer videre at styring av øvrige operasjonelle risikoer overvåkes av den uavhengige kontrollfunksjonen samt at funksjonen vurderer hensiktsmessigheten og effektiviteten i foretakets internkontroll.

Foretaket har etablert én kontrollfunksjon med ansvar for både risikostyring og etterlevelse. Leder for risikostyring og etterlevelse, som rapporterer til foretakets CFO, er også utpekt som foretakets hvitvaskingsansvarlig. For å bøte på interessekonflikter ved at rollene som hvitvaskingsansvarlig og etterlevelsesansvarlig kombineres er foretakets CFO utpekt som etterlevelsesansvarlig på hvitvaskingsområdet.

Finanstilsynet vurderte i foreløpig tilsynsrapport at iboende interessekonflikter mellom CFO-rollen og rollen som uavhengig etterlevelsesansvarlig på hvitvaskingsområdet gjør kombinasjonen av disse rollene uheldig. Finanstilsynet vurderte videre at foretakets iverksatte tiltak for å forebygge interessekonfliktene ikke adresserer det underliggende behovet for å etablere et klart skille og tydelig uavhengighet mellom enhetene i henholdsvis første og andre linje. Foretaket bør vurdere å organisere hvitvaskingsansvaret som del av foretakets førstelinje. Det ble også pekt på at foretaket har en betydelig nøkkelpersonrisiko som bør følges opp og reduseres.

Finanstilsynet noterer fra styrets svar at en organisering og ansvarsfordeling der man unngår at enkelte personer har roller i både første og andre linje vurderes å være optimal. Styret viser til at foretaket fortløpende vil evaluere ressursbehovet, både i første og andre linje, basert på blant annet virksomhetens vekst, kompleksitet og nye satsningsområder. Styret opplyser videre at endringer som følge av den planlagte sammenslåingen av flere nordiske lommebokselskaper og utskillelsen av BankAxept og BankID, gjør det naturlig å vurdere den fremtidige organiseringen av antihvitvaskingsarbeidet i både første og andre linje. Styret viser også til at reduksjon av nøkkelpersonrisiko vil være prioritert i arbeidet med et nytt organisasjonsoppsett.

Finanstilsynet tar styrets svar til etterretning.

2 FORHOLD KNYTTET TIL RISIKOSTYRING OG INTERNKONTROLL

2.1 Beredskaps- og krisehåndtering

Finansforetak skal etter finansforetaksloven § 13-5 (1) ha hensiktsmessige retningslinjer og rutiner for å identifisere, styre overvåke og rapportere risiko foretaket er, eller kan bli, eksponert for. Videre skal foretak etter IKT-forskriften § 11 ha en dokumentert kriseplan som skal iverksettes dersom IKT-driften ikke kan opprettholdes som følge av en krise. Finanstilsynet forventer at finansforetak vedtar retningslinjer og etablerer planverk for å håndtere alle typer kriser som kan være til hinder for virksomhetens drift og for kritiske funksjoner i særdeleshet.

Vipps har utarbeidet en beredskapsplan for foretaket som består av en administrativ del, også omtalt som policy, og en operativ del. Vipps har også utarbeidet en egen kriseplan for samarbeidet om BankID. For virksomhetsområdene BankAxept og BankID har foretaket ansvar for krise- og avvikshåndtering på vegne av bankene og har forpliktet seg til å etterleve kravene knyttet til driftsavbrudd og krisehåndtering i IKT-forskriften for disse virksomhetsområdene. Videre ble det i forbindelse med fusjonen med BankAxept og BankID stilt som vilkår for konsesjonen at Vipps måtte utarbeide en særskilt beredskapsplan for videreføring av samfunnskritiske funksjoner.

Finanstilsynet pekte i foreløpig tilsynsrapport på at foretaket ikke hadde vedtatt retningslinjer for beredskap og krisehåndtering i et eget styringsdokument, men at en administrativ del i én av foretakets kriseplaner ble omtalt som policy. Deler av beskrivelsene i denne delen var overlappende

med øvrige av foretakets kriseplaner, og Finanstilsynet vurderte at det kan være hensiktsmessig om den administrative delen av foretakets beredskapsplan skilles ut og gjøres til et overordnet styringsdokument for beredskap og krisehåndtering. Det ble i denne sammenheng også pekt på viktigheten av at det som grunnlag for planene gjennomføres grundige risikoanalyser av hvordan ulike krisescenarier kan påvirke kritiske funksjoner i virksomheten. Finanstilsynet pekte også på noe manglende oppdatering og presiseringer i beredskapsplanen for BankID, blant annet knyttet til beredskapsledelse. Det ble understreket at gjeldende planer må gjenspeile faktiske forhold, og at innfasing av endringer må hensyntas tidsriktig i planene. Finanstilsynet understreket også at Vipps må ha en operativ beredskapsplan for BankID som man vet vil fungere i en krise, og at dette testes tilstrekkelig og verifiseres.

Finanstilsynet noterer fra styrets svar at foretaket vil følge anbefalingen om å vedta en overordnet retningslinje for beredskap og krisehåndtering. Foretaket vil i henhold til styrets svar også igangsette et prosjekt for å analysere og vurdere hvordan mulige krisescenarier vil kunne påvirke kritiske funksjoner i virksomheten. Styret vil videre sikre at det gjennomføres tilstrekkelig hyppige øvelser av beredskapsplanene samt at planene på de ulike nivåene er avstemt.

Fra styrets svar går det også frem at styret vil påse at foretaket gjenopptar dialogen med Bits når det gjelder vilkåret om å utarbeide en særskilt beredskapsplan for videreføring av samfunnskritiske funksjoner. Arbeidet med blant annet avtaleendringer og kriseavviklingstiltak vil bli gjenopptatt så snart dette blir mulig etter at migrering til ny driftsleverandør for BankID er avsluttet.

Finanstilsynet tar styrets svar til etterretning. Migreringsprosjektet følges opp i separat sak.

2.2 Produkt- og tjenesteutvikling

Etter forskrift om risikostyring og internkontroll § 6 første ledd skal det foreligge en risikovurdering før vesentlige endringer eller nye produkter og rutiner etableres. I tråd med nevnte bestemmelse og med finansforetaksloven § 13-5 legger Finanstilsynet til grunn at finansforetak etablerer en særskilt prosess for risikovurderinger og godkjenning av nye produkter, tjenester og andre vesentlige endringer før slike lanseres. Det forventes at relevante ressurser fra både forretnings- og støttefunksjoner i første linje samt fra uavhengige kontrollfunksjoner involveres i prosessen og at vurderingene dokumenteres og arkiveres.

I henhold til foretakets policy for risikostyring og internkontroll skal det gjennomføres risiko- og kontrollvurderinger før større lanseringer, ved endringer av betydning og ved hendelser. Foretaket har etablert og dokumentert en særskilt prosess for produktutvikling hvor det legges vekt på at risikovurderinger gjennomføres med et helhetlig perspektiv, at det involverer bredt og at risikovurderingene starter tidlig i prosessen. Finanstilsynet vurderte at risikostyrings- og compliance-funksjonen har en sentral rolle i risikovurderingene. Foretaket har også vedtatt og dokumentert en egen "Gå-til-marked"-prosess med egen sjekkliste for oppgaver og ansvarsfordeling. Prosessbeskrivelsene tar utgangspunkt i prinsippene i foretakets vedtatte policy for produktutvikling. Finanstilsynet vurderte at beslutningsfullmakter og tidspunkt for den endelige godkjenningen av nye produkter fremsto noe uklare i retningslinjene, og stilte spørsmål om dette var tilstrekkelig tydelig i styringsdokumentene.

Styret klargjør i sitt svar at den styregodkjente fullmaktsmatrisen gjelder både for beslutningen om å utvikle et nytt produkt og for beslutningen om å lansere et nytt produkt. Ved begge beslutningspunkter involveres alle relevante eksperter fra både fagmiljøer og kontrollfunksjonene. Det fremgår videre fra styrets svar at foretaket vil gjennomgå fullmaktsmatrisen med sikte på å sikre tilstrekkelig tydelighet.

Finanstilsynet tar styrets svar til etterretning.

2.3 Avviks- og hendelsehåndtering

Finansforetak skal etter finansforetaksloven § 13-6 til enhver tid ha oversikt over, og med jevne mellomrom vurdere, hvilke enkelte risikoer og samlet risiko som er knyttet til virksomheten. God oversikt over operasjonelle avvik og andre uønskede hendelser vil være viktig for å vurdere nivået for operasjonell risiko i et foretak. Videre skal foretak etter IKT-forskriften § 9 sikre at det foreligger prosedyrer for avvikshåndtering og at alle avvik som oppstår i IKT-virksomheten håndteres i tråd med vedtatt prosedyre.

Foretakets policy for risikostyring og internkontroll viser til at foretaket skal ha en standardisert prosess for risikostyring og internkontroll som skal være tett integrert med andre forretningsprosesser og bidra til kontinuerlig læring og forbedring. I foretakets standard for operasjonell risiko pekes det på at kunnskap om faktiske hendelser er et viktig grunnlag for nye risikovurderinger, skadeforebygging og kostnadsbesparelser. Standarden sier videre at alle hendelser, også hendelser som ikke medfører faktisk tap eller skade, skal registreres i foretakets hendelsesregister for å sikre god oversikt og historikk over alle former for taps- og skadehendelser. Videre har foretaket etablert en standard samt rutine- og prosedyreskrivelser for håndtering av hendelser, problemer og endringer i virksomheten. Prosessene bygger i stor grad på internasjonale bransjestandarder for IKT-virksomhet.

Finanstilsynet vurderte i foreløpig tilsynsrapport at foretakets praksis for håndtering og rapportering av avvik og hendelser i hovedsak var begrenset til IKT-relaterte forhold og understreket viktigheten av at alle typer avvik og operasjonelle hendelser registreres og håndteres. Finanstilsynet pekte på et potensial for å tydeliggjøre dette og enkelte andre forhold i foretakets styrende dokumenter. Det ble også pekt på at foretakets risikorapportering kun inneholdt hendelser som var blitt rapportert til tilsynsmyndigheter. Finanstilsynets syn er at en helhetlig rapportering av hendelser er en viktig del av rapporteringen om operasjonell risiko til styret.

Finanstilsynet uttrykte også en forventning om at foretaket informerer noe mer omfattende til Finanstilsynet i den første rapporteringen av en hendelse knyttet til driften, herunder at det kan indikeres hva man antar kan være årsaken til hendelsen samt en vurdering av om hendelsen kan være forårsaket av tilsiktede handlinger. Finanstilsynet forventer imidlertid at dette ikke begrenses til driftshendelser.

Styret opplyser i sitt svar om at foretaket kommer til å sette i gang en vurdering av etablerte arbeids- og rapporteringsprosesser med mål om å sikre en mer helhetlig tilnærming til hendelsehåndtering- og rapportering, som skal omfatte alle typer hendelser. Foretaket vil i den sammenheng også gjennomføre en revisjon av styrende dokumenter for å sikre enhetlig begrepsbruk og konsistens mellom dokumenter og prosesser. Styret tar også innspillene knyttet til rapportering av hendelser til Finanstilsynet til etterretning og vil sørge for at det informeres mer omfattende i den første (foreløpige) meldingen, så langt det foreligger relevant informasjon.

Finanstilsynet tar styrets svar til etterretning.

2.4 Håndtering av kundeklager

Finansforetak skal ha skriftlige rutiner som sikrer grundig klagebehandling, herunder at alle kundeklager registreres i et eget register. Kundeklager skal også rapporteres årlig til Finanstilsynet, jf. rundskriv 4/2019 - Retningslinjer for klagebehandling i bank-, finans-, forsikrings- og

verdpapirverksemd. Klagebehandlingsrutinene skal være offentlig tilgjengelige og det er krav til å etablere rutiner for å svare personer som klager.

I foretakets interne rutine for håndtering av kundeklager er det vist til at formålet med rutinen er å oppfylle kravene i Finanstilsynets rundskriv 4/2019.

Finanstilsynet pekte i foreløpig tilsynsrapport på at foretaket ikke har offentliggjort foretakets klagebehandlingsrutiner og dermed ikke innrettet seg etter forventningene i rundskrivet på dette punktet.

Det går frem av styrets svar at foretaket har igangsatt forbedring av rutinen for kundeklagebehandling, og at en forbedret rutine skal offentliggjøres på foretakets nettside.

Finanstilsynet tar styrets svar til etterretning.

2.5 Overvåking og rapportering

Etter finansforetaksloven § 13-6 skal styret overvåke og styre finansforetakets samlede risiko og jevnlig vurdere om finansforetakets styrings- og kontrollordninger er tilpasset risikonivå og omfang av virksomheten. Styret skal etter § 8-6 sørge for at daglig leder regelmessig gir styret underretning om foretakets virksomhet, stilling og resultatutvikling. Daglig leder plikter etter § 8-12 (1), i møte eller skriftlig, å underrette styret om foretakets virksomhet, stilling og resultatutvikling minst hver måned. Finanstilsynet forventer at styret sikrer seg tilstrekkelig informasjon om risiko og øvrige forhold i virksomheten ved å fastsette omfang, format og frekvens for administrasjonens rapportering. Det forventes videre at uavhengig kontrollfunksjon overvåker foretakets risiko løpende og rapporterer uavhengig til styret og ledelsen om risikosituasjonen.

Finanstilsynets vurderte i foreløpig tilsynsrapport at foretaket har en omfattende rapportering om virksomheten og om vesentlige risikoer til styret, men pekte på at risikorapporteringen fra kontrollfunksjonene i større grad bør fremme et uavhengig syn på risiko- og etterlevelsessituasjonen samt inkludere konkrete råd og anbefalinger knyttet til risikoforhold som tas opp i rapporten.

Styret viser i sitt svar til at foretaket tar innspillene fra Finanstilsynet til etterretning og vil sørge for at det skilles tydeligere mellom virksomhetsrapporteringen i første linje og uavhengig risiko- og etterlevelsesrapportering fra kontrollfunksjonene til styret og ledelsen samt at konkrete råd og anbefalinger inkluderes i kontrollfunksjonenes rapportering.

Finanstilsynet tar styrets svar til etterretning.

3 FORHOLD KNYTET TIL RISKOEN FOR HVITVASKING OG TERRORFINANSIERING

3.1 Risikovurdering

Hvitvaskingsloven § 7 krever at rapporteringspliktige identifiserer og vurderer risikoen for hvitvasking og terrorfinansiering knyttet til sin virksomhet og virksomhetens art. Formålet med risikovurderingen er å kartlegge og beskrive foretakets risiko for hvitvasking og terrorfinansiering, og på den måten danne grunnlag for rutinene som foretaket må etablere for utførelsen av tiltakene for å forebygge hvitvasking og terrorfinansiering. Risikovurderingen skal blant annet ta i betraktning foretakets egen virksomhet, virksomhetens omfang, produkter, tjenester og kundeforhold, samt typer kunder/kundegrupper og geografiske forhold. Risikovurderingen skal dokumenteres, holdes oppdatert og stilles til rådighet for tilsynsmyndigheten, jf. hvitvaskingsloven § 7 femte ledd.

Foretakets virksomhetsinnrettede risikovurdering består av flere dokumenter. Dette fremsto som uklart for Finanstilsynet før tilsynsmøtet, og Finanstilsynet pekte i foreløpig tilsynsrapport på at foretaket bør tydeliggjøre hva som inngår, for blant annet å skille risikovurderingen tydeligere fra foretakets status- og risikoreporter til styret og ledelsen. Finanstilsynet vurderte også at risikovurderingen bør utvides med vurderinger basert på foretakets ulike produkter og tjenester, distribusjonskanaler og ulike kunde/kundegrupper. Selv om geografisk risiko vurderes å være begrenset i foretaket, viste Finanstilsynet også til at denne risikoen bør vurderes ved reelle rettighetshavere, eller andre kunden har tilknytning til eller er eksponert mot. Finanstilsynet understreket også at risikovurderingen ved behov må oppdateres hyppigere enn ved de faste halvårlige terminene.

Styret viser i sitt svar til at risikovurderingen allerede inneholder vurderinger på produktnivå, og at foretaket vil utvide analysene med flere elementer, eksempelvis distribusjonskanaler, mer detaljerte kundegrupper og geografisk risiko i forbindelse med utenlandske reelle rettighetshavere. Styret bekrefter videre at risikovurderingen oppdateres minimum halvårlig, og at det ved behov gjennomføres ad hoc oppdateringer.

Finanstilsynet tar styrets svar til etterretning.

3.2 Risikoklassifisering

For å gjennomføre hensiktsmessige kundetiltak, må alle kunder risikoklassifiseres, jf. hvitvaskingsloven § 9. Foretaket må ha rutiner for hvordan risikoklassifiseringen skal skje og påse at kundenes risikoprofiler er oppdaterte. Risikoklassifiseringen skal bygge på generelle vurderinger fra virksomhetens risikovurdering, i tillegg til konkrete forhold tilknyttet den enkelte kunde. I henhold til rundskriv 8/2019 punkt 2.4 skal risikoklassifiseringen blant annet hensynta alle kundens produkter og tjenester i foretaket, kundeforholdets formål og tilsiktede art, mengden kundemidler som skal inngå i kundeforholdet, kundens samlede kontoer og engasjement, transaksjoners størrelse og regelmessighet, samt varigheten på kundeforholdet.

Finanstilsynet viste i foreløpig tilsynsrapport til at foretaket ikke er konsekvent i klassifiseringsinndelingen da det opereres med ulike inndelinger i henholdsvis rutinene og i rapporteringen til styret. Finanstilsynet vurderte også at foretaket bør utvide momentene som vurderes ved etablering av kundeforholdet ved at det i større grad tas hensyn til forhold som kundens valg av produkter og tjenester, samt kundeforholdets formål og tilsiktede art. Videre bør risikoklassifiseringen i større grad forankres i foretakets risikovurdering. Finanstilsynet pekte også på at rutinene for endring av risikoklassifisering etter etablering av kundeforholdet bør formaliseres.

Finanstilsynet noterer fra styrets svar at rutinene vil bli oppdatert slik at det vil bli konsistens mellom disse og rapporteringen til styret. Styret fremholder i sitt svar at momentene som Finanstilsynet savner i vurderingene ved etablering av kundeforholdet inngår i risikoklassifiseringen, og peker videre på at det i den løpende risikoklassifiseringen også legges til andre forhold som går utover kravene i lov og veileder, slik som for eksempel å vurdere det helhetlige kundebildet (kombinasjon av sluttbruker- og brukerstedsdata, roller i næringslivet, osv.), betalingshistorikk, chat-meldinger, osv. Finanstilsynet noterer at foretaket vil formalisere og beskrive prosessen for endring av risikoklassifisering i løpende kundeforhold mer utfyllende i foretakets rutiner for antihvitvasking og -terrorfinansiering.

3.3 Kundetiltak

Hvitvaskingsloven § 9 pålegger foretaket å gjennomføre kundetiltak etter §§ 10 til 20, og løpende oppfølging etter § 24 på grunnlag av en vurdering av risiko for hvitvasking og terrorfinansiering. Foretaket skal videre registrere og lagre opplysninger og dokumenter som er innhentet og utarbeidet i forbindelse med tiltak, jf. § 30.

Etter hvitvaskingsloven § 12 tredje ledd skal rapporteringspliktige avgjøre om det finnes en reell rettighetshaver i tillegg til kunden, når kunden er en fysisk person. For kunde som ikke er fysisk person, skal det innhentes opplysninger om reelle rettighetshavere som er identifisert i samsvar med hvitvaskingsloven § 14.

I henhold til hvitvaskingsloven § 12 fjerde ledd og § 13 fjerde ledd skal rapporteringspliktige ha systemer for å avgjøre om kunden, personer som kan handle på vegne av kunden eller er gitt disposisjonsrett over en konto eller et depot, eller reell rettighetshaver, er politisk eksponert person eller nært familiemedlem eller kjent medarbeider til en politisk eksponert person (PEP). Det følger av Finanstilsynets rundskriv 8/2019 punkt 4.9.5 at rapporteringspliktige som et minimum må innhente en egenerklæring fra kunden hvor det spørres kunden om en PEP er involvert i kundeforholdet.

Rapporteringspliktige må innhente og vurdere nødvendige opplysninger om kundeforholdets formål og tilsiktede art, jf. hvitvaskingsloven § 12 femte ledd og § 13 femte ledd. Det følger av Finanstilsynets rundskriv 8/2019 punkt 4.2.2 at kundeforholdets formål gjelder bakgrunnen for at kunden ønsker å opprette det aktuelle kundeforholdet, og hvorfor kunden vil benytte aktuelle produkter eller tjenester. I henhold til punkt 4.2.3 gjelder kundeforholdets tilsiktede art karakteren av det spesifikke kundeforholdet, altså hvordan kunden skal bruke tjenestene og produktene. Relevante opplysninger er midlenes og formuens opprinnelse, opplysninger om juridiske personers forretningsmodell og hvordan kunden tenker å anvende midlene som inngår i kundeforholdet. Det er også relevant med opplysninger om hvem kunden skal handle med, forventet transaksjonsmønster.

Foretaket har systemer for screening mot PEP- og sanksjonslister ved kundeetablering og i den løpende oppfølgingen av kundeforholdet. Finanstilsynet pekte imidlertid på at foretaket bør oppdatere sine rutiner og praksis når det gjelder rundskrivets presisering om at det som minimum skal innhentes en egenerklæring fra alle kunder hvor det spørres om en PEP er involvert i kundeforholdet. Finanstilsynet noterer fra styrets svar at foretaket, i tillegg til allerede etablerte systemer, prosesser og rutiner for etterlevelse av krav om å innhente opplysninger om PEP-er for brukersteder, vil igangsette arbeid med å etablere og implementere systemer for å ivareta etterlevelsen av tilsvarende krav for sluttbrukere, både i kundeetableringen og den løpende oppfølgingen av kundeforholdet.

Finanstilsynet uttrykte i foreløpig tilsynsrapport også en forventning om at foretaket løpende vurderer behovet for å innhente opplysninger, også fra sluttbrukere, om kundeforholdets formål og tilsiktede art, hensyntatt virksomhetens utvikling, og at rutinene oppdateres ved behov. Finanstilsynet noterer fra styrets svar at foretaket vil imøtekomme Finanstilsynets forventning.

Foretakets rutiner for sluttbrukere inneholder ingen informasjon om identifisering av reelle rettighetshavere, og det ble bekreftet av foretaket under tilsynsmøtet samt dokumentert gjennom stikkprøvekontroller at foretaket ikke innhenter eller registrerer opplysninger om reelle rettighetshavere for slike kunder. Finanstilsynet vurderte i foreløpig tilsynsrapport at foretaket dermed ikke etterlever hvitvaskingsloven § 12 tredje ledd og uttrykte en forventning om at foretaket oppdaterer sine rutiner og praksis på dette punktet.

Styret peker i sitt svar på at de ulike tjenestene i Vipps-applikasjonen utelukkende er til for personlig bruk samt til foretakets vilkår og brukerbegrensninger. Finanstilsynet oppfatter svaret slik at styret ikke ser behov for å innhente opplysninger om reelle rettighetshavere for sluttbrukere. Finanstilsynet er av den oppfatning at vilkår og brukerbegrensningene som foretaket viser til i sitt svar ikke eliminerer alle muligheter for misbruk av tjenestene og underliggende bankkonto. Det er Finanstilsynets vurdering at foretaket bør kunne iverksette enkle tiltak for å etterleve kravet, uten at det vil kreve større tekniske eller administrative grep. Eksempelvis en bekreftelse, i forbindelse med kundens aksept av kundeavtalen, om at det er personens egen konto og at ingen andre disponerer kontoen. *Finanstilsynet legger til grunn at foretaket iverksetter nødvendige tiltak for å etterleve kravet.*

3.4 Elektronisk transaksjonsovervåking

Rapporteringspliktige skal etter hvitvaskingsloven § 24 gjøre løpende oppfølging av kundeforholdet, noe som blant annet innebærer å overvåke om kundens transaksjoner er i tråd med det rapporteringspliktige har fått opplyst om kunden og kundeforholdets formål, samt kundens virksomhet, risikoprofil og midlenes opprinnelse. Hvitvaskingsloven § 38 stiller krav til at foretak skal ha elektroniske overvåkningssystemer for å avdekke forhold som kan indikere hvitvasking og terrorfinansiering. Hensikten med bestemmelsen er å sørge for at den rapporteringspliktige følger opp kunder og innretter egnede kundekontrolltiltak. Selv om rapporteringspliktige benytter seg av systemer som støtteverktøy, er foretaket likevel ansvarlig for at systemene er egnet til å ivareta pliktene etter regelverket. Systemene må være tilpasset virksomhetens art og omfang, og inneha mulighet for tilpasninger og således være egnet for å oppfylle regelverket. Foretaket må også kjenne til hvilke eventuelle svakheter systemet har, slik at den rapporteringspliktige har en oversikt over hvilke ytterligere kontrolltiltak som er nødvendige å foreta.

Finanstilsynet viste i foreløpig tilsynsrapport til at foretaket har etablert et eget kompetansemiljø og utviklet et system for elektronisk transaksjonsovervåking og analyse som brukes for å avdekke både svindel og hvitvasking. Det ble notert at regler for kunde- og transaksjonsovervåking utvikles og justeres i takt med avdekkede risikoer knyttet til brukersteder og sluttkunder. Finanstilsynet viste videre til at foretaket ikke hadde oversendt rutinebeskrivelser for arbeidsflyten/saksbehandlingen for den daglige behandlingen av alarmer fra transaksjonsovervåkingen med tidsfrister, prioritering av alarmer og eventuelle rutiner for å fjerne falske positive alarmer. Finanstilsynet ba foretaket oversende foretakets rutiner på dette området.

Finanstilsynet understreket i foreløpig tilsynsrapport at transaksjonsovervåkingen skal samsvare med risikovurderingen og tilpasses foretakets virksomhet og kunnskap samt at foretakets erfaringer om relevante risikoer skal benyttes i regelutviklingen. Finanstilsynet kunne ikke se at foretaket har dokumenterte rutiner for evaluering av reglene for å sikre at de er tilstrekkelig dekkende og treffsikre, herunder med spesiell oppfølging av nye og endrede regler. Finanstilsynet ba foretaket etablere og dokumentere rutiner for kvalitetskontroll og evaluering av reglene som benyttes i transaksjonsovervåkingen.

Finanstilsynet noterer fra styrets svar at enheten som jobber med transaksjonsovervåking og håndtering av alarmer har blitt betydelig styrket de siste årene, og at foretaket kommer til å fortsette arbeidet med kontinuerlig forbedring av systemet. Styret viser til at foretaket herunder skal etablere rutiner for kvalitetskontroll og evaluering av de elektroniske filtre som benyttes i transaksjonsovervåkingen. Styret viser videre til at foretaket vil revidere sitt AML-rammeverk innen utgangen av 2021. AML-rutiner og arbeidsinstrukser som omhandler saksbehandling av alarmene skal oppdateres med tidsfrister og prioritering av alarmer i den sammenheng.

Finanstilsynet understreker viktigheten av at foretaket dokumenterer viktige arbeidsprosesser fortløpende. Det bes om at foretaket oversender nye og reviderte dokumenter, som det ble bedt om i foreløpig tilsynsrapport, innen 31. januar 2022.

3.5 Opplæring

Hvitvaskingsloven § 36 pålegger rapporteringspliktige å sikre ansatte opplæring slik at de er kjent med virksomhetens forpliktelser etter loven og er i stand til å gjenkjenne forhold som kan indikere hvitvasking og terrorfinansiering. Opplæringen skal gis jevnlig slik at kunnskapen vedlikeholdes og oppdateres. Videre presiserer Finanstilsynets rundskriv 8/2019 punkt 10.1 at opplæringsplikten også omfatter styret, samt at kravet om en opplæringsplan for foretaket defineres. Rapporteringspliktige bør kunne dokumentere opplæringstiltak med tidspunkt, beskrivelse, deltakelse og type tiltak (e-læring eller fremmøte).

Vipps gjennomfører opplæring i form av årlig nanokurs i antihvitvasking og -terrorfinansiering for alle ansatte. Nanokurset inneholder i tillegg en opplæringspakke alle nyansatte får tilsendt i løpet av de første arbeidsdagene. Det dokumenteres hvem som har gjennomført kurset. Ytterligere opplæring er prioritert etter behov, avhengig av ansattes ansvar, roller og funksjon. Medarbeidere med særlige roller som er mer eksponert for risiko tilknyttet hvitvasking og terrorfinansiering får grundigere opplæring. Det gjennomføres ingen særskilt opplæring for styret tilpasset styrets rolle.

Finanstilsynet vurderte i foreløpig tilsynsrapport at innholdet i nanokurset er noe overordnet og med fordel kan utvides og oppdateres. Den særskilte opplæringen bør etter Finanstilsynets vurdering formaliseres og dokumenteres, og foretaket bør vurdere å implementere test- og beståelseskrav til nanokurset og den særskilte opplæringen. Finanstilsynet viste videre til at foretaket bør fastsette en opplæringsplan for virksomheten og sikre at også styret og ledelse får tilpasset opplæring basert på sine roller i hvitvaskingsarbeidet.

Finanstilsynet merker seg fra styrets svar at foretaket har igangsatt en oppdatering av opplæringsmaterialet før høstens opplæringsrunde for hele virksomheten. Finanstilsynet noterer videre at foretaket kommer til å inkludere opplæringsaktiviteter i årshjulet og at det kommer til å utarbeides rolletilpasset opplæring for styret og ledelsen.

Kopi av denne tilsynsrapporten bes sendt til bankens valgte revisor.

For Finanstilsynet

Linda Støle Hårstad
seksjonssjef

Frode Holmeide
tilsynsrådgiver

Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.