



SANTANDER CONSUMER BANK AS  
Postboks 177  
1325 LYSAKER

VÅR REFERANSE  
21/6151

DERES REFERANSE

DATO  
28.10.2022

## Tilsynsrapport og vedtak om overtredelsesgebyr

Finanstilsynet gjennomførte stedlig tilsyn i Santander Consumer Bank AS (heretter banken eller Santander) 1. og 2. september 2021 som ledd i den risikobaserte tilsynsvirksomheten. Formålet var å gjennomgå bankens etterlevelse av IKT-forskriften og hvitvaskingsregelverket i tilknytning til bankens elektroniske systemer for å avdekke hvitvasking og terrorfinansiering. Tilsynet var begrenset til bankens virksomhet i Norge.

For å kunne gjennomføre en tilstrekkelig vurdering av de aktuelle systemenes egnethet til å ivareta pliktene som følger av aktuelt regelverk, dekket tilsynet også etterlevelsen av enkelte andre relevante plikter i hvitvaskingsregelverket. Pliktene omfattet av tilsynet var således IKT-forskriften samt deler av hvitvaskingsloven med forskrift.

Til grunn for denne tilsynsrapporten ligger Finanstilsynets foreløpige rapport av 7. februar 2022 samt styrets kommentarer til rapporten i brev av 7. april 2022.

I foreløpig tilsynsrapport ble det varslet ileggelse av overtredelsesgebyr basert på vurderinger av at banken hadde overtrådt §§ 7, 8, 9, 12, 13, 17, 18, 24, 25 og 26 i lov om tiltak mot hvitvasking og terrorfinansiering. Finanstilsynet varslet også pålegg om retting.

Finanstilsynet merker seg at banken i tilsvaret til foreløpig rapport har beskrevet flere tiltak og rettinger knyttet til etterlevelsen som er utført i etterkant av tilsynet. Grunnlaget for overtredelsesgebyret er status på tilsynstidspunktet.

### 1. Organisering

#### Rettslig grunnlag og Finanstilsynets forventninger

Det følger av finansforetaksloven § 13-5 første ledd at foretaket skal ha en klar organisasjonsstruktur og ansvarsfordeling, samt klare og hensiktsmessige styrings- og kontrollordninger. Et finansforetak skal videre ha uavhengige kontrollfunksjoner med ansvar for internrevisjon, risikostyring og etterlevelse, jf. samme paragraf andre ledd.

Hvitvaskingsloven § 8 femte ledd stiller krav til at foretaket skal utpeke en person i ledelsen (Hvitvaskingsansvarlig) som skal ha et særskilt ansvar for å følge opp rutinene. Hvitvaskingsansvarlig må sitte i førstelinje og ha tilstrekkelig erfaring, kompetanse og gjennomføringskraft til å fatte avgjørelser tilknyttet virksomhetens tiltak mot risiko for hvitvasking og terrorfinansiering.

## **Bankens etterlevelse og Finanstilsynets vurderinger**

På tidspunktet for det stedlige tilsynet hadde banken nylig gjennomført omorganiseringer på anti-hvitvaskingsområdet. I foreløpig rapport pekte Finanstilsynet på at banken har valgt en organisering der hvitvaskingsansvarlig innehar en ledende stilling, men ikke inngår i konsernledelsen. Finanstilsynet viste til at dersom hvitvaskingsansvarlig ikke er plassert i øverste ledelse, må foretaket ha en dokumentert, risikobasert begrunnelse for dette. Hvitvaskingsansvarlig hadde på tilsynstidspunktet ingen stillingsinstruks, men det fremgikk av et mottatt notat om stillingen at hvitvaskingsansvarlig må kunne rapportere direkte til styret og daglig leder (CEO). Hvitvaskingsansvarlig rapporterte imidlertid til et medlem i bankens nordiske ledelse og hadde således kun en indirekte rapporteringslinje til styret og CEO.

Videre bemerket Finanstilsynet at banken de senere år har gjennomført flere større omorganiseringer, og at Chief Compliance Officer, som tiltrådte stillingen i september 2020, er den fjerde lederen for etterlevelse i banken på få år. På bakgrunn av dette samt funnene i tilsynet, stilte Finanstilsynet spørsmål ved om bankens hyppige organisatoriske endringer kan ha lagt press på organisasjonen og blant annet økt risikoen for redusert effektivitet og produktivitet, manglende regulatorisk etterlevelse samt andre uønskede hendelser og operasjonelle tap. Finanstilsynet viste til at hyppige endringer av nøkkelfunksjoner og uavhengige kontrollfunksjoner kan vanskeliggjøre kontinuitet og langsiktighet i kontrollarbeidet, og det kan være et signal om at det kan være underliggende årsaker i organisasjonen til at funksjonene ikke fungerer.

Finanstilsynet merker seg styrets tilsvarende om bakgrunnen for plasseringen av hvitvaskingsansvarlig, og at denne funksjonen fremover vil rapportere direkte til CEO. Finanstilsynet noterer seg videre styrets kommentar hva gjelder endringene i nøkkelfunksjoner.

## **2. Risikovurdering**

### **Rettslig grunnlag og Finanstilsynets forventninger**

Rapporteringspliktige må identifisere og forstå risikoen foretaket er eksponert for. Alle rapporteringspliktige skal ha en risikovurdering, jf. hvitvaskingsloven § 7. Gjennom risikovurderingen skal den rapporteringspliktige identifisere og vurdere risikoen for hvitvasking og terrorfinansiering knyttet til egen virksomhet, da denne skal danne utgangspunktet for den rapporteringspliktiges utarbeidelse av rutiner, samt den øvrige implementeringen av hvitvaskingsregelverket.

Risikovurderingen skal omfatte foretakets egen virksomhet, produkter, tjenester og kundeforhold, type kunder, kundegrupper og geografiske forhold. Også terrorfinansieringsrisikoen skal vurderes, selv om risikoen anses lav. Sentrale elementer i risikovurderingen vil være erfaringene den rapporteringspliktige gjør seg gjennom virksomheten, herunder kunnskap om egen kundemasse, samt fra undersøkelser og rapportering om mistenkelige forhold. Av eksterne kilder forventer Finanstilsynet at alle rapporteringspliktige som et minimum benytter gjeldende Nasjonal risikovurdering av hvitvasking og terrorfinansiering samt Finanstilsynets risikovurdering for foretak under tilsyn.

Risikovurderingen må oppdateres jevnlig for å kunne være et praktisk verktøy for rapporteringspliktige. En fornyet vurdering bør gjøres minimum årlig eller hyppigere ved behov. Relevante momenter vil være ny kunnskap om metoder og trender for hvitvasking og terrorfinansiering, enten basert på oppdaterte erfaringer fra den rapporteringspliktige selv, eller fra

eksterne kilder. Videre skal rapporteringspliktige særskilt vurdere risikoen for hvitvasking og terrorfinansiering før nye produkter og tjenester tilbys, og før ny teknologi tas i bruk, jf. hvitvaskingsloven § 7 tredje ledd.

Finansforetaksloven § 13-6 pålegger også bankene til enhver tid å ha oversikt over, og med jevne mellomrom vurdere, hvilke risikoer som er knyttet til egen virksomhet, herunder operasjonell risiko.

### **Bankens etterlevelse og Finanstilsynets vurderinger**

I forbindelse med tilsynet mottok Finanstilsynet to risikovurderinger, den ene fra 2019 og den andre vedtatt av styret 22. juli 2021. Banken hadde besluttet å ikke gjennomføre en fornyet risikovurdering av virksomheten i 2020, på grunn av manglende ressurskapasitet, kompetanse, samt prioritering av nøkkelressurser til heller å implementere bankens nye elektroniske overvåkingssystem. Fra 2020-2021 hadde banken gjennomgått to større omorganiseringer, blant annet for å effektivisere arbeidet på hvitvaskingsområdet, som begge omfattet opprettelsen av nye enheter og rapporteringslinjer for anti-hvitvasking og terrorfinansieringsarbeidet. Frem til ny risikovurdering i 2021 hadde derfor risikovurderingen fra 2019 blitt lagt til grunn.

I foreløpig rapport viste Finanstilsynet til flere mangler ved risikovurderingen fra 2019. Blant annet var den lite tilpasset bankens egen virksomhet og erfaringer, da den i hovedsak pekte på generelle og åpenbare risikoer for bransjen og gruppen generelt. Den omfattet videre bankens samlede virksomhet i Norden og inneholdt derfor i svært liten grad vurdering av lokale risikoer og kjente kriminalitetstrender. Finanstilsynet oppfattet også risikovurderingen som utdatert på flere områder, ettersom den fremsto lite representativ for bankens virksomhet, art og omfang i 2020. Blant annet reflekterte den ikke erfaringer og identifiserte risikoer ved planlagt omorganisering av arbeidet på området samt innføringen av nytt elektronisk overvåkingssystem. Videre ble en del risikofaktorer beskrevet, men det fremsto uklart hvorfor akkurat disse var løftet frem og aktuelle for banken. Under tilsynet ble det kjent at vurderingen i hovedsak var utviklet av eksterne aktører med støtte fra interne ressurspersoner. Banken hadde ikke foretatt andre særskilte vurderinger av risiko for hvitvasking og terrorfinansiering i perioden 2019-2021, ei heller i tilknytning til den planlagte lanseringen av transaksjonsovervåkingssystemet, som ble tatt i bruk i juni 2020.

Finanstilsynet viste i foreløpig rapport til at banken plikter å særskilt vurdere risikoen for hvitvasking og terrorfinansiering før ny teknologi tas i bruk, jf. hvitvaskingsloven § 7 tredje ledd. Risikovurderingen skal danne utgangspunktet for den risikobaserte tilnærmingen i det øvrige arbeidet, herunder utviklingen av logikk i de aktuelle systemene som benyttes til både risikoklassifisering og transaksjonsovervåking. Finanstilsynet viste til at bankens manglende oppdatering syntes å delvis være et resultat av at systemutvikling og omorganiseringen i banken generelt krevde ressurser fra nøkkelpersoner, som dermed hadde begrenset kapasitet til andre oppgaver. Det vises for øvrig til Finanstilsynets merknader ellers i denne rapporten.

Etter Finanstilsynets vurdering oppfyller heller ikke risikovurderingen fra 2021 lovens krav. Finanstilsynet viste i den foreløpige rapporten blant annet til at selv om den berører flere sentrale risikoer, er det mangler på mange områder ved at den er for kort, overfladisk og lite virksomhetsinnrettet. Risikovurderingen var utviklet felles for alle landene i Norden og reflekterte derfor i liten grad lokale risikoer og kjente fremgangsmåter. I vurderingen av kunder og kundegrupper identifiseres det for personkunder ingen risikoer utover PEP, nasjonalitet,

bostedsadresse og handling på vegne av tredjepart. Banken opplyste imidlertid at 99,5 prosent av egen kundemasse var av samme nasjonalitet eller bor i landet der tjenesten tilbys, noe som gjør at eksponeringen mot disse risikodriverne i realiteten er marginal. Videre hadde banken definert sju høyrisikobransjer, herunder skogbruk, ikke-statlige, frivillige organisasjoner (NGOs), våpen- og forsvarsindustrien, uten at det fremkom hvorfor disse var aktuelle for Santander. Det var heller ikke gjort rede for hvorfor bransjer banken selv peker på å ha eksponering mot, slik som eiendom, samt reparasjon og handel med motorvogner, ikke anses som høyrisikobransjer på tross av at den iboende risikoen for disse er blitt fremhevet av en rekke aktører over flere år, herunder av Økokrim og NTAES<sup>1</sup>.

Finanstilsynet viste også i den foreløpige rapporten til at banken i langt større grad må vurdere egen risiko ved å bygge eksplisitt på relevante data og informasjon fra egen virksomhet. Det var heller ikke mulig å lese ut fra risikovurderingen hvilke kunder, kundegrupper, produkter, tjenester og transaksjoner som anses å utgjøre høyere eller lavere risiko. På spørsmål fra Finanstilsynet om hvilke produkter banken selv anså å inneha høyere risiko enn andre, pekte banken på kredittkort og innskudd. Imidlertid er ikke dette reflektert i tilhørende dokumentasjon eller bankens praksis. For Finanstilsynet fremsto også vurderingene flere steder som ulogiske. Blant annet var det påpekt en rekke risikofaktorer samt mangler ved bankens risikoreducerende tiltak og generelle etterlevelse av regelverket, men likevel konkludert med at risikoen for å bli utnyttet til hvitvasking og terrorfinansiering var moderat eller lav uten at dette var videre begrunnet. Flere av de tilhørende tiltakene som var beskrevet, vurderes av Finanstilsynet heller ikke som adekvate for å redusere den identifiserte risikoen som påpekes.

Finanstilsynet merker seg anførselene i styrets svar, herunder styrets oppfatning av at risikovurderingen har mangler, men at det er vesentlig forskjell mellom potensialet for forbedring og manglende etterlevelse av lovkravet. Finanstilsynet understreker imidlertid at risikovurderingen skal identifisere og vurdere risikoen for hvitvasking og terrorfinansiering tilknyttet egen virksomhet, noe som nødvendigvis forutsetter at vurderingene tar utgangspunkt i relevante risikoer lokalt samt bygger på data og informasjon om egen virksomhet. Finanstilsynet merker seg videre at styret ikke er enig i at det er manglende logikk i risikovurderingen, men at styret vil påse arbeid med forbedring av nåværende metodikk. Finanstilsynet kan imidlertid ikke se at anførselene i tilsvaret gir grunn til å endre Finanstilsynets vurdering fra foreløpig rapport.

Basert på det ovennevnte fastholder Finanstilsynet derfor vurderingen om at banken på tilsynstidspunktet ikke hadde en risikovurdering som oppfyller kravene i hvitvaskingsloven § 7. Finanstilsynet forventer at foretaket utarbeider en fornyet risikovurdering som identifiserer og vurderer risikoen for hvitvasking og terrorfinansiering knyttet til egen virksomhet i Norge, og viser til pålegget i tilsynsrapportens siste kapittel.

### **3. Rutiner**

#### **Rettslig grunnlag og Finanstilsynets forventninger**

Banken plikter å ha oppdaterte rutiner for å sikre at virksomheten håndterer identifisert risiko og oppfyller plikter etter bestemmelser gitt i, eller i medhold av, hvitvaskingsloven, jf. § 8. Dette innebærer at det blant annet må utarbeides rutiner for risikoklassifisering av kunder, gjennomføring

---

<sup>1</sup> Nasjonalt tverretatlig analyse- og etterretningscenter (NTAES)

av løpende kundetiltak, bruk av støtteverktøy, rutiner om undersøkelse og rapportering av mistenkelige forhold mv. Rutinene skal være operasjonelle og beskrive hvordan foretaket i praksis skal etterleve hvitvaskingsregelverket. De skriftlige rutinene må dekke både plikter som skal sikre at foretaket har forsvarlig styring og kontroll med antihvitvaskingsarbeidet, og plikter som skal ivaretas av de ansatte i det daglige arbeidet. Rutinene må blant annet beskrive hvordan banken skal etterleve hvitvaskingsregelverket, herunder angi hva som skal gjøres, hvordan og når dette skal gjøres og hvilke vurderinger som skal ligge til grunn.

### **Bankens etterlevelse og Finanstilsynets vurderinger**

I foreløpig rapport viste Finanstilsynet til at alle rutiner på hvitvaskingsområdet med unntak av én, tilsynelatende var opprettet i perioden juni 2020 til juli 2021, og flertallet av disse opprettet så sent som i slutten av juni og juli 2021. Av rutinene Finanstilsynet spesifikt etterspurte, var tre av fire nylig blitt opprettet og vedtatt av styret den 30. juli 2021. Den fjerde var opprettet i juni 2020 og revidert 30. juni 2021.

I foreløpig rapport pekte Finanstilsynet på at rutinene var lite tilpasset bankens virksomhet og risiko, ettersom det ikke var noen tydelig sammenheng mellom rutinene og de aktuelle risikoene identifisert i bankens risikovurdering. Rutinene fremsto videre som overordnede og retningslinjepregede, og i liten grad som operasjonelle rutiner som ga de ansatte veiledning om hvordan oppgavene skulle gjøres. For eksempel beskrev rutinene for løpende oppfølging i all hovedsak når oppfølgingen skulle finne sted, heller enn hva saksbehandler skulle gjøre og hvilke vurderinger som skulle foretas. Rutinene ga heller ikke anvisning på hvordan risikoklassifisering skulle skje, utover henvisninger til det automatiske systemet. Finanstilsynet viste i foreløpig rapport særskilt til manglende rutiner knyttet til produktet Auto Stock Finance som i tillegg til automatiserte prosesser også ble risikoklassifisert og fulgt opp manuelt. Det vises for øvrig til merknadene i rapportens del om elektronisk overvåking.

Finanstilsynet påpekte også at bankens AML-manual fra 2020 i liten grad omtaler hvordan undersøkelser faktisk skulle gjennomføres og hvilke vurderinger som måtte ligge til grunn. Bankens "Investigation and Reporting Guideline" (IRG), opprettet 30. juni 2021, fremsto mer som generell og retningslinjepreget, enn som en operasjonell rutine for håndteringen av spesifikke alarmer. Den reflekterte heller ikke bankens risikovurdering eller lokale forhold. Rutinen var fokusert på systemet, og det manglet eksempelvis spesifikke rutiner for identifisering og håndtering av mistanke utover det som genereres av systemene. Utover kategoriene PEP, RCA<sup>2</sup> og sanksjoner, manglet det operasjonelle rutiner for hvordan alarmer spesifikt skulle håndteres. Det ble ikke differensiert mellom falske positive alarmer og alarmer som utløser undersøkelsesplikt. Etter Finanstilsynets vurdering underbygges fraværet av slike rutiner ytterligere av bankens informasjon om at alle alarmer som ikke har ført til MT-rapport, er klassifisert som falske positive. Finanstilsynet ble heller ikke forelagt dokumentasjon som påviser at banken før IRG hadde særskilte rutiner som beskrev hvordan undersøkelser og rapportering til Økokrim skulle gjennomføres, eller rutiner for rangering av alarmer med tidsfrister for behandling. Finanstilsynet påpeker viktigheten av riktig håndtering og klassifisering av alarmer, herunder for å kunne vurdere reglens kvalitet og treffsikkerhet. Se også Finanstilsynets kommentarer i kapittel 7.

Også en rekke av de mottatte rutinene på IT-området var opprettet i juli 2021 eller udaterte/ikke godkjente. Her kan nevnes dokumentene for endringshåndtering datert juli 2021, dokumentene for

---

<sup>2</sup> RCA= Relatives And Close Associates

tilgangsstyring som var udatert og ikke godkjent, rutinen for logging datert juli 2021 og dokumentene for gjenopprettingsplaner som var udaterte. I sitt svar anfører styret at systemrutiner ikke er underlagt formelle krav for godkjenning og datering fordi de er systemspesifikke, og at hver system- og prosesseier vedlikeholder disse. Finanstilsynet imøtegår denne argumentasjonen. Uten datering og versjonsstyring kan den som bruker rutinen, være i tvil om hva som gjelder. De udaterte dokumentene det vises til over, har dessuten felt både for dato og godkjenning, men feltene er ikke fylt ut.

Finanstilsynet vurderer at banken frem til midten av 2021 har hatt vesentlige mangler i rutineverket, og at banken fremdeles har mangler. Banken hadde også selv sett et behov for å videreutvikle rutineverket, noe som blant annet har ført til opprettelsen og oppdateringen av rutinene som ble fremlagt under det stedlige tilsynet.

Finanstilsynet understreker at adekvate rutiner er en forutsetning for at de ansatte skal kunne gjennomføre tilstrekkelige vurderinger og iverksette nødvendige tiltak. Finanstilsynet viser også til at banken selv har identifisert eksisterende mangler ved eget rutineverk, og at oppdatering og videreutvikling av rammeverk og rutiner står oppført på tiltaksplanen med frist i første kvartal 2022. Basert på det ovennevnte er Finanstilsynets vurdering at banken frem til juli 2021 ikke har etterlevd hvitvaskingsloven § 8, og at den fortsatt har mangler i etterlevelsen av samme bestemmelse.

I tilsvaret fremhever styret blant annet at innsendt oversikt over rutiner kun viste gjeldende rammeverk, men at banken også hadde rutiner før disse ble opprettet. Finanstilsynet merker seg innsendte vedlegg som angivelig utgjør en komplett samling av rutiner for perioden 2018-2020, men påpeker samtidig at de vedlagte rutinene fremstår mangelfulle og overfladiske ved at de i hovedsak gjengir overordnede plikter og forventninger som følger direkte av lov og rundskriv. Flere er også svært korte, ofte stikkordsbaserte, og i liten grad operasjonelle. De kan således ikke anses egnede i å utgjøre et operasjonelt rutineverk som sikrer at virksomheten håndterer identifisert risiko og oppfyller plikter etter hvitvaskingsloven, jf. hvitvaskingsloven § 8.

Finanstilsynet merker seg videre styrets kommentar hva gjelder Finanstilsynets merknader til innholdet i det gjeldende rutineverket, med henvisninger til ulike deler i allerede innsendt dokumentasjon. Finanstilsynet kan imidlertid ikke se at delene det vises til, inneholder en beskrivelse av hvordan oppgavene skal utføres, eller hvilke vurderinger som til enhver tid må foretas. Finanstilsynet kan heller ikke se at det gis informasjon om håndteringen av spesifikke alarmer, herunder om klassifisering og prioritering. Finanstilsynet understreker at rutinene må operasjonaliseres på en slik måte at de fungerer som et godt arbeidsverktøy for de ansatte. Finanstilsynet påpeker dessuten at flertallet av rutinene i det eksisterende rammeverket enten var opprettet eller oppdatert rett i forkant av tilsynet, noe som nødvendigvis påvirker hvor godt banken hadde rukket å innarbeide de nye rutinene på tidspunktet for det stedlige tilsynet.

Finanstilsynet fastholder derfor sin vurdering om at banken frem til juli 2021 ikke har etterlevd hvitvaskingsloven § 8, og at det på tidspunktet for det stedlige tilsynet fortsatt var mangler i etterlevelsen av samme bestemmelse.

## 4. Internkontroll og rapportering på hvitvaskingsområdet

### Rettslig grunnlag og Finanstilsynets forventninger

Finansforetaksloven § 13-5 første ledd fastsetter krav om at foretaket skal ha hensiktsmessige retningslinjer og rutiner for å identifisere, styre, overvåke og rapportere risiko foretaket er, eller kan bli, eksponert for.

Videre fastsetter CRR/CRD IV-forskriften § 35 første ledd krav om at styret skal sikre seg tilgang til risikoinformasjon og fastsette omfang, format og frekvens på rapporteringen.

Det følger av hvitvaskingsloven § 35 at de rapporteringspliktige skal gjennomføre en forsvarlig internkontroll for å påse at kravene etter hvitvaskingsloven overholdes. Internkontrollen skal gjøre banken i stand til å avdekke svakheter og identifisere forbedringspotensial ved eget arbeid med tiltak mot hvitvasking og terrorfinansiering. Formålet med å identifisere eventuelle svakheter er at banken kan iverksette nødvendige tiltak for å forhindre at manglende etterlevelse fortsetter, herunder gjøre endringer i virksomhetens rutiner for å sikre overholdelse av hvitvaskingsloven. Forsvarlig internkontroll er en forutsetning for at adekvate tiltak skal kunne iverksettes, og for at blant annet rutiner effektivt skal kunne oppdateres av foretakets øverste ledelse.

I tillegg til kravene til internkontrollen i hvitvaskingsloven § 35 fremgår det av CRR/CRD IV-forskriften at det minst årlig skal foretas en oppsummerende vurdering av om internkontrollen har vært gjennomført på en tilfredsstillende måte og om det er behov for nye tiltak. Daglig leder skal utarbeide en samlet vurdering som skal forelegges styret til behandling, jf. CRR/CRD IV-forskriften § 37.

### Bankens etterlevelse og Finanstilsynets vurderinger

I foreløpig tilsynsrapport viste Finanstilsynet til at det fremgår av den årlige internkontroll-bekreftelsen for 2020 fra daglig leder, behandlet av styret i juni 2021, at regulatorisk etterlevelsrisiko for hvitvasking og terrorfinansiering har vært, og også fremover forventes å være, et fokusområde. Videre peker internkontrollrapporten på flere områder innen hvitvasking og terrorfinansiering hvor restrisikoen vurderes å være høy. Det konkluderes likevel med at basert på det generelle kontrollmiljøet, vurderes risikoen på området å kunne nedjusteres fra rødt ("Weak") til gult ("Needs improvement"), uten at det omtales hva som ligger til grunn for denne konklusjonen.

Fra styrets svar oppfatter Finanstilsynet at resultatet fra andrelinjens krysstesting av et sett kontrollaktiviteter i førstelinjen var avgjørende for å nedjustere risikoen. For Finanstilsynet fremstår det som uklart om det kun er utført en vurdering av førstelinjens kontrollrammeverk, eller om andrelinjen har foretatt en uavhengig kontroll av faktisk etterlevelse. Etter Finanstilsynets vurdering kan ikke risikoen nedjusteres så lenge den faktiske kvaliteten på rutiner, systemer og data ikke er kontrollert. Finanstilsynet har for øvrig merket seg at styret er av den oppfatning at det har mottatt oppdatert informasjon om daglig leders vurdering av internkontroll i banken.

Finanstilsynet pekte i foreløpig rapport på at det ikke fremgikk av mottatt dokumentasjon hvordan bankens uavhengige kontrollfunksjon for kontroll av etterlevelse rapporterer om etterlevelse av hvitvaskingsregelverket til styret og ledelsen i banken. Finanstilsynet tar til etterretning styrets svar om kontrollfunksjonens rapportering av bankens etterlevelse av hvitvaskingsregelverket, blant annet rapporten som ble presentert for styrets risikoutvalg og for styret i juni 2021, samt rapporteringen av etterlevelsen i "Q2 Compliance report".

Finanstilsynet pekte videre i foreløpig rapport på at det kun var utført *en* kontroll i andrelinjen på AML-området etter konverteringen til nytt system. Etter Finanstilsynets vurdering bør bankens uavhengige kontrollfunksjon for etterlevelse både kontrollere, vurdere og rapportere om banken etterlever regelverket. Resultater av gjennomførte kontroller og utvikling i andre risikoinndikatorer kan bidra til en tydeliggjøring av bankens faktiske situasjon og utvikling over tid. Spesielt viktig er dette etter skifte av systemplattform som med stor sannsynlighet påvirker risikobildet. Se også Finanstilsynets kommentar under punkt 7 (jf. omtale av endringshåndtering) som viser til flere feil i dataoverføringene til AML-systemet som oppsto under konverteringen til nytt system i juni 2020, men først ble avdekket over et halvt år etter og noen av dem så sent som i mars 2021.

Finanstilsynet har merket seg at styret i sitt svar viser til at andrelinjen vurderte at det ikke var ytterligere risiko å avdekke eller redusere fordi risikoområdene allerede var identifisert av internrevisjonen, og at andrelinjen dermed ville bekreftet allerede kjente problemer. Finanstilsynet finner imidlertid ikke at dette kan gi banken grunn til å unnlate å gjennomføre egne kontroller i andrelinjen for å sikre kvaliteten i konverteringen til ny systemplattform.

Finanstilsynet viste også i foreløpig rapport til at revisor har gjennomført flere revisjoner de siste årene, og at 2021-oppfølgingen av revisjonen fra 2018 fortsatt konkluderer med rødt og utilfredsstillende. Revisor kommenterer at til tross for at det er iverksatt tiltak, har banken utfordringer spesielt relatert til kundedata og manglende kontroller, samt at banken bør forsterke overvåking, testing og kontroll som utføres både av første og andre linje. Av tiltakene som revisor anbefalte, hvor tre ble klassifisert som tiltak som umiddelbart bør iverksettes og fire som bør prioriteres, noterte Finanstilsynet at flere tiltak ikke hadde fått frist før i februar 2022, mer enn ett år etter revisors rapport.

Finanstilsynet merker seg styrets svar om iverksatte tiltak på området. Finanstilsynet forventer at styret påser at det etableres et tilstrekkelig kontrollmiljø i banken, som er i stand til å avdekke mangler, og at tiltak iverksettes rettidig.

## 5. Risikoklassifisering

### Rettslig grunnlag og Finanstilsynets forventninger

For å gjennomføre korrekte kundetiltak, må alle kunder risikoklassifiseres, jf. hvitvaskingsloven § 9. Risikoklassifiseringen skal bygge på virksomhetens risikovurdering, i tillegg til konkrete forhold tilknyttet den enkelte kunde. Blant annet skal risikoen vurderes ut fra kundeforholdets formål og tilsiktede art, mengden kundemidler som skal inngå i kundeforholdet, kundens samlede kontoer og engasjementer, transaksjoners størrelse og regelmessighet, og varigheten på kundeforholdet. Til grunn for risikoklassifiseringen kan det også ligge andre forhold, basert på identifiserte risikoer i virksomhetens risikovurdering.

Det er anledning til å anvende standardiserte risikoprofiler for kundemassen, men disse må tilpasses virksomhetens konkrete risikoer. Banken må ha et system som dokumenterer hvorfor en kunde er klassifisert i en bestemt risikokategori. Rapporteringspliktige må påse at kundenes risikoprofiler er oppdaterte, slik at kundene endrer risikokategori ved endringer som tilsier det. Banken må jevnlig gjennomgå og tilpasse risikoklassifiseringssystemet, blant annet i forbindelse med justeringer i risikovurderingen. Foretaket må også ha rutiner, herunder for hvordan risikoklassifiseringen skal skje, samt for bruk og håndtering av eventuelle automatiske støtteverktøy.



## Bankens etterlevelse og Finanstilsynets vurderinger

Banken benyttet to systemer for å risikoklassifisere kundene, det ene til etablering og det andre til løpende klassifisering. I tillegg hadde banken et tredje system, integrert med det førstnevnte, som videresendte kundeforhold til manuell behandling dersom risikoen ble ansett høy. Bankens selv utviklet reglene/metodikken, og alle systemene søkte i utgangspunktet å følge samme logikk. Det vises til nærmere beskrivelser i den foreløpige tilsynsrapporten.

Finanstilsynet vurderte i foreløpig rapport bankens risikoklassifiseringsmetodikken som lite tilpasset bankens egen risikovurdering, egne produkter og virksomhet. Flere av de definerte reglene i systemene gjaldt dessuten kun for enkelte produkttyper. Blant annet ble ikke informasjon om midlenes opprinnelse og tilsiktede art hensyntatt for sparekunder, hverken ved etablering eller løpende oppfølging, på tross av at bankens selv påpekte en rekke aktuelle risikoer knyttet til dette ved bruk av produktet. Sparekunder ble heller ikke spurt om å oppgi slik informasjon, og var følgelig ekskludert fra den tilhørende regelen ved etablering. For øvrige kunder hvor midlenes opprinnelse ble hensyntatt ved etablering, var det kun valget "annet" som utløste høy risiko, uten at det fremkom som veldig sannsynlig at alternativet noen gang ble valgt ut fra mangfoldet i de øvrige kategoriene som var pre-definert. Videre ble kredittkortkunder stilt en rekke spørsmål om forventet bruk, men det var i realiteten kun ett valg som utløste klassifiseringen høy. Kredittkortkundene ble også stilt spørsmål om hva lånet skulle benyttes til, men her var det også kun kategorien "annet" som utløste høy risiko, på tross av flere alternativer som relaterte seg til aktivitet som kan indikere høy risiko for hvitvasking og terrorfinansiering.

Heller ingen av produktene banken tilbyr, ble ansett av systemet å inneha høy risiko ved etablering av kundeforhold, og dermed kreve at ytterligere kundetiltak gjennomføres. For bedriftskunder var det kun fire bransjer/sektorer som var definert som høyrisikobransjer og dermed utløste forsterkede kundetiltak før kundeforholdet ble etablert. Bransjene fremkom også som lite relevante med tanke på bankens kundemasse. Systemet hensyntok heller ikke mengden kundemidler som skulle inngå i kundeforholdet, transaksjoners størrelse, regelmessighet og varighet, jf. lovens § 9. Slik Finanstilsynet vurderte metodikken og innretningen til systemet, var det i all hovedsak adresse i høyrisikoland, PEP, listetreff og handling på vegne av tredjepart som førte til klassifiseringen høy ved etablering. Dette ble også underbygget av funnene som omtales senere i rapporten, herunder i avsnittet om stikkprøver.

Videre oppfattet Finanstilsynet metodikken bak den løpende klassifiseringen som svært enkel og ulogisk på flere måter, blant annet ved at alle risikoindikatorer for personkunder var vektet identisk i den algoritmebaserte logikken. Alle indikatorer for bedriftskunder var også vektet tilsvarende. Basert på en samlet gjennomgang av systemet fant Finanstilsynet det svært lite sannsynlig at kunder ble klassifisert som høyrisiko og dermed underlagt forsterkede tiltak, med mindre en av de faste/triggerbaserte reglene ble utløst. Dette var også fordi kombinasjonsrisiko ikke var ivaretatt ved den underliggende poengtildelingen som lå til grunn for de algoritmebaserte reglene. Systemet hensyntok dessuten kun data som automatisk ble hentet fra ulike eksterne kilder, som Folkeregisteret, Brønnøysundregisteret, Skatteregisteret og Bisnode, og ikke informasjon som kundene selv måtte inngi. Kundespesifikk informasjon, herunder om formål og tilsiktede art, midlenes opprinnelse, mengden kundemidler, transaksjoners størrelse og regelmessighet, jf. lovens § 9, var således ikke hensyntatt i den løpende scoringen.

Etter Finanstilsynets vurdering eksisterte det lite sammenheng mellom logikk, valgte risikoparametere og metodikk i de ulike systemene, blant annet i vektingen av høyrisikobransjer,

produkter og land. Finanstilsynet bemerket også at systemet for løpende klassifisering vektla andre risikofaktorer enn det som var tilfellet i systemet ved etablering. Kundeforholdet var derfor allerede etablert når disse øvrige risikoene ble vurdert. Flere av risikoene som var definert ut fra høyrisikofaktorer i systemet ved etablering av kundeforholdet hadde videre ikke betydning for den løpende klassifiseringen. Kunder som ble ansett for å være høyrisiko ved etablering, basert på bankens egne vurderinger og vektning av ulike risikofaktorer, ble dermed ikke nødvendigvis ansett å innebære høy risiko i den løpende oppfølgingen, og omvendt.

Finanstilsynet pekte i foreløpig rapport på den økte risikoen for feil i bankens risikoklassifisering av kunder ved at flere systemer, med ulike forutsetninger og muligheter hva gjelder metodikk, sammen skal ivareta kundens risikoklasse og i utgangspunktet reflektere samme logikk. Dette krever blant annet at tilstrekkelig datakvalitet, flyt, testing og integrasjon mellom de ulike systemene til enhver tid er sikret, men også at aktuelt risikonivå følger kundene i de forskjellige systemene, jf. også kommentarer under kapitlet om elektronisk overvåking. De ulike forutsetningene systemene baseres på, påvirker etter Finanstilsynets syn nødvendigvis kvaliteten på kundenes endelige risikoklassifisering.

Finanstilsynet vurderte at banken i praksis ikke har et system for risikoklassifisering. Mottatt dokumentasjon til tilsynet viste også at kun 1,3 prosent av bankens totale kundemasse var identifisert å utgjøre høy risiko og dermed underlagt forsterkede kundetiltak. Av personkundene, som utgjør nesten 97 prosent av bankens totale kundemasse, var kun 0,1 prosent klassifisert som høyrisiko etter at PEP ble ekskludert. Flere av disse var dessuten også blitt klassifisert med høy risiko i etterkant av gjentatte alarmer om mistenkelige transaksjoner og/eller rapportering til Økokrim. Det fremkom også av innsendt dokumentasjon at antallet bedriftskunder med høy risiko var unøyaktig grunnet feil på bransjekoder i systemet for løpende klassifisering, noe som følgelig reiste spørsmål ved troverdigheten av de tallene som ble presentert under tilsynet, samt bankens kontroll med egen kundemasse.

Det ble også opplyst at 198 kunder ikke hadde risikoklassifisering grunnet mangler i data som hentes fra Bisnode. Banken manglet også per 31. september 2021 fortsatt informasjon om reelle rettighetshavere på 13 171 bedriftskunder, noe som utgjør 54 prosent av det totale antallet bedriftskunder. Dettens skyltes også mangler i informasjon som automatisk ble hentet fra Bisnode. Videre kunne banken ikke dokumentere at den hadde legitimasjon på omtrent 30 000 kunder. Etter Finanstilsynets vurdering tilsier også omfanget av mangler som eksisterer i nødvendig og lovpålagt kundeinformasjon, at antallet høyrisikokunder burde vært enda høyere.

Banken manglet videre informasjon om formål og tilsiktede art for en stor andel av kundemassen, der dette også av banken selv var ansett å være nødvendig kundeinformasjon. Banken opplyste under tilsynet at 82,6 prosent av bankens kredittkort- og forbrukslånskunder manglet slik nødvendig informasjon, ettersom spørsmålet til kundene først ble implementert i juni 2021. Finanstilsynet fikk i ettersendt dokumentasjon også opplyst at 51 310 av innskuddskundene manglet informasjon om formål og tilsiktede art. Etter Finanstilsynets syn svekker dette ytterligere troverdigheten av tallene banken har presentert om risikoklassifiseringen, da mangler i kundeinformasjonen nødvendigvis påvirker bankens evne til å risikoklassifisere kundene riktig. Det vises for øvrig til kommentarer om manglende kundeinformasjon som nevnt under avsnittet om stikkprøvene.

Finanstilsynet bemerker at det ovennevnte ikke er uttømmende, men et utvalg av kritikkverdige forhold ved bankens risikoklassifisering og nåværende metodikk som særlig peker seg ut.

Finanstilsynet finner det alvorlig at banken ikke etterlever kravene til risikoklassifisering og viser til at dette har den uheldige effekten at kunder forbundet med høyere risiko ikke blir underlagt forsterkede kundetiltak, både ved etablering og i den løpende oppfølgingen. Banken kan således heller ikke påvise at tiltakene til enhver tid er tilpasset den aktuelle risikoen. Finanstilsynet bemerker at det fortsatt gjenstår en stor mengde arbeid med systemene for å heve kvaliteten, herunder utvikling av tilstrekkelige regler, testing, forbedring av datakvaliteten og integrasjon mellom de ulike systemene, noe som også er påpekt i bankens egen risikovurdering, internkontrollrapport for 2020 og ulike revisjonsrapporter.

Under tilsynet ble det også klart at svakheter i systemene ikke var nye for banken, da mangler over tid hadde blitt kommunisert, blant annet i revisjonsrapporter. Imidlertid redegjorde banken under det stedlige tilsynet for at det nå var iverksatt en rekke tiltak på området. Finanstilsynet viste i den foreløpige rapporten til at hovedvekten av tiltakene som ble beskrevet under tilsynet, nylig (i perioden juni til august 2021) var blitt vedtatt og satt i system, samt at en rekke tiltak ikke hadde frist før langt ut i 2022. Dette på tross av at bankens egen risikovurdering fra 2019 også beskrev en rekke svakheter og mangler ved eksempelvis risikoklassifiseringen. Finanstilsynet mener banken på et mye tidligere tidspunkt burde ha iverksatt tiltak og avsatt ressurser for raskere å kunne etterleve gjeldende lovkrav. Finanstilsynet understreket i foreløpig rapport at styret og ledelsen har et særlig ansvar for å påse at adekvate tiltak iverksettes når mangler identifiseres og rapporteres, og for at tilstrekkelige ressurser prioriteres slik at banken snarlig etterlever relevant regelverk.

Basert på det ovennevnte var Finanstilsynets vurdering i foreløpig rapport at bankens risikoklassifiseringsmetodikk på tidspunktet for tilsynet ikke var egnet til å avdekke kunders reelle risiko for hvitvasking og terrorfinansiering. Finanstilsynets vurdering var at banken ikke etterlevde kravene i hvitvaskingsloven § 9. Basert på omfanget av identifiserte mangler i nødvendig og lovpålagt kundeinformasjon, som skal ligge til grunn for risikoklassifiseringen, var det også Finanstilsynets vurdering at banken hadde omfattende mangler i etterlevelsen av krav til kundetiltak, jf. lovens §§ 12 og 13.

I tilsvaret erkjenner styret at den nåværende risikoklassifiseringsmodellen ikke fullt ut reflekterer risikoen identifisert i bankens risikovurdering og heller ikke i tilstrekkelig grad vurderer risiko. Likevel fremhever styret at det er en forskjell på fullstendig manglende etterlevelse og beste praksis. Styret viser til at banken vurderer risikoen knyttet til hvert kundeforhold, selv om metodikk og synkronisering av systemer er vurdert til å ikke være tilstrekkelig tilpasset banken. Finanstilsynet kan imidlertid ikke se at anførselene i tilsvaret gir grunnlag for å endre vurderingen i foreløpig rapport. Finanstilsynet viser til at omfanget og alvorligheten av manglene som beskrives i denne rapporten, samt fraværet av tiltak som kompenserer for disse, gjør at systemene ikke kan anses som egnede til å fange opp risiko og klassifisere kunder i henhold til regelverket. De hensyntar videre ikke momentene som minimum skal hensyntas etter hvitvaskingsloven § 9. Finanstilsynet fastholder derfor vurderingen fra foreløpig rapport.

Finanstilsynet merker seg styrets kommentar hva gjelder planlagt arbeid med systemene for risikoklassifisering, og forventer at banken gjør nødvendige endringer snarest, slik at regelverket etterleves.

## 6. Kundetiltak – Stikkprøver av etterlevelsen

### Rettslig grunnlag og Finanstilsynets forventninger

Banken plikter å gjennomføre kundetiltak etter hvitvaskingslovens kapittel 4 på grunnlag av en vurdering av risikoen for at banken blir utnyttet som ledd i hvitvasking og terrorfinansiering. Banken skal innhente, dokumentere og vurdere informasjon om kunden for å gjøre seg kjent med denne, samt kundeforholdets formål og tilsiktede art. På bakgrunn av informasjonen skal banken vurdere risikoen for at kunden er involvert i hvitvasking eller terrorfinansiering og klassifisere denne i henhold til risikoen, jf. hvitvaskingsloven § 9. Banken plikter å løpende gjennomføre kundetiltak, jf. § 24. Formålet er å tilpasse den løpende oppfølgingen av kunden i henhold til hvitvaskings- eller terrorfinansieringsrisikoen. For kundeforhold som innebærer høy risiko for slik utnyttelse, skal det gjennomføres forsterkede kundetiltak, jf. hvitvaskingsloven § 17. Gjennomførte kundetiltak skal dokumenteres og lagres, jf. hvitvaskingsloven § 30, og foretaket skal ha systemer som muliggjør raske og fullstendige svar på forespørsler fra blant annet tilsynsmyndigheten.

### Bankens etterlevelse og Finanstilsynets vurderinger

Som del av det stedlige tilsynet ble det foretatt stikkprøvekontroller for å bedre kunne vurdere systemenes funksjonalitet og kvalitet opp mot kravene i gjeldende regelverk og bankens rutiner. Det ble foretatt stikkprøver av både fysiske og juridiske personer i ulike risikoklasser og innenfor ulike produktområder. Etter Finanstilsynets vurdering underbygger stikkprøvene manglene som er påpekt ellers i denne rapporten. Nedenfor følger et sammendrag av funnene som ble avdekket. Finanstilsynet viser til nærmere omtale av funnene i foreløpig tilsynsrapport.

#### Mangler i risikoklassifiseringen av kunder

Mottatte stikkprøver av høyrisikokunder besto utelukkende av kundeforhold med PEP-treff eller kundeforhold der de faste/triggerbaserte-reglene i den løpende klassifiseringen var utløst, herunder kunder satt til høy risiko i etterkant av rapporteringer til Økokrim. Dette på tross av at flere av de algoritmebaserte risikofaktorene var til stede ved mange av kundeforholdene Finanstilsynet undersøkte, men hvor poengsummen ikke var tilstrekkelig til å utløse kategoriseringen "høy risiko". Kunder ble heller ikke klassifisert som "høy risiko" ved ulike kombinasjoner som etter Finanstilsynets vurdering, og også etter bankens egen risikovurdering, burde utløst et høyere risikonivå. Finanstilsynet etterspurte blant annet informasjon om de fire første juridiske kundene som ble etablert med forsterkede tiltak etter februar 2021, men banken kunne bare vise til to tilfeller.

Stikkprøvene viste også at kunder regelmessig scores til "høy risiko" ved etablering og tas ut til manuell gjennomgang på bakgrunn av risikofaktorer knyttet til kredittområdet og ikke hvitvaskingsområdet. Finanstilsynet påpekte at flere av disse faktorene også kunne være relevante for vurderingen av risikoen for hvitvasking/terrorfinansiering, som eksempelvis hyppige endringer i styret og ledelsen, stadige adresseendringer, usikkerhet knyttet til midlenes/egenkapitalens opprinnelse, objektets verdi, kundens betjeningsevne, nedbetalingstid, m.m. Blant annet viste Finanstilsynet til et konkret kundeforhold som ble plukket ut av systemet på grunn av kredittrisiko, men hvor det etter Finanstilsynets vurdering også eksisterte flere aktuelle hvitvaskingsrisikoer som burde blitt hensyntatt. Det var imidlertid ikke dokumentert noen vurderinger eller tiltak knyttet til risikoen for hvitvasking/terrorfinansiering. Det vises til nærmere omtale i den foreløpige tilsynsrapporten.

### Mangler i forsterkede kundetiltak.

I de få tilfellene hvor banken hadde gjennomført forsterkede tiltak, var heller ikke disse tilpasset den aktuelle risikoen eller tilstrekkelige til å sikre kjennskap om kunden, reelle rettighetshavere, kundeforholdets formål og tilsiktede art, jf. hvitvaskingsloven § 17. Mottatte stikkprøver av PEP-kunder redegjorde i all hovedsak for et gjennomført googlesøk på kundene, samt korte kommentarer som inneholdt antakelser på bakgrunn av søket og automatisk innhentet informasjon fra skattelikningen. Utover dette var det ikke gjennomført andre forsterkede tiltak eller hentet annen informasjon fra kundene. Finanstilsynet kunne heller ikke se at tiltakene som ble beskrevet i stikkprøvene av PEP, var tilstrekkelige til å kunne fastslå formuens og midlenes opprinnelse, jf. § 18.

### Mangler i data om kundene

Stikkprøvene viste også mangler i innhenting av kundeinformasjon ved etablering av kundeforhold. Flere påkrevde felt i kundebildene sto tomme. I flere tilfeller eksisterte det svært lite informasjon utover det som ble hentet automatisk fra ulike eksterne kilder. Det var videre ikke gjennomført andre tiltak for å innhente informasjonen som manglet, heller ikke i de tilfellene hvor kunden var vurdert manuelt på grunn av høy score i systemet ved etablering. Som påpekt tidligere i rapporten har banken omfattende mangler i kundeinformasjonen om formål og tilsiktede art, noe som underbygges av funnene i stikkprøvene. Bankens erkjente også selv under tilsynet at det i flere tilfeller manglet nødvendig kundeinformasjon. Revisjonsrapporter peker på at dette også skyldes eksisterende mangler i etterlevelsen hos oppdragstaker av utkontrakterte oppgaver. Stikkprøvene underbygget dette, hvor informasjon om blant annet midlenes opprinnelse og ansettelsesforhold særlig var mangelfullt for kunder etablert via tredjepart med produktet "Auto Indirect". Finanstilsynet understreket i foreløpig rapport at banken selv innehar ansvaret for etterlevelse av regelverket også der oppgaver er utkontraktert. Mangler i kundeinformasjonen påvirker bankens evne til å foreta en risikobasert oppfølging av kundeforhold, da slik informasjon er en forutsetning for å kunne gjennomføre tilstrekkelig risikoklassifisering og løpende oppfølging, jf. §§ 9 og 24.

### Manglende legitimasjon.

Finanstilsynet kunne ikke gjennom stikkprøvene verifisere at legitimasjon var innhentet, da dette ikke fremkom av innsendt dokumentasjon. Finanstilsynet ble gjennom tilsynet kjent med at banken ikke kan dokumentere gyldig legitimasjon for om lag 30 000 av sine kunder. Ifølge banken skyldes dette enten at dokumentasjonen ikke finnes, at den er lagret i arkiv som ikke er tilgjengelige i bankens systemer, at kunder er legitimert under andre regelverk eller at kvaliteten er for dårlig.

I foreløpig rapport fant Finanstilsynet det nødvendig å understreke bankens plikt til løpende å følge opp kundeforhold, og at gyldig legitimasjon i alle tilfeller skal innhentes før kundeforholdet etableres. Videre plikter banken å gjennomføre kundetiltak som ledd i løpende oppfølging, og kundetiltak skal uansett gjennomføres når det er tvil om tidligere innhentede opplysninger er korrekte eller tilstrekkelige, jf. hvitvaskingsloven § 24 annet ledd. Finanstilsynet minnet også om at loven § 30 pålegger banken å ha systemer som muliggjør raske og fullstendige svar til tilsynsmyndigheten, noe som følgelig også setter krav til lagringsmåten for opplysninger og dokumenter. Bankens manglende tilgang til fullstendig kundeinformasjon har innvirkning på muligheten til å foreta løpende oppfølging av kundeforholdene. Usikkerheten rundt det faktiske antallet kunder det mangler informasjon om, og hvor mange som faller inn under hver av de nevnte kategoriene, reiser ytterligere spørsmål ved bankens faktiske kontroll på egen kundemasse, risiko og

etterlevelse. Mangelfull tilgang til fullstendig informasjon vil påvirke bankens risiko for å bli utnyttet til hvitvasking og terrorfinansiering.

#### Manglende identifisering av reelle rettighetshavere

Finanstilsynet fant også mangler i dokumenterte tiltak for å identifisere reelle rettighetshavere, samt i å forstå eierskap og kontrollstrukturen til juridiske personer, jf. hvitvaskingsloven § 13. Under tilsynet ble det klart at banken fortsatt manglet informasjon om reelle rettighetshavere på 13 171 av bedriftskundene. I januar 2021 var tallet 18 857. Banken redegjorde under tilsynet for at dette i hovedsak skyldtes mangelfull informasjon i Bisnode. Finanstilsynet understreket at banken selv er ansvarlig for etterlevelsen av regelverket, uavhengig av hvilke kilder banken benytter eller om banken utkontrakterer oppgaver.

Ettersom alle data om reelle rettighetshavere ble hentet automatisk fra Bisnode, stilte Finanstilsynet i foreløpig rapport også spørsmål ved hvordan banken ivaretar kravene i hvitvaskingsloven § 13 om å forstå eierskaps- og kontrollstrukturen til kundene. Finanstilsynet viste blant annet til at det er kjent at Bisnode ofte har mangler i slik informasjon hva gjelder selskaper med utenlandsk eierskap, og at banken plikter å innhente slik informasjon før kundeforholdet etableres. Banken erkjente at den har mangelfull etterlevelse hva gjelder dokumenterte tiltak for å forstå eierskap og kontrollstruktur, men fremhevet samtidig at de fleste av bankens kunder er helnorske med enkle eierskapsstrukturer hvor informasjonen foreligger. Imidlertid underbygges bankens manglende etterlevelse av kravene i § 13 av funn i stikkprøvene, hvor Finanstilsynet avdekket at reelle rettighetshavere ikke var identifisert, eksempelvis for kunder hvor strukturen omfattet utenlandske selskaper.

#### Manglende løpende oppfølging, herunder også av kunder med høy risiko

Stikkprøvene avdekket også mangler i den løpende oppfølgingen av kundeforhold. Blant annet fikk ikke Finanstilsynet dokumentasjon som viste at andre løpende kundetiltak, som eksempelvis transaksjonsanalyser, ble utført utover det som ble gjort automatisk av transaksjonsovervåkingssystemet. Finanstilsynets oppfatning var at det kun var kunder med systemgenererte alarmer om mistenkelige transaksjoner som var gjenstand for transaksjonsanalyser, herunder analyser som omfattet vurdering av om transaksjoner var i samsvar med innhentet kundeinformasjon. Finanstilsynet pekte i foreløpig rapport videre på at det heller ikke ble hentet ny informasjon fra kundene i etterkant av etablering, utover det som automatisk ble hentet fra eksterne kilder, eksempelvis om formål, tilsiktede art eller midlenes opprinnelse. Det ble heller ikke gjennomført andre risikobaserte tiltak for å sikre kjennskap til kunden og kundeforholdet. Dette var også fremhevet som en svakhet i bankens egen risikovurdering. Finanstilsynet viste til at dette videre ble reflektert i overvåkingssystemets valgte logikk, som kun benyttet generiske data automatisk hentet fra ulike eksterne kilder og ikke hensyntok kundespesifikk informasjon, som oppgitt informasjon om formål, tilsiktede art og midlenes opprinnelse. Videre ble dette underbygget av de store restanselistene på periodisk løpende oppfølging, se neste avsnitt, som banken begrunnet med at det var utfordringer knyttet til å innhente nye og oppdaterte kundeopplysninger. Finanstilsynet viser også til tidligere merknader i denne rapporten.

Finanstilsynet kunne ikke se at bankens løpende oppfølging av høyrisikokunder skilte seg fra oppfølgingen av øvrige kunder med lav og normal risiko på annen måte enn at systemet trigget en manuell periodisk gjennomgang av kundeforholdet hvert år, i stedet for hvert tredje år. Det forelå imidlertid ingen dokumenterte vurderinger eller redegjørelser som viste at kunder hadde vært

gjenstand for slik oppfølging, eller at ytterligere risikobaserte tiltak var blitt, eller løpende ble gjennomført. Det forelå heller ingen redegjørelser for kundens valgte risikonivå. Finanstilsynets oppfatning var at det i stor grad ble stolt på den løpende risikoscoren og alarmene som systemet automatisk genererte. Dette ble underbygget av hvordan rutinene var formulert, ved at de i hovedsak beskrev systemene og deres funksjonalitet, heller enn hvilke vurderinger som skal legges til grunn.

Under tilsynet ble det klart at banken også hadde et stort antall kunder på restanseliste som skulle vært gjenstand for periodisk løpende oppfølging. På forespørsel fra Finanstilsynet fremla banken dokumentasjon som viste at totalt 565 251 kundeforhold skulle vært gjenstand for periodisk løpende oppfølging, men som ikke hadde blitt fulgt opp. Det utgjorde 71,5 prosent av det totale antallet kunder i banken. Av disse var 9 001 kunder klassifisert som høyrisikokunder. Banken forklarte restansene med at de hadde utfordringer med å innhente nye og oppdaterte kundeopplysninger og informasjon. For Finanstilsynet fremsto det som at banken heller ikke hadde en konkret plan for å redusere restansene. Basert på bankens svar og dokumentasjon, var Finanstilsynets forståelse at det for flere av kundene dreide seg om en betydelig overskridelse av bankens egne frister for løpende oppfølging.

Finanstilsynet viste i foreløpig rapport til omtalen av mangler i bankens transaksjonsovervåking, at banken kun hadde ni regler, hvorav mange var begrenset til spesifikke produkter, samt til fraværet av regler for bankens høyrisikokunder. Finanstilsynet merket seg at kundeforhold som skulle vært gjenstand for løpende oppfølging, ikke hadde blitt fulgt opp. Dette gjaldt særlig det store antallet kundeforhold som var identifisert å utgjøre høy risiko for hvitvasking og terrorfinansiering, og som skulle vært underlagt løpende forsterkede kundetiltak. Av de totalt 10 544 kundene klassifisert som høy risiko, var 85 prosent ikke blitt fulgt opp.

#### Mangler i undersøkelsene av alarmer

Finanstilsynet avdekket også mangler i tilstrekkelige undersøkelser av alarmer.

Finanstilsynet kunne ikke se at det i de aktuelle sakene ble gjennomført tilstrekkelige undersøkelser slik at mistanken kunne anses avkrefet, da konklusjonene utelukkende var basert på korrespondanse med andre banker og antakelser gjort i lys av dette. Ut fra bankens rutineverk, observasjoner under tilsynet samt gjennomgang av stikkprøver, fant Finanstilsynet at banken hadde vesentlige mangler i gjennomføringen av undersøkelser av mulige mistenkelige forhold. Utgangspunktet for undersøkelser var også vanskelig siden banken i mange tilfeller manglet nok informasjon om kunden til å kunne avgjøre om kundens transaksjoner var uvanlige eller avvikende fra forventet adferd. Med dette utgangspunktet fremsto det som desto mer mangelfullt at undersøkelsene av mulig mistanke ikke omfattet kontakt med, eller innhenting av informasjon fra, kunden. I samtlige stikkprøver, med ett unntak, var bankens eneste ytterligere informasjonskilde opplysninger gitt av andre banker, og mistanken var avskrevet basert på en erklæring om at den andre banken ikke fant transaksjonene mistenkelige. I disse stikkprøvene var det heller ikke innhentet ytterligere underlagsmateriale, dokumentasjon av faktiske gjennomførte kundetiltak, eller vurderinger som underbygget den andre bankens konklusjon. Det ble ikke gjennomført egne undersøkelser utover dette.

Finanstilsynet viste i foreløpig rapport til at informasjon fra andre banker kan være egnet til å avkrefte mistanker om hvitvasking og terrorfinansiering, men det må i hver enkelt sak vurderes

hvilke konkrete handlinger som er nødvendige og egnede for å belyse og oppklare mistankegrunnlaget. Undersøkelsene må med andre ord være innrettet etter mistankegrunnlaget. Informasjon fra andre banker vil i mange tilfeller ikke være tilstrekkelig for å etterleve undersøkelsesplikten, og i alle tilfeller må informasjonen være substansielt egnet til å opplyse mistankegrunnlaget (ikke kun et binært ja/nei-svar på om den andre banken finner kundens adferd mistenkelig). Informasjonen fra den andre banken må vurderes i lys av Santanders informasjon om kunden og adferden som utløste alarmen hos Santander selv.

Finanstilsynet understreket at hver alarm skal behandles, og at alarmer ikke nødvendigvis kan lukkes utelukkende på bakgrunn av undersøkelser som er gjort i forbindelse med andre utløste alarmer. Stikkprøvene viste også at det går lang tid fra alarmene utløses til sakene undersøkes og eventuelt blir lukket eller rapportert til Økokrim, se også merknader i kapittelet om elektronisk overvåking.

Videre påpekte Finanstilsynet at stikkprøvene indikerte mangler i bankens hendelsesbaserte løpende oppfølging. I alarmutredningen fremsto det ikke som at banken søkte å oppdatere kundeinformasjon eller risikovurderingen av kunden i lys av hendelsen, for å eksempelvis avdekke midlenes opprinnelse; om informasjon kunden tidligere hadde gitt var korrekt eller tilstrekkelig; eller om adferd var i tråd med Santanders egen kjennskap til kunden. I etterkant av alarmene ble det heller ikke gjennomført kundetiltak for å sikre fremtidig kjennskap om eksempelvis formål og tilsiktede art. Ettersom det ikke ble gjort egne kundetiltak, var banken heller ikke i stand til å vurdere om fremtidige og lignende transaksjoner kunne anses naturlige for kundeforholdet.

Finanstilsynet oppfatter ut fra tilsvaret at styret i hovedsak er enig i Finanstilsynets vurderinger hva gjelder manglene i stikkprøvene. Finanstilsynet fastholder derfor vurderingen fra foreløpig rapport om at banken på tidspunktet for det stedlige tilsynet hadde omfattende mangler i etterlevelsen av kravene i hvitvaskingsloven §§ 9, 12, 13, 17, 18, 24, 25 og 30. Finanstilsynet merker seg for øvrig styrets redegjørelser, herunder om tiltak på området.

## **7. Systemer for elektronisk overvåking**

### **Rettslig grunnlag og Finanstilsynets forventninger**

Hvitvaskingsloven § 24 stiller krav til løpende oppfølging, som blant annet innebærer å påse at transaksjoner som utføres i kundeforholdet er i samsvar med den rapporteringspliktiges innhentede opplysninger om kunden, kundens virksomhet og risikoprofil, midlenes opprinnelse og kundeforholdets formål og tilsiktede art. Videre stiller lovens § 25 krav til at det *alltid* skal gjennomføres nærmere undersøkelser dersom det avdekkes forhold som avviker fra bankens kjennskap til kunden, kundeforholdets formål og tilsiktede art, dersom en transaksjon synes å mangle et legitimt formål, er usedvanlig stor eller kompleks, er uvanlig for kundens kjente mønster av transaksjoner, er til eller fra person i et land eller et område som ikke har tilfredsstillende tiltak mot hvitvasking og terrorfinansiering eller på annen måte har uvanlig karakter. Dersom nærmere undersøkelser ikke avkrefter mistanken, skal forholdet rapporteres til Økokrim, jf. hvitvaskingsloven § 26. Banken skal videre lagre opplysninger og dokumenter som er innhentet og utarbeidet i forbindelse med tiltak etter hvitvaskingsloven §§ 9 til 26, jf. § 30. I hvitvaskingsloven § 38 stilles eksplisitte krav til at banken skal ha elektroniske overvåkingssystemer.

Hvitvaskingsloven §§ 26 og 27 omhandler plikten til å rapportere mistenkelige transaksjoner til Økokrim, herunder hovedregelen om at en mistenkelig transaksjon ikke skal gjennomføres før



Økokrim er underrettet. Unntaket i § 27 andre ledd gjelder de situasjoner der stans av transaksjonen er umulig, eller kan vanskeliggjøre undersøkelser.

Hvitvaskingsforskriften § 7-3 angir minimumskrav til det elektroniske overvåkingssystemet, herunder at reglene i systemet skal være egnet til å avdekke forhold som kan indikere at midler har tilknytning til hvitvasking- og terrorfinansiering, som identifisert i den rapporteringspliktiges risikovurdering, jf. hvitvaskingsloven § 7. Det forventes at systemet omfatter kundespesifikke regler.

Dokumentasjonen skal være versjonsstyrt slik at det er mulig på et tidspunkt tilbake i tid å se hvilke regler en transaksjon er kontrollert mot. Foretaket skal ha rutiner for kvalitetssikring og evaluering av effekten av reglene. Dette innebærer rutiner for test av nye og endrede regler og for oppfølging av treffsikkerheten til reglene. Foretaket skal videre ha rutiner for daglig oppfølging av resultatet av den elektroniske overvåkingen. Alarmer skal behandles uten at det bygger seg opp restanselister på alarmene.

Alarmhåndtering skal skje uten ugrunnet opphold og være risikobasert. Dette betyr at treff i det elektroniske overvåkingssystemet i utgangspunktet skal undersøkes innen en til to dager, jf. rundskriv 8/2019, og videre at foretakene må behandle treffene ut fra hvilken risiko de utgjør for hvitvasking og terrorfinansiering. Dersom det tar lenger tid å igangsette undersøkelser, må foretaket ha en risikobasert begrunnelse for dette.

### **Bankens etterlevelse og Finanstilsynets vurderinger**

I juni 2020 migrerte banken til et nytt system for elektronisk overvåking (AML-systemet). Dette erstattet to tidligere systemer. I foreløpig rapport påpekte Finanstilsynet en rekke mangler ved systemene, som oppsummeres under:

#### Risikoklassifisering av kundene

I den foreløpige rapporten viste Finanstilsynet til merknadene om bankens risikoklassifiseringssystemer, som omtales i rapportens kapittel 5, og den økte risikoen for feil og inkonsistens ved å programmere samme logikk i ulike systemer. Dette ble også omtalt som en aktuell utfordring i bankens egen risikovurdering 2021. Finanstilsynet viste også til at banken på tilsynsmøtet informerte om at det eksisterte en feil i risikoklassifiseringen av bedriftskunder, som gjorde at for mange kunder ble satt på høy risiko. Dette førte til at banken ikke kunne gjengi det korrekte antallet bedriftskunder med høy risiko til Finanstilsynet.

At flere systemer med ulike forutsetninger og metodikk sammen skal ivareta kundens risikoklasse og i utgangspunktet reflektere samme logikk, svekker etter Finanstilsynets vurdering kvaliteten på risikoklassifiseringen og understøttet Finanstilsynets merknader i kapittel 5 om at banken ikke etterlever kravene i hvitvaskingsloven § 9. Finanstilsynet ga i foreløpig tilsynsrapport uttrykk for en forventning om at banken snart iverksetter tiltak for samkjøring av systemenes logikk og kode for risikoklassifisering av kundene. Finanstilsynet viser til styrets svar og Finanstilsynets vurdering av dette under rapportens kapittel 5.

#### Screening mot PEP- og sanksjonslister

Finanstilsynet pekte i foreløpig rapport på at selv om PEP- og sanksjonslistescreening av bedriftskunder omfattet screening av reelle rettighetshavere, manglet banken på tilsynstidspunktet informasjon for majoriteten av bedriftskundene om reelle rettighetshavere. Screeningen kunne

således ikke utelukke sanksjonsliste- eller PEP-treff på manglende reelle rettighetshavere. Finanstilsynet har i etterkant av tilsynet (mars 2022) i tillegg mottatt en hendelsesrapport fra banken som beskriver en feil i selve screeningen av reelle rettighetshavere, slik at screeningen i mange tilfeller heller ikke har fungert der reelle rettighetshavere er registrert. Finanstilsynet fastholder sin vurdering av at banken har mangler i etterlevelsen av kravene i hvitvaskingsloven § 13 fjerde ledd og frysforpliktelsene.

#### Regler i transaksjonsovervåkingssystemet

Elektroniske transaksjons- og/eller kundekontroller kan betegnes som regler, filtre, kontroller, risikoparametre eller scenarier. I denne rapporten brukes betegnelsen "regel" eller "scenario" der "elektronisk transaksjons- og kundekontroll" ikke er skrevet fullt ut.

Banken hadde på tidspunktet for tilsynet kun ni regler, hvorav tre ble kjørt daglig, tre ble kjørt ukentlig og tre ble kjørt månedlig. Den enkelte regel omfattet imidlertid et begrenset antall produkter. Finanstilsynet pekte i foreløpig rapport på at det ikke var mulig ut fra bankens risikovurdering eller dokumentasjon av reglene, å se om banken anså reglene som adekvate for å imøtekomme aktuelle risikoer for hvitvasking og terrorfinansiering, eller hvilke risikoer som utesto å dekke. Med unntak av for to av reglene, ble Finanstilsynet heller ikke presentert analyser som viste at det øvrige systemets kvalitet og treffsikkerhet faktisk var blitt analysert eller vurdert siden systemet ble satt i produksjon.

Finanstilsynet pekte på at reglene i svært liten grad differensierte mellom kunder med høy risiko og kunder med normal risiko. Finanstilsynet påpekte at det kun eksisterte én regel som utelukkende var ment til å overvåke høyrisikokunder. Med unntak av én regel, differensierte heller ikke de øvrige reglene i parametersettingen mellom kunder med normal eller høy risiko. De to nevnte reglene overvåket imidlertid kun kunder som benytter produktet kredittkort, og de øvrige kundene var derfor gjenstand for den samme løpende oppfølgingen uavhengig av den aktuelle risikoklassen. Finanstilsynet fant det kritikkverdige at kunder som var identifisert til å utgjøre en forhøyet risiko for hvitvasking og terrorfinansiering, ikke var underlagt forsterket løpende oppfølging i transaksjonsovervåkingen.

Finanstilsynet pekte videre på at ingen regler kontrollerte om transaksjoner var i samsvar med innhentede opplysninger om kunden, kundens virksomhet og risikoprofil, midlenes opprinnelse eller kundeforholdets formål og tilsiktede art.

Kun to regler omfattet bedriftskunder. Bilforhandlere, herunder med produktet Auto Stock Finance, som i risikovurderingen var vurdert å inneha høy risiko for hvitvasking, var omfattet kun av én regel, og for bedriftskunder hadde denne regelen ikke gitt noen alarmer.

Finanstilsynet viste i foreløpig rapport videre til at flere av reglene hadde svært mange treff og var lite treffsikre, og at låneproduktet i praksis kun var dekket av én velfungerende regel. Det vises til nærmere omtale av reglene i den foreløpige tilsynsrapporten.

Finanstilsynet stilte i foreløpig tilsynsrapport også spørsmål ved bankens logikk knyttet til frekvens på kjøring av reglene, aggregering og "lookback perioder". Finanstilsynet påpekte at kvaliteten til reglene forringes når regler som kjøres ukentlig eller månedlig er begrenset til å måle mot fastsatte daterte perioder som utelukker treff i andre perioder. Kontrollen blir kun en stikkprøve på akkurat det tidspunktet scenariet kjøres. Finanstilsynet forventer at alle scenarier som bruker akkumulerte

data, kontrollerer daglig mot terskelverdiene for den akkumulerte perioden spesifisert for scenariet. Styret har i sitt tilsvarende ikke kommentert dette.

Finanstilsynet har fra styrets svar merket seg at styret har vært kjent med at transaksjonsovervåkingen ikke har vært tilstrekkelig. Banken har undervurdert kompleksiteten i dagens elektroniske overvåkningssystem, og styret erkjenner at banken ikke utførte tilstrekkelig analyse av transaksjonsovervåkingsregler og parametere i forkant av implementeringen av det nye elektroniske overvåkningssystemet i 2020.

### Behandling av alarmer

Banken hadde på tilsynstidspunktet et etterslep på 14 684 ubehandlede alarmer fra den elektroniske transaksjonsovervåkingen, og en gjennomsnittlig behandlingstid av alarmene på 110 dager. På tilsynsmøtet ble Finanstilsynet informert om at banken nå hadde økt ressursene til å behandle etterslepet av alarmer. Imidlertid ble alarmer fra enkelte scenarioer prioritert over andre, slik at alarmer fra øvrige scenarier lå ubehandlet i systemet i enda lengre tid. Det totale etterslepet var på tilsynstidspunktet forventet å først være ferdig behandlet 1. januar 2022. Finanstilsynet ba i foreløpig rapport banken bekrefte at etterslepet av alarmer var ferdig behandlet innen den planlagte fristen.

Finanstilsynet merker seg fra styrets svar at etterslepet av automatisk genererte alarmer var ferdig behandlet 28. november 2021, og at alarmene generert som følge av tidligere rapporterte hendelser, var ferdig behandlet 23. mars 2022. Styret informerer i sitt svar om at deler av alarmene har blitt analysert og lagt i "dvale" etter rekalkibreringen av regler og parametere, som vil si at alarmene ikke vil bli behandlet med mindre en ny alarm eller tilsvarende trigger på bakgrunn av løpende oppfølging, oppstår. Beslutningen er ifølge banken basert på "stordataanalyser og et særlig lavt antall rapporter om mistenkelig aktivitet sett i forhold til utløste alarmer, som viste at disse alarmene ikke omhandlet forhold som var mistenkelige eller uvanlige". Styret spesifiserer imidlertid ikke hvor mange alarmer som faktisk identifiserte mistenkelig aktivitet.

Finanstilsynet finner det kritikkverdig at banken ikke behandler alle alarmer, ettersom det faktisk er oppdaget mistenkelig aktivitet i alarmene som er blitt undersøkt. Finanstilsynet stiller seg spørrende til hvordan banken kan være sikker på at alarmene ikke omhandler forhold som utløser undersøkelsesplikt, også med tanke på at transaksjonsovervåkningssystemet ikke hensyntar innhentede data om kunden. Selv om regler på et senere tidspunkt er kalibrert fordi de gav for mange treff, kan det ikke utelukkes at reglene utløste alarmer som kunne avdekket mistanke om hvitvasking eller terrorfinansiering. Finanstilsynet forutsetter derfor at samtlige alarmer gjennomgås.

Finanstilsynet påpekte i foreløpig rapport at sett i lys av etterslepet av alarmer og gjennomsnittlig behandlingstid for alarmene, fremsto bankens tidsfrister for behandling av alarmene ikke å være relevante. Finanstilsynet vurderte at etterslepet av alarmer som hadde bygd seg opp etter at det nye systemet ble tatt i bruk i juni 2020, hadde forringet kvaliteten på bankens elektroniske transaksjonsovervåking. I tillegg til at en tredjedel av et allerede fåtall regler åpenbart ikke avdekket den risikoen for hvitvasking eller terrorfinansiering det var ment å gjøre, syntes etterslepet også å ha fjernet oppmerksomhet fra ferske alarmer på de andre scenariene.

Finanstilsynet kan ikke se at det oppstilles forhold i styrets tilsvare som gir grunn til å endre Finanstilsynets vurdering fra foreløpig rapport.

Basert på ovennevnte fastholder Finanstilsynet derfor vurderingen om at banken på tilsynstidspunktet hadde store mangler i det elektroniske overvåkingssystemet, og at systemet ikke sikret at banken etterlevde kravene i hvitvaskingsloven §§ 24, 25, 26 og 27. Banken anses også å ha overtrådt hvitvaskingsforskriften § 7-3 andre ledd. Hele produktgrupper og kundegrupper manglet i praksis transaksjonsovervåking. Risikovurderingens identifiserte risikoer var ikke gjenspeilet i reglene, og det manglet en kartlegging av om reglene dekket alle risikoene. Reglene var få, og mange var lite treffsikre. Ukentlige og månedlige scenarier ble kjørt sjeldent og målte mot tilfeldige perioder. Det var store restanser på behandlingen av alarmer som medførte at det gikk lang tid fra forholdet som utløste alarmen, oppsto, til det ble undersøkt. Finanstilsynet finner det ikke tilfredsstillende at alarmer legges i 'dvale' og ikke undersøkes med mindre det oppstår en ny alarm.

### **IKT-forskriften: Rettslig grunnlag og Finanstilsynets forventninger**

IKT-forskriften omfatter IT-systemer som er av betydning for foretakets virksomhet, herunder bankens elektroniske overvåkingssystem for å avdekke hvitvasking og terrorfinansiering og systemene som leverer data til dette.

IKT-forskriften § 5 stiller krav til at foretaket skal utarbeide prosedyrer som skal sikre beskyttelse av utstyr, systemer og informasjon av betydning for foretakets virksomhet mot skader, misbruk, uautorisert adgang og endring, samt hærverk. Videre skal prosedyrene inneholde retningslinjer for tildeling, endring, sletting og kontroll med autorisasjon for tilgang til IKT-systemene. Finanstilsynet forventer at banken har etablerte rutiner og kontroller som skal sikre beskyttelse mot misbruk, uautorisert adgang og endring av informasjon i systemer med betydning for bankens arbeid med å avdekke hvitvasking og terrorfinansiering, herunder kjernesystemer, datavarehus og elektroniske overvåkingssystemer.

IKT-forskriften § 8 stiller krav til at drift av IKT-virksomheten skal være basert på dokumenterte prosedyrer, som sikrer fullstendig, rettidig og korrekt behandling og oppbevaring av data. IKT-systemer skal ha dokumenterte driftsløsninger som sikrer en tilgjengelighet i tråd med foretakets dokumenterte krav.

IKT-forskriften § 9 stiller krav til at foretaket skal sikre at prosedyrer for avviks- og endringshåndtering foreligger og følges. Prosedyrene for avvikshåndtering skal omfatte alle avvik som oppstår i driften av IKT-systemene. Avviksbehandlingen skal ha som formål å gjenopprette normal tilstand i IKT-virksomheten. Avviksbehandlingen skal identifisere årsaken til avvik, hindre gjentakelser og sikre forsvarlig og formell behandling av avviket. Finanstilsynet forventer at foretaket har dokumenterte rutiner for å håndtere avvikssituasjoner der det elektroniske overvåkingssystemet ikke fungerer som forutsatt. Rutinene skal beskrive hvordan det sikres at alle transaksjoner etterkontrolleres når systemet fungerer igjen. Prosedyrene for endringshåndtering skal omfatte alle endringer som kan påvirke IKT-systemene og skal sikre forsvarlig, formell behandling og dokumentering av endringene. Foretaket skal sikre at prosedyrene for endringshåndtering gir en stabil, planlagt og forutsigbar drift. Finanstilsynet forventer at foretaket har rutiner for å kontrollere at uttrekket av transaksjoner til det elektroniske overvåkingssystemet er komplett etter endringer i kjernesystem, datavarehus eller det elektroniske overvåkingssystemet selv.

IKT-forskriften § 11 stiller krav til at foretaket skal ha etablert og dokumentert en kriseplan som skal iverksettes dersom IKT-driften ikke kan opprettholdes ved en krise som vil si en hendelse som

forårsaker driftsavbrudd slik at foretakets IKT-drift ikke kan fortsette med normalt tilgjengelige ressurser. Finanstilsynet forventer at foretaket bygger sitt planverk på en forretningsmessig kontinuitetsanalyse og risikovurdering. Videre stiller § 11 krav til at det minimum årlig skal gjennomføres opplæring, øvelse og testing av kriseløsningen for å sikre at denne virker som forutsatt. Utfallet av slike tester skal dokumenteres.

### **Bankens etterlevelse og Finanstilsynets vurderinger**

#### Tilgangsstyring, jf. IKT-forskriften § 5

Finanstilsynet vurderte i foreløpig rapport at tilgangsstyringen til AML-systemet ikke var tilfredsstillende. Systemet var ikke omfattet av bankens Identity and Access Management (IAM)-policy og dermed ikke underlagt de samme formaliserte kontrollene og eksterne vurderingen av kontrollutførelsen som policyen beskrev. Finanstilsynet viste til at tilgang til systemet for elektronisk overvåking gir mulighet for å endre regler, parametre og driftsmønstre som kan hindre at hvitvasking eller terrorfinansiering avdekkes.

Fra styrets svar har Finanstilsynet merket seg kompensierende tiltak banken hadde iverksatt for å redusere risikoen for misbruk av systemet, herunder etablert en egen administratorrolle for AML-systemet som begrenser tilgangen til å drifte og parametersette systemet til brukeren med denne tilgangen.

Finanstilsynet har fra styrets svar videre merket seg tiltak banken har iverksatt i etterkant av tilsynet for å styrke tilgangskontrollen til AML-systemet. Finanstilsynet tar styrets svar til etterretning.

#### Logging og oppfølging av logger fra det elektroniske overvåkingssystemet, jf. IKT-forskriften § 5

Finanstilsynet påpekte i foreløpig rapport at logger fra det elektroniske overvåkingssystemet ikke ble overført til bankens system for analyse av loggfiler.

Fra styrets svar har Finanstilsynet merket seg at fra februar 2022 ble loggfiler fra det elektroniske overvåkingssystemet overført til systemet for logganalyse og fra andre kvartal 2022 inkludert i bankens periodiske kontrollaktiviteter for logging og tar det til etterretning.

#### Arkitektur- og plattformssikkerhet, jf. IKT-forskriften § 5

Finanstilsynet viste i foreløpig rapport til en risikovurdering av nettverksinfrastrukturen banken hadde fått utført og mottok resultatene av i januar 2021. Rapporten viste til fem risikoer vurdert som 'Svært høy'. I oversendelsen som Finanstilsynet mottok i august 2021, ble det opplyst om at funnene nylig var overlevert til risikoeier. For Finanstilsynet fremsto det ikke som forenlig med god risikostyring, at risikoer på nettverksområdet klassifisert som 'Svært høy', ble overlevert risikoeier først etter nærmere et halvt år.

I sitt tilsvare fremfører styret at banken på tilsynstidspunktet allerede hadde etablert flere risikoreduserende tiltak og derfor burde kommunisert restrisiko og ikke iboende risiko til Finanstilsynet. Finanstilsynet har merket seg at styret er enig i at alle risikoer vurdert som 'Svært høy' skal adresseres rettidig.

#### Drift av AML-systemet, jf. IKT-forskriften §§ 8 og 9

Finanstilsynet uttrykte i foreløpig rapport forventning om at banken har dokumenterte rutiner for å håndtere avvikssituasjoner der det elektroniske overvåkingssystemet ikke fungerer som forutsatt.

Rutinene skal beskrive hvordan det sikres at alle transaksjoner etterkontrolleres når systemet fungerer igjen.

Finanstilsynet har merket seg at styret bekrefter at banken har slike rutiner. Ved re-kjøring etter en avvikssituasjon, er det sikret at alle transaksjoner som har blitt utført siden forrige vellykkede datalast til AML-systemet, blir inkludert i den nye kjøringen.

#### Endringshåndtering, jf. IKT-forskriften § 9

Finanstilsynet viste i foreløpig rapport til at kvaliteten på dataene som ligger til grunn for den elektroniske kunde- og transaksjonsovervåkingen har vært en utfordring for banken. Blant annet er dette påpekt i rød revisjonsrapport for AML-området fra januar 2021. I tillegg til manglende innhenting av data ved etablering av kundeforhold som omtalt tidligere i denne rapporten, hadde det vært alvorlige hendelser knyttet til at transaksjoner ikke hadde blitt overført fra kjernesystemene til AML-systemet. Dette hadde ikke blitt avdekket før etter lang tid, med den følge at transaksjonene ikke hadde blitt kontrollert. Risikoen for at datagrunnlaget ikke er komplett, er spesielt høy etter fusjoner av systemer og porteføljer og ved konvertering til nye systemer. Dette var årsaken til hendelse rapportert til Finanstilsynet i 2018 og til hendelse rapportert i april 2021. For sistnevnte hendelse fremgikk det av ettersendt dokumentasjon at ca. 462 000 transaksjoner manglet monitorering pga. feil logikk i overføringen fra kjernesystemet til AML-systemet. Det viste seg også vanskelig å rekonstruere manglende transaksjoner.

Finanstilsynet forventet at banken hadde rutiner for å sikre at uttrekket av transaksjoner til det elektroniske overvåkingssystemet var komplette etter endringer i kjernesystemer, datavarehus eller AML-systemet selv. Finanstilsynet stilte spørsmål om rutinene for endringshåndtering, herunder for testing, var tilstrekkelig detaljerte og fulgte hele denne verdikjeden.

Styret viser i sitt svar til at bankens svakheter har vært knyttet til dataflyt og ikke datakvalitet. For Finanstilsynet fremstår denne nyansen som lite relevant så lenge resultatet ble mangelfullt datagrunnlag for kontrollene i AML-systemet.

Styret viser videre til at det på tilsynstidspunktet var gjort forbedringstiltak som at ende-til-ende dataflyt for AML-relaterte systemer hadde blitt dokumentert.

Finanstilsynet har fra styrets svar merket seg at banken i etterkant av tilsynet har etablert kvartalsvise datakvalitetskontroller for å sikre fullstendighet, integritet og sporbarhet mellom kunder, kontoer og transaksjoner, og for å kontrollere dataflyten. Kontrollene iverksettes andre kvartal 2022.

Finanstilsynet viste i foreløpig rapport til at Finanstilsynet tidligere har reagert (ref. overtredelsesgebyr 2019) på at det har tatt lang tid å avdekke mangler i dataoverføringene i Santander. Hendelsen rapportert til Finanstilsynet i april 2021 som det er referert til over, oppsto i forbindelse med konverteringen til nytt AML-system i juni 2020. Finanstilsynet pekte i foreløpig rapport på at ved en slik konvertering er det en åpenbar forhøyet risiko for at denne typen hendelser kan forekomme, og at det er derfor viktig at det ikke bare kontrolleres i første linjen, men også gjøres kontroller i andre linjen.

Fra styrets svar slutter Finanstilsynet at bankens andrelinje ikke vurderte dette som et aktuelt risikoområde å gjøre kontroller på, fordi risikoen allerede var adressert i revisjonsrapporter. Dette underbygger Finanstilsynets kritikk av at det tar for lang tid å avdekke mangler i dataoverføringene i Santander. For hver dag banken kontrollerer mot mangelfullt datagrunnlag, øker risikoen for at mistenkelige transaksjoner ikke blir identifisert. Se også merknadene under punkt 4 i denne rapporten.

#### Kriseberedskap, jf. IKT-forskriften § 11

Finanstilsynet har fra styrets svar merket seg at banken etter tilsynet har etablert gjenopprettingsplan for det elektroniske overvåkingssystemet og gjennomført gjenopprettningstest i første kvartal 2022. Finanstilsynet har videre merket seg at banken årlig utfører en Business Impact Assessment analysis (BIA) i førstelinjen for å identifisere kritiske prosesser. Applikasjoner som understøtter disse prosessene utgjør basis for gjennomføring av IT-gjenopprettningstester, og AML-systemet er omfattet av dette.

Finanstilsynet vurderer at banken har mangler i etterlevelsen av IKT-forskriften, særskilt § 9. Finanstilsynet forventer at styret påser at banken styrker testing og kontroller etter endringer slik at feil etter endringer avdekkes raskere. Finanstilsynet vurderer at det er enkelte mangler også i bankens etterlevelse av IKT-forskriften § 5 og forventer, i tråd med styrets svar, at alle risikoer avdekket i sikkerhetsgjennomganger vurdert som 'Svært høy', adresseres rettidig.

### **8. Finanstilsynets samlede vurdering av foretakets etterlevelse**

Finanstilsynets vurdering er at banken ikke etterlever en rekke av bestemmelsene i hvitvaskingsregelverket. Det er også avdekket mangler i etterlevelsen av IKT-forskriften. Det bemerkes dessuten at tilsynet var avgrenset til å kun gjelde enkelte plikter i hvitvaskingsregelverket, og at manglene som er avdekket, anses alvorlige ettersom de omfatter grunnleggende krav. Finanstilsynet viser videre til at det også etter tilsyn i september 2018 ble pekt på at banken ikke etterlevde flere av de samme bestemmelsene i hvitvaskingsloven. Dette understreker at den manglende etterlevelsen har pågått over lengre tid. Alvorlighetsgraden av den manglende etterlevelsen økes ytterligere av at styret i brev datert 18. oktober 2019, i etterkant av tilsynsrapport og overtredelsesgebyr, bekreftet overfor Finanstilsynet at bankens styre og ledelse ville følge opp at arbeidet med å implementere tiltak for å sikre bankens etterlevelse av hvitvaskingslovens bestemmelser, prioriteres. Styret viste den gangen til en rekke iverksatte tiltak på området, herunder arbeid med å bytte ut systemet for transaksjonsovervåking. Bekreftelsen styret ga i 2019 om at mange av de daværende identifiserte gapene og anbefalingene var håndtert, forsterker etter Finanstilsynets vurdering alvorret i den manglende etterlevelsen Finanstilsynet nå finner ved dette tilsynet.

I lys av den foreløpige rapportens kritikk av styrets oppfølging av bankens manglende etterlevelse, stilte Finanstilsynet også spørsmål ved om styret besitter den nødvendige kompetansen. Finanstilsynet minnet om at banken etter finansforetaksloven plikter å ha et allsidig sammensatt styre, og at styret til sammen oppfyller kompetansekravene, som utdypet i Rundskriv 1/2020. Styret ble derfor bedt om å særskilt kommentere hvilke vurderinger som er gjort av styrets samlede kompetanse innen anti-hvitvasking og terrorfinansiering, og hvilke(n) styremedlemmer som anses å bidra til at kompetansekravet er oppfylt. Finanstilsynet noterer styrets tilsvarende, herunder om tidligere

gjennomførte vurderinger, og om nylige endringer i styresammensetning i etterkant av en ny evaluering i mars 2022.

## 9. Oppsummering

Finanstilsynet mener at manglene i etterlevelsen av hvitvaskingsloven som påpekes i denne rapporten, er alvorlige. Alvoret forsterkes av at det etter tidligere tilsyn er avdekket alvorlige overtredelser av hvitvaskingsregelverket i banken, der banken også er ilagt overtredelsesgebyr. Overtredelsene vurderes videre av Finanstilsynet å være av en art og et omfang som gir grunnlag for å ilegge banken et overtredelsesgebyr.

I foreløpig tilsynsrapport varslet Finanstilsynet et overtredelsesgebyr på NOK 150 000 000, jf. hvitvaskingsloven § 49, basert på overtredelser av lovens §§ 7, 8, 9, 12, 13, 17, 18, 24, 25 og 26.

## 10. Finanstilsynets vurderinger av overtredelsene i foreløpig rapport

Finanstilsynet ga i foreløpig rapport uttrykk for at det er Finanstilsynets vurdering at foretaket ikke har en virksomhetsinnrettet risikovurdering som identifiserer og vurderer risiko i henhold til hvitvaskingsloven § 7. Dette påvirker nødvendigvis etterlevelsen av kravene til risikobaserte kundetiltak, forsterkede kundetiltak og løpende oppfølging, jf. loven §§ 9, 17 og 24. Det anses videre som skjerpene at banken velger å ikke gjennomføre en fornyet risikovurdering i 2020, før nye systemer tas i bruk, da risikovurderingen skal danne utgangspunktet for den risikobaserte tilnærmingen banken skal legge til grunn i implementeringen av systemene og det øvrige arbeidet, herunder i utviklingen av risikoklassifiseringsmetodikken og reglene i transaksjonsovervåkingen. Finanstilsynet understreker at det er nødvendig å identifisere forhold forbundet med høyere risiko innenfor egen virksomhet for å kunne iverksette riktige tiltak, samt allokere ressursene til de områdene hvor hvitvaskings- og terrorfinansieringsrisikoen er størst. Når kundenes og bankens reelle hvitvaskingsrisiko ikke gjenspeiles tilfredsstillende i risikovurderingen, eller i vurderingen av relevante høyrisikofaktorer, får dette nødvendigvis konsekvenser for den videre etterlevelsen av kravene i hvitvaskingsregelverket, herunder den løpende oppfølgingen av kundeforholdene.

Tilstrekkelige, risikobaserte og oppdaterte rutiner, jf. hvitvaskingsloven § 8, er en forutsetning for at foretaket og dets ansatte skal kunne være i stand til å identifisere, vurdere og håndtere ulike typer risiko, samt oppfylle plikter etter bestemmelsene gitt i eller i medhold av hvitvaskingsloven. Det er også vesentlig at rutinene er tilpasset virksomhetens art og omfang, slik at banken kan påvise at iverksatte tiltak er tilpasset virksomhetens risiko. Flertallet av bankens nåværende rutiner på hvitvaskingsområdet ble først etablert sommeren 2021, rett i forkant av tilsynet. Bankens gjeldende rutiner vurderes fortsatt å være mangelfulle og lite operasjonelle, og de gjenspeiler i liten grad risikoene som er påpekt i foretakets egen risikovurdering. Manglende og mangelfulle rutiner påvirker nødvendigvis de ansattes mulighet til å gjennomføre tilstrekkelige vurderinger og iverksette nødvendige tiltak. Det vises til merknadene i rapporten, herunder til den mangelfulle gjennomføringen av tilstrekkelige og risikobaserte kundetiltak som er avdekket i stikkprøvene. Etter Finanstilsynets vurdering må funnene i rapporten ses i sammenheng med det historiske fraværet av tilstrekkelige og oppdaterte rutiner, samt manglene påpekt i tilknytning til risikovurderingen over.

For å avdekke mulig hvitvasking og terrorfinansiering er det nødvendig å identifisere kunder forbundet med høyere risiko og iverksette riktige og tilstrekkelige tiltak. At banken i praksis ikke



har et egnet system for risikoklassifisering, hvor kunder klassifiseres med høy risiko og underlegges forsterkede tiltak, påvirker også den generelle etterlevelsen av relevante lovkrav. Finanstilsynet finner det videre alvorlig at banken på tilsynstidspunktet fortsatt hadde kunder som ikke var risikoklassifisert. Finanstilsynet presiserer at tiltak til enhver tid skal baseres på kundens iboende risiko. Når kundenes iboende risiko ikke i tilstrekkelig grad identifiseres og ikke hensyntas i risikoklassifiseringen og i utførelsen av kundetiltak, innebærer dette at banken også har et mangelfullt utgangspunkt for å gjøre riktige undersøkelser av mistenkelige forhold. Det vil heller ikke være mulig å påvise at omfanget av utførte tiltak er tilpasset aktuell risiko, jf. hvitvaskingsloven § 9 tredje ledd. Finanstilsynets vurdering er at korrekt risikoklassifisering heller ikke er gjennomført for en betydelig del av kundemassen, som følge av manglene i bankens risikovurdering, risikoklassifiseringsmetodikk og utførte kundetiltak.

Manglene i kundetiltak, jf. §§ 12 og 13, innebærer videre at banken ikke har nødvendig informasjon til å foreta en korrekt risikoklassifisering av kundene, jf. vurderingsmomentene i § 9. Finanstilsynet finner det særlig alvorlig at banken fortsatt ikke kan dokumentere gyldig legitimasjon på omtrent 30 000 av sine kunder, samt fortsatt mangler informasjon om reelle rettighetshavere på 13 171 av bedriftskundene. Finanstilsynet understreker at mangler i kundetiltak øker risikoen for at mistenkelige forhold ikke lar seg identifisere, da banken ikke har tilstrekkelig informasjon å basere den risikobaserte tilnærmingen på, herunder informasjon om riktig identitet, reelle rettighetshavere og politisk eksponerte personer. Bankens manglende informasjon om kundeforholdene i realiteten utgjør en økt risiko, ettersom manglende korrekt og tilstrekkelig informasjon også gjør det umulig å vite om blant annet reelle rettighetshavere er politisk eksponerte personer eller personer underlagt sanksjoner.

Manglende informasjon om blant annet midlenes opprinnelse, kundeforholdets formål og tilsiktede art gjør det videre utfordrende å avgjøre om transaksjoner og annen kundeforføring utløser undersøkelsesplikt. Dette kan bidra til underrapportering til Økokrim. Foruten å ha effekt på tilstrekkelig risikoklassifisering, har manglende kundetiltak også en direkte negativ effekt på løpende oppfølging. Herunder nevnes den elektroniske transaksjonsovervåkingens treffsikkerhet, ettersom det er vanskelig å etablere regler som skal fange opp avvik fra normal kundeforføring uten å ha tilstrekkelig informasjon som skal bidra til å avgjøre hva som kan anses normal og legitim adferd for kunden.

Særlig alvorlig er det at banken ikke har gjennomført tilstrekkelige forsterkede kundetiltak tilpasset kundens iboende risiko i henhold til §§ 17 og 18, heller ikke for kunder banken selv har identifisert å utgjøre en høy risiko for hvitvasking og terrorfinansiering. Herunder nevnes også tilstrekkelige kundetiltak for politisk eksponerte personer, som anses å utgjøre en potensiell høy risiko. Finanstilsynet vurderer fraværet av forsterkede kundetiltak, også som del av løpende oppfølging, som alvorlig, da manglende kunnskap og oppfølging av kundeforholdene øker risikoen for at banken utnyttes til hvitvasking og terrorfinansiering.

Videre har banken over lengre tid hatt en mangelfull løpende oppfølging av kundemassen, jf. hvitvaskingsloven § 24. Det vises i den sammenheng til manglende gjennomføring av blant annet risikobaserte og forsterkede kundetiltak, også i etterkant av alarmer, og fraværet av både tilstrekkelige og kundespesifikke regler, samt egne regler for kunder identifisert med høy risiko for hvitvasking og terrorfinansiering. Finanstilsynet kan videre ikke se at banken har benyttet den løpende oppfølgingen til å rydde opp i åpenbare mangler i tidligere gjennomførte kundetiltak, selv om dette er et krav i henhold til lovens § 24 annet ledd. Finanstilsynet finner det videre alvorlig at

det ikke hentes ny informasjon fra kunden i etterkant av kundeetablering, men at banken utelukkende baserer den løpende oppfølgingen, herunder transaksjonsovervåkingen, på generiske data hentet fra ulike kilder.

Finanstilsynet anser ikke bankens løpende oppfølging å være tilstrekkelig for å håndtere ulike kunders iboende risiko. Dette gjenspeiles blant annet i at oppfølgingen av kunder banken selv har identifisert som høyrisikokunder, ikke skiller seg nevneverdig fra oppfølgingen av øvrige kunder med lav og normal risiko. Særlig alvorlig er det at banken har store restanser i den løpende oppfølgingen av kundemassen, herunder av de kunder som er identifisert av banken selv å utgjøre høy risiko. Dette øker risikoen for at banken blir utnyttet til hvitvasking og terrorfinansiering. Sammen med manglene som er påpekt om bankens elektroniske transaksjonsovervåking, anser Finanstilsynet den løpende oppfølging som lite egnet til å identifisere aktuelle indikatorer for mistenkelig adferd. Etter Finanstilsynets vurdering øker manglene som påpekt i omtalen av bankens oppfølging av kundeforholdene, risikoen for at mistenkelig forhold ikke avdekkes, undersøkes og rapporteres til Økokrim.

Finanstilsynet ga i foreløpig rapport også uttrykk for at det vurderer at banken ikke etterlever hvitvaskingslovens krav om undersøkelser og rapportering av mistenkelige transaksjoner til Økokrim, jf. §§ 25 og 26. Banken har blant annet hatt et omfattende etterslep knyttet til undersøkelser av alarmer om mistenkelige forhold. Alarmer har også historisk blitt liggende ubehandlet i systemet over lengre tidsperioder, og langt utover det som kan anses som et rimelig tidsrom for å gjennomføre tilstrekkelige undersøkelser som belyser mistanken. Dette skyldes også bankens prioritering av enkelte alarmtyper over andre alarmer. Også stikkprøvene underbygger at det har gått lang tid fra alarmer ble utløst til undersøkelser ble iverksatt. Finanstilsynet avdekket også i stikkprøvene tilfeller hvor alarmer var avskrevet, men hvor mistanken etter Finanstilsynets vurdering ikke kan anses å være avkrefte. Det er heller ikke gjennomført ytterligere kundetiltak for å håndtere risikoen de aktuelle kundene representerer i lys av alarmene. Finanstilsynet understreker at konsekvensen av manglende oppfølging og undersøkelser av mistenkelige forhold, kombinert med manglende gjennomføring av tilstrekkelige kundetiltak, er at mistenkelig adferd kan vedvare ettersom den ikke identifiseres, undersøkes eller rapporteres av banken.

Finanstilsynet viser til at hvitvaskingsregelverket skal bidra til at rapporteringspliktige forebygger og avdekker hvitvasking og terrorfinansiering, og at banken har en mangelfull etterlevelse på flere områder som samlet sett utgjør en vesentlig svekkelse av muligheten til å etterleve regelverkets krav og formål. Bankens manglende etterlevelse av pliktene i hvitvaskingsregelverket er også tidligere blitt påpekt av Finanstilsynet, blant annet i rapport etter stedlig tilsyn i 2018, uten at banken har gjennomført tilstrekkelige avhjelpende tiltak for å etterleve lovens krav.

Banken ble også i 2019 ilagt et overtredelsesgebyr for overtredelse av lovens §§ 24 og 25, som følge av svikt i den løpende oppfølgingen over lengre tid, hvor en mengde transaksjoner ikke hadde blitt underlagt hvitvaskingskontroll. Finanstilsynet finner det spesielt alvorlig at bankens styre høsten 2019, i etterkant av tidligere tilsyn og overtredelsesgebyr, bekreftet overfor Finanstilsynet at bankens styre og ledelse ville følge opp at arbeidet med å implementere tiltak som skulle sikre bankens etterlevelse av hvitvaskingslovens bestemmelser, ble prioritert. Det vises også til rapportens kommentarer vedrørende bankens styring av risiko, samt nye hendelser rapportert til Finanstilsynet i tilknytning til transaksjonsovervåkingen. Så sent som i april 2021 rapporterte

banken at ytterligere transaksjoner ikke er blitt overvåket, som følge av konverteringen til nye systemer samt tilhørende fusjoner av systemer og porteføljer.

Finanstilsynets gjennomgang viser at det over tid har vært for lav oppmerksomhet om risikoen for hvitvasking og terrorfinansiering, også på tross av internrevisjonens påpekning av vesentlige svakheter i etterlevelsen. Finanstilsynet merker seg også at banken selv har identifisert og rapportert til ledelsen og styret om flere av manglene som påpekes i denne rapporten, uten at avhjelpende tiltak har blitt iverksatt på et tidligere tidspunkt. Manglene er gjennomgripende i hele organisasjonen og har pågått over flere år. Dette må etter Finanstilsynets vurdering ses i sammenheng med at antihvitvaskingsområdet ikke har fått tilstrekkelig prioritet i den overordnede styringen av bankens virksomhet.

## 11. Vurdering av om overtredelsesgebyr bør ilegges

Ovennevnte omhandler overtredelse av bestemmelsene hvitvaskingsloven §§ 7, 8, 9, 12, 13, 17, 18, 24, 25 og 26. Med hjemmel i hvitvaskingsloven § 49 kan overtredelse av disse bestemmelsene medføre overtredelsesgebyr. I vurderingen av om det skal ilegges overtredelsesgebyr, og ved utmålingen av denne, skal det, jf. hvitvaskingsloven § 50, blant annet tas hensyn til:

- a) overtredelsens grovhet og varighet
- b) overtrederens grad av skyld
- c) overtrederens økonomiske evne
- d) den rapporteringspliktiges risikovurderinger etter § 7 og rutiner etter § 8
- e) fordeler som er oppnådd eller kunne ha vært oppnådd ved overtredelsen
- f) om tredjeparter er påført tap
- g) graden av samarbeid med myndighetene
- h) eventuelle tidligere overtredelser av hvitvaskingsloven eller forskrifter med hjemmel i loven

Hvitvaskingsregelverket skal bidra til at rapporteringspliktige forebygger og avdekker hvitvasking og terrorfinansiering. Banken har en mangelfull etterlevelse på flere sentrale områder, som samlet sett utgjør en betydelig svekkelse av muligheten til å avdekke mistanke. Funnene fra tilsynet underbygger også at den mangelfulle etterlevelsen har pågått over lang tid, uten at tilstrekkelige avhjelpende tiltak er blitt iverksatt av bankens styre og ledelse. Lovovertredelsene som er påpekt, anses også alvorlige i lys av virksomhetens karakter, med høy iboende risiko for hvitvasking.

Finanstilsynet finner særlig å peke på fraværet av en virksomhetsinnrettet risikovurdering og historisk fravær av rutiner frem til sommeren 2021, jf. hvitvaskingsloven §§ 7 og 8. En oppdatert og virksomhetsinnrettet risikovurdering skal ligge til grunn for bankens øvrige tiltak på hvitvaskingsområdet, og rutiner skal sikre at banken håndterer identifisert risiko, samt beskrive hvordan banken skal praktisere etterlevelsen. Når banken ikke har en tilstrekkelig forståelse av risiko eller tilstrekkelige rutiner for å håndtere den, vil risikoklassifisering, kundetiltak og løpende oppfølging i liten grad være risikobasert eller treffende. Dette svekker videre bankens mulighet til å oppdage, undersøke og eventuelt rapportere mistenkelige forhold til Økokrim.

Finanstilsynet anser at manglene som er avdekket i rapporten, herunder i stikkprøvene, underbygger konsekvensene av de gjennomgående manglene knyttet til krav om risikovurdering, rutiner, samt risikoklassifisering og løpende oppfølging. Særlig bankens manglende oppfølging av høyrisikokunder anses alvorlig, ettersom forsterket oppfølging av slike kunder er et av de viktigste

tiltakene mot hvitvasking og terrorfinansiering. Finanstilsynet finner det også alvorlig at banken fortsatt har omfattende mangler i grunnleggende kundeinformasjon, jf. §§ 12 og 13, slik som gyldig legitimasjon, informasjon om reelle rettighetshavere, samt informasjon om kundeforholdets formål og tilsiktede art. Dette påvirker nødvendigvis evnen til å foreta korrekt risikoklassifisering og kundetiltak som til enhver tid er tilpasset den aktuelle risikoen. Manglende transaksjonsovervåking, samt manglende etterlevelse av pliktene til å undersøke mistenkelige transaksjoner, er videre alvorlig, ettersom manglende identifisering og rapportering av mistenkelige transaksjoner gjør at hvitvasking og terrorfinansiering ikke avdekkes og dermed heller ikke straffefølges.

De fleste lovkravene som banken ikke etterlever, er også forpliktelser som var gjeldende under hvitvaskingsloven av 2009. Finanstilsynet finner det skjerpene at det fortsatt avdekkes alvorlige mangler i etterlevelsen av de samme bestemmelser og innenfor samme områder som tidligere har vært gjenstand for kritikk fra Finanstilsynet. Det vises til at banken i 2019 fikk overtredelsesgebyr for overtredelse av hvitvaskingsloven §§ 24 og 25 på grunn av mangelfull løpende oppfølging og transaksjonsovervåking. Etter Finanstilsynets vurdering skyldes overtredelsene som nå er avdekket, klart klanderverdig adferd fra banken, da den manglende etterlevelsen synes å være et resultat av manglende prioritering over lengre tid.

Banken har også selv vært klar over flere av manglene i etterlevelsen som beskrevet i denne rapporten. Blant annet er dette blitt tydeliggjort over tid gjennom påpekninger i egne risikovurderinger og rapporter fra internrevisor. Til tross for dette har bankens ledelse og styre ikke påsett at det gjennomføres tilstrekkelige tiltak for å etterleve regelverket. Hovedvekten av tiltakene banken nå har iverksatt på området, ble først vedtatt av styret og ledelsen sommeren 2021. Dette på tross av at styret selv bekreftet overfor Finanstilsynet tilbake i 2019 at bankens styre og ledelse ville følge opp at arbeidet med å implementere tiltak som skal sikre bankens etterlevelse av hvitvaskingslovens bestemmelser, ble prioritert.

Vurderingsmomentene i hvitvaskingsloven § 50 er obligatoriske, men ikke uttømmende. Forvaltningsloven § 46 oppstiller en rekke momenter som kan hensyntas i saker om administrative sanksjoner. Bestemmelsens bokstav a) gjelder vurderingen av sanksjonens preventive virkning. Etter Finanstilsynets vurdering er overtredelsene av en slik art og av et slikt omfang at det taler for sanksjonering, både av allmennpreventive og individualpreventive hensyn. Overtredelsene følger av at banken ikke har avsatt riktige ressurser til oppfyllelsen av lovkravene, og at ledelsen ikke har iverksatt de nødvendige tiltak selv når den visste, eller burde ha visst, at etterlevelsen av hvitvaskingsregelverket var utilstrekkelig.

På bakgrunn av rettspraksis legger Finanstilsynet til grunn at det ved ileggelse av overtredelsesgebyr overfor foretak stilles krav om at den eller de som har opptrådt på vegne av foretaket, har utvist skyld i form av minimum alminnelig uaktsomhet. Skyldkravet kan oppfylles ved anonyme og kumulative feil. Etter Finanstilsynets vurdering skyldes uaktsomheten styrets og ledelsens manglende oppfølging av hvitvaskingslovens krav. Finanstilsynets vurdering er at dette har ledet til svikt på flere nivåer i foretaket, og at overtredelsene kunne vært unngått dersom foretaket hadde viet etterlevelsen av regelverket tilstrekkelig oppmerksomhet.

## 12. Vurdering av utmåling

Forholdene som har betydning for om overtredelsesgebyr bør ilegges, som redegjort for ovenfor, har også betydning for utmålingen av gebyret. Som omtalt over, vektlegges det at overtredelsene anses som grove og varige og at banken har opptrådt klanderverdig. Nedenfor fremheves noen ytterligere utmålingsspesifikke vurderinger.

Ved utstedelse av overtredelsesgebyr skal det etter § 50 første ledd bokstav e) vurderes hvorvidt fordeler er oppnådd gjennom overtredelsen. "Fordeler" tolkes videre enn kun at overtredelsen har gitt inntekter, og omfatter også andre fordeler, herunder besparelser. Finanstilsynet vurderer at banken har oppnådd fordeler i form av besparelser i forbindelse med den mangelfulle etterlevelsen av hvitvaskingsregelverket, og at banken på et mye tidligere tidspunkt burde ha tilført ytterligere ressurser til hvitvaskingsområdet.

Utmålingen av overtredelsesgebyret skal videre ta hensyn til overtrederens økonomiske evne, jf. § 50 bokstav c). I lovens forarbeider fremheves betydningen av lovens kriminalitetsforebyggende formål. For at sanksjoneringen skal være proporsjonal, effektiv og avskrekkende, må den utmåles slik at beløpet utgjør en følbar reaksjon som speiler overtredelsenes alvorlighet for det enkelte foretak.

Ved utstedelse og utmåling av overtredelsesgebyr skal også eventuelle tidligere overtredelser av hvitvaskingsloven eller forskrifter med hjemmel i loven hensyntas, jf. § 50 bokstav h). Finanstilsynet viser til tidligere merknader etter tilsyn i 2018, samt illeggelsen av overtredelsesgebyr i 2019, som begge ble gitt på bakgrunn av manglende etterlevelse av hvitvaskingslovens bestemmelser. Finanstilsynet konstaterer at det ikke bare foreligger gjentatte overtredelser, men at overtredelsene fremdeles er såpass omfattende og alvorlige at det må stilles spørsmål ved om nevnte kritikk og overtredelsesgebyr har vært egnet til å endre bankens adferd og etterlevelse. Tilsynet i 2018 ble gjennomført under 2009-loven, som ikke hjemlet overtredelsesgebyr. Overtredelsesgebyret ilagt i 2019 var basert på manglende transaksjonsovervåking av et stort antall transaksjoner over flere år, men var ikke basert på et bredt tilsyn av bankens etterlevelse. Sammenholdt med bankens økonomiske evne, jf. § 50 bokstav c, var gebyret på ni millioner kroner i 2019 beskjedent. Blant annet sett hen til bankens tidligere overtredelser, anses det i dette tilfellet som nødvendig å utmåle et vesentlig høyere overtredelsesgebyr enn gebyret ilagt i 2019.

Etter en vurdering av overtredelsene, i lys av bankens økonomiske evne og gjentatte overtredelser av de samme bestemmelsene i gjeldende regelverk, varslet Finanstilsynet i brev av 7. februar 2022 at overtredelsesgebyret burde fastsettes til kroner 150 000 000 (ett-hundre og femti-millioner-kroner).

## 13. Bankens tilsvaret og Finanstilsynets kommentarer til disse

I tilsvaret til varslet om overtredelsesgebyr gir styret blant annet uttrykk for at det vurderer at det ikke eksisterer et faktisk grunnlag for å anta at banken ikke har en virksomhetsinnrettet risikovurdering eller noen risikoklassifisering. Imidlertid mener styret at risikovurderingen og klassifiseringen har mangler og bør forbedres, som også er nevnt tidligere i denne rapporten. Styret er også uenig i at det foreligger overtredelse av hvitvaskingsloven § 26, ettersom Finanstilsynet ikke har identifisert noen faktiske overtredelser av denne bestemmelsen.

Styret angir videre at Finanstilsynet blant annet bør ta i betraktning de rekke målrettede endringene og forbedringene banken har foretatt de siste årene, og at det også bør tas hensyn til hvordan banken opptrådte da den fikk vite at de iverksatte tiltakene ikke hadde hatt ønsket effekt. Styret erkjenner at tiltakene ikke har vært vellykkede, men stiller spørsmål ved om manglende suksess kan anses som uaktsom opptreden. Det vises til at banken selv har identifisert manglene og kontinuerlig arbeidet med å rette disse. Styret er også uenig i at banken har tjent på å ikke bevilge tilstrekkelige ressurser for å hindre manglende etterlevelse, og viser blant annet til de økonomiske kostnadene banken både har og har hatt på området. Gitt tidligere saker, er også styrets oppfatning at det varslede overtredelsesgebyret synes høyt.

Finanstilsynet tar til etterretning at banken har iverksatt flere tiltak i forsøket på å bedre etterlevelsen på området, også i etterkant av tilsynet i 2018. Det er bankens faktiske etterlevelse av gjeldende regelverk slik det er beskrevet i denne rapporten som ligger til grunn for vurderingene i denne rapporten og vedtaket om overtredelsesgebyr. Flere av lovbruddene som er påvist, gjaldt forpliktelser i hvitvaskingsloven av 2009 samt forhold som også tidligere har blitt påpekt av Finanstilsynet. Tatt i betraktning omfanget av manglene som fortsatt avdekkes, og den betydelige tiden banken har hatt på å rette flere av de påviste manglene, er det etter Finanstilsynets vurdering klart at nevnte tiltak og bankens oppfølging av disse ikke har vært tilstrekkelig for å få banken til å etterleve gjeldende regelverk. At de foregående tiltakene ikke har gitt bedre effekt, og at ytterligere tiltak således var nødvendig å iverksette, er noe Finanstilsynet også mener burde vært identifisert og fulgt opp på et tidligere tidspunkt av bankens styre og ledelse, også sett i lys av at banken selv hevder å ha identifisert manglene som påpekes i denne rapporten.

Hva gjelder kommentarene rundt påløpte kostnader, er Finanstilsynets oppfatning, og som banken også selv skriver i tilsvaret, at disse representerer forutsigbare driftskostnader i virksomheten. En akkumulering av kostnader som har gjort seg gjeldende de senere år, som en direkte følge av historisk og betydelig manglende etterlevelse av regelverket på området, kan etter Finanstilsynets syn ikke tillegges vekt i denne utmålingen, ettersom kostnadene som nå påløper også kan anses som et resultat av tidligere besparelser, gitt omfanget av den vedvarende og historisk manglende etterlevelsen som er påvist på området.

Hva gjelder styrets anførsler om risikovurdering og risikoklassifisering, kan Finanstilsynet videre ikke se at de punktene styret oppstiller i tilsvaret, gir grunnlag for å endre Finanstilsynets vurderinger eller konklusjon, som også redegjort for tidligere i denne rapporten.

Når det gjelder spørsmålet om det kan konstateres overtredelser av hvitvaskingsloven § 26, som dermed skal inngå i et vedtak om overtredelsesgebyr, har Finanstilsynet basert på styrets tilsvaret kommet til en annen konklusjon enn i foreløpig rapport. Finanstilsynets vurdering er at det formodentlig er mistenkelige forhold som ikke er rapportert til Økokrim med grunnlag i at mange alarmer ennå ikke er ferdig undersøkt, fordi en betydelig andel er lagt i "dvale". Det er likevel slik at Finanstilsynet for å ilegge overtredelsesgebyr må dokumentere klar sannsynlighetsovervekt for at det foreligger overtredelse av loven. Ettersom foreløpig rapport ikke individualiserer enkeltforhold som utgjør overtredelse av rapporteringsplikten, jf. § 26, frafaller Finanstilsynet overtredelse av denne bestemmelsen i vedtaket om overtredelsesgebyr.

Finanstilsynet kan ikke se at det oppstilles andre forhold i tilsvaret som har betydning for de øvrige vurderingene eller for gebyrets størrelse. Som nevnt skal beløpet utgjøre en følbar reaksjon som

gjenspeiler overtredelsenes alvorlighet for det enkelte foretak, og Finanstilsynet anser at det i dette tilfellet er nødvendig å utmåle et vesentlig høyere overtredelsesgebyr enn gebyret banken ble ilagt i 2019, også sett hen til at gebyret i 2019 var beskjedent sammenholdt med bankens økonomiske evne. Finanstilsynet påpeker også at vilkåret etter § 50 første ledd bokstav h) heller ikke har vært til stede i tidligere sammenlignbare saker hvor Finanstilsynet har ilagt overtredelsesgebyr.

#### **14. Finanstilsynets vurdering på bakgrunn av bankens anførsler**

Finanstilsynet har på bakgrunn av bankens anførsler funnet at det ikke er klar sannsynlighetsovervekt for at banken har overtrådt hvitvaskingslovens § 26. Likevel finner Finanstilsynet grunn til å tillegge dette liten vekt, også i gebyrets utmåling, da banken over tid og for et betydelig volum transaksjoner ikke har behandlet alarmer fra overvåkingssystemet og dermed satt seg selv ute av stand til å avdekke og rapportere mistenkelige forhold rettidig. Det vises også til forarbeidenes understrekning av det straffverdige ved at en rapporteringspliktig stiller seg sårbar for hvitvasking og terrorfinansiering, også der sårbarhetene rent faktisk ikke utnyttes av kriminelle. Finanstilsynet mener at dette punktet derfor ikke har påvirkning på det varslede gebyrets størrelse.

For øvrig har Finanstilsynet ikke funnet grunn til å endre vurderingene som ble kommunisert i forhåndsvarselet, da det etter Finanstilsynets vurdering ikke oppstilles forhold i tilsvaret som gir grunnlag for dette. Det vises også til Finanstilsynets kommentarer til bankens tilsvare, som redegjort for i øvrige deler av denne tilsynsrapporten.

Finanstilsynet viser videre til alvorligheten av at alarmer ikke behandles rettidig, at enkelte legges i "dvale" og ikke undersøkes i det hele tatt, samt til ytterligere rapportert hendelse på hvitvaskingsområdet i etterkant av tilsynet (mars 2022). Forholdene som ligger til grunn for hendelsesrapporten strekker seg også flere år bakover i tid og underbygger etter Finanstilsynets vurdering det historiske fraværet av styring og kontroll med risikoen på hvitvaskingsområdet.

Basert på forholdene som oppstilles i denne rapporten, er Finanstilsynets konklusjon at banken har overtrådt bestemmelsene i lovens §§ 7, 8, 9, 12, 13, 17, 18, 24 og 25. Med hjemmel i hvitvaskingsloven § 49, kan overtredelse av disse bestemmelsene medføre overtredelsesgebyr. Finanstilsynets samlede vurdering er at de avdekkede overtredelsene ved tilsynet er av en slik art og omfang at overtredelsesgebyr skal ilegges.

Finanstilsynet finner derfor å underrette Santander Consumer Bank AS om følgende:

#### **Vedtak om overtredelsesgebyr**

Santander Consumer Bank AS ilegges et overtredelsesgebyr på kroner 150 000 000 (ett-hundre-og femti-millioner-kroner) for overtredelse av §§ 7, 8, 9, 12, 13, 17, 18, 24 og 25 i lov om tiltak mot hvitvasking og terrorfinansiering, jf. lovens § 49, jf. § 50.

Dette vedtaket kan påklages innen tre uker etter at vedtaket er mottatt. Klage sendes Finanstilsynet. Klageinstans er Finansdepartementet. Forvaltningsloven §§ 18 og 19, om partenes adgang til å gjøre seg kjent med sakens dokumenter, gjelder.

Overtredelsesgebyret innkreves av Statens innkrevingsentral. I tilfeller der vedtaket ikke påklages, vil Statens innkrevingsentral sende krav om betaling umiddelbart etter klagefristens utløp. I

tilfeller der vedtaket påklages, sendes kravet etter at klagen er avgjort av Finansdepartementet. Statens innkrevingssentrals frist for betaling er tre uker etter faktura er sendt.

## 15. Pålegg om retting

### Rettslig grunnlag

Hvitvaskingsloven § 47 gir Finanstilsynet hjemmel til å vedta pålegg om at forhold i strid med loven eller forskrift gitt i medhold av loven skal opphøre. Finanstilsynet kan sette en frist for å etterkomme pålegget. Dersom pålegget ikke etterkommes innen den fastsatte fristen, kan Finanstilsynet ilegge tvangsmulkt til det ulovlige forholdet opphører, jf. hvitvaskingsloven § 47 annet ledd.

### Finanstilsynets vurdering

Finanstilsynet fant i foreløpig rapport grunn til å varsle banken om pålegg om retting, jf. hvitvaskingsloven § 47. På bakgrunn av manglene som er avdekket, og beskrevet i denne rapporten, er Finanstilsynets endelige vurdering at pålegg skal ilegges.

Finanstilsynet finner derfor å underrette Santander Consumer Bank AS om følgende:

### Vedtak om pålegg om retting

På bakgrunn av den manglende etterlevelsen som er beskrevet i tilsynsrapporten, finner Finanstilsynet grunn til å vedta pålegg om retting, jf. hvitvaskingsloven § 47. Pålegget omfatter følgende forhold:

1. Banken må utarbeide en risikovurdering som på en fullstendig måte identifiserer og vurderer risikoen for hvitvasking og terrorfinansiering tilknyttet egen virksomhet, produkter, kundeforhold, type kunder, kundegrupper og geografiske forhold, jf. hvitvaskingsloven § 7.
2. Banken må endre risikoklassifiseringsmetodikken slik at den baseres på bankens risikovurdering, jf. lovens § 7, og minimum omfatter kriterier tilknyttet kundeforholdets formål, mengden kundemidler som skal inngå i kundeforholdet, transaksjoners størrelse og regelmessigheten og varigheten på kundeforholdet, jf. lovens § 9. Dersom nevnte endringer ikke lar seg gjennomføre i det elektroniske systemet innen fristen, må det sikres gjennom manuelle tiltak.
3. Banken må gjennomføre og dokumentere tilstrekkelige kundetiltak på samtlige av bankens kunder som har mangler i kundetiltakene, i henhold til hvitvaskingsloven kapittel 4, herunder §§ 12, 13, 17, 18 og 24.
4. Banken må forbedre løpende oppfølging av kundeforholdene ved å vurdere adferden i lys av innhentede kundeopplysninger, samt ved å utvide regelsettingen i transaksjonsovervåkingen, jf. hvitvaskingsforskriften § 7-3 andre ledd. Banken må også påse at det etableres rutiner for jevnlig evaluering av reglene i systemet, deres funksjonalitet og treffsikkerhet, for å avdekke eventuelle svakheter og behov for supplerende tiltak.

Frist for oppfyllelse av pålegget er 1. februar 2023. Banken må innen samme dato legge frem for Finanstilsynet en bekreftelse fra bankens styre på at påleggene er oppfylt samt dokumentasjon på dette.



Manglende oppfyllelse av pålegg om retting kan være grunnlag for vedtak om tvangsmulkt, jf. hvitvaskingsloven § 47 andre ledd.

Vedtaket om pålegg kan påklages innen tre uker etter at vedtaket er mottatt. Klage sendes Finanstilsynet. Klageinstans er Finansdepartementet. Forvaltningslovens §§ 18 og 19 om partenes adgang til å gjøre seg kjent med sakens dokumenter, gjelder.

Til samme frist som pålegget bes banken også om å redegjøre for følgende forhold:

- Endringer i rutineene på bakgrunn av den fornyede risikovurderingen og kommentarene i rapportens kapittel 3.

For Finanstilsynet

Ann Viljugrein  
direktør for bank- og forsikringstilsyn

Anne-Marte Hee Teigmo  
seniorrådgiver

*Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.*