

BDO I SVERIGE

Penningtvättstillsyn i förändring

En analys av Finansinspektionens sanktionspraxis
och tillsynsrapporter 2015 - 2024

Martin Tidesten, Head of Risk Advisory Services

INNEHÅLL

1. INLEDNING	3
2. SANKTIONSBeslut ÖVER TID: OMFATTNING OCH UTVECKLING	4
3. ÅTERKOMMANDE BRISTER I ARBETET MOT PENNINGTVÄTT	5
3.1 RISKANALYS OCH RISKKLASSIFICERING	5
3.2 KUNDKÄNNEDOM (KYC)	6
3.3 TRANSAKTIONSÖVERVAKNING OCH RAPPORTERING	7
3.3.1 Modellkalibrering, datagrund och validering - bortglömda komponenter	7
3.3.2 Organisatoriska brister och centraliserade strukturer	7
3.4 STYRNING OCH INTERN KONTROLL	8
4. FI:S TILLSYNSRAPPORTER: SEKTORSVISA OBSERVATIONER	10
5. SANKTIONSAVGIFTER FÖRDELADE PER SEKTOR	11
6. SLUTSATSER	12
7. FRAMTIDENS AML-TILLSYN: AMLA OCH DEN NYA EUROPEISKA STRUKTUREN	13

1. Inledning

Finansinspektionen (FI) har under det senaste decenniet intensifierat sin tillsyn av finansiella företags arbete mot penningtvätt och finansiering av terrorism.

Flera uppmärksammade sanktionsbeslut har fattats mot banker och andra aktörer som brustit i att följa penningtvättsregelverket. Parallellt har FI publicerat tillsynsrapporter som belyser vanliga brister och förväntningar på finanssektorns arbete mot penningtvätt.

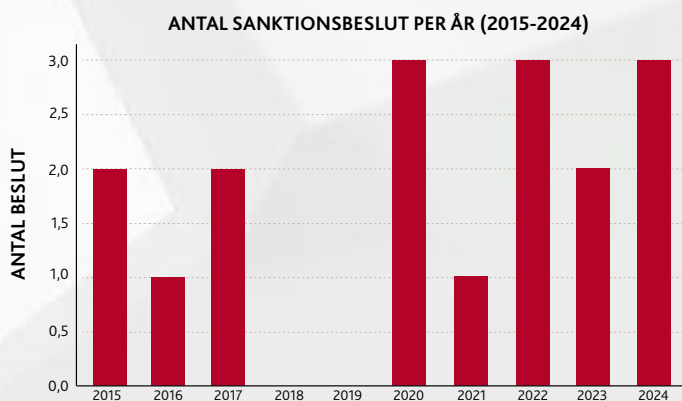
Denna rapport granskar FI:s sanktionsbeslut inom penningtvättsområdet och sammanfattar slutsatser från centrala tillsynsrapporter.



2. Sanktionsbeslut över tid: omfattning och utveckling

FI har möjlighet att ingripa mot företag som inte lever upp till kraven i penningtvättslagstiftningen, genom bland annat anmärkningar, varningar, sanktionsavgifter och i allvarliga fall återkallelse av tillstånd. Under perioden 2015 - 2024 har FI meddelat ett flertal sanktionsbeslut kopplade till penningtvättsregelverket, med en markant ökning i både antal och belopp från 2020 och framåt.

(utan avgift) i sin svenska verksamhet, 2022 meddelades varningar eller anmärkningar till bl.a. Trustly (130 Mkr) och ClearOn (14 Mkr) samt Länsförsäkringar Bank (90 Mkr) för olika brister. Under 2023 fortsatte tillsynen med t.ex. Aros Kapital (varning och 45 Mkr) och kryptoföretaget Goobit (anmärkning och 2 Mkr). I slutet av 2024 tilldelades även fintech-banken Klarna en anmärkning med 500 Mkr i sanktionsavgift för överträdelser av penningtvättsreglerna.



Figur 1: Antal sanktionsbeslut per år inom penningtvättsområdet 2015 - 2024. En anmärkning eller varning med sanktionsavgift räknas här som ett sanktionsbeslut. Trenden visar toppar 2015, 2017, 2020, 2022 - 2023 och en tydlig intensifiering efter 2020.

Som Figur 1 illustrerar var FI:s aktivitet relativt begränsad före 2020, med enstaka ingripanden vissa år. År 2015 utfärdade FI två sanktionsbeslut (mot Nordea och Handelsbanken), 2016 endast ett (Resurs Bank) och 2017 två beslut (bl.a. Sörmlands Sparbank). Under 2018 - 2019 tillkom inga nya sanktionsavgifter inom penningtvättsområdet.

Däremot förändrades situationen år 2020 i spåren av de stora penningtvättsskandalerna i Baltikum, då FI fattade tre tunga sanktionsbeslut: Swedbank fick en varning och historiskt hög sanktionsavgift på 4 miljarder kronor, SEB ålades en anmärkning med 1 miljard i avgift, och den mindre JAK Medlemsbank fick en anmärkning och 1,6 miljoner i avgift. Efter 2020 har FI årligen ingripit mot överträdelser: 2021 beslutade FI att förelägga Danske Bank att åtgärda brister

Den markanta ökningen av sanktionsbeloppen efter 2019 hänger ihop med skärpt lagstiftning och högre tillåtna maxbelopp. Enligt 2017 års penningtvättslag och EU-direktiv kan FI nu sätta sanktionsavgifter i nivå med en andel av företagets omsättning, vilket möjliggjort miljardbeloppen mot storbankerna. Som jämförelse var det högsta möjliga bötesbeloppet före lagändringarna 50 miljoner kronor, ett tak som nåddes i flera tidiga fall (t.ex. Forex Bank 2008 och 2013 samt Nordea 2015). Även små institut kan dock drabbas av kännbara sanktioner. FI har vid upprepade tillfällen varnat Forex Bank för allvarliga brister (2008 och 2013, båda gångerna 50 Mkr), och senare ingripit mot mindre aktörer som betalningsinstitut och växlingskontor (t.ex. förelägganden mot Safello och Goobit 2015 respektive 2023).

Under perioden 2015 - 2024 har FI meddelat ett flertal sanktionsbeslut kopplade till penningtvättsregelverket, med en markant ökning i både antal och belopp från 2020 och framåt.

3. Återkommande brister i arbetet mot penningtvätt

En genomgång av FI:s sanktionsbeslut och tillsynsundersökningar visar att vissa typer oförätter återkommer hos många företag. Dessa bristområden kan betraktas som de vanligaste orsakerna till att ett institut får en anmärkning eller varning kopplad till penningtvättslagen:

3.1 RISKANALYS OCH RISKKLASSIFICERING

Finansinspektionens beslut visar tydligt att många verksamhetsutövare har genomgripande brister i den allmänna riskbedömningen, ett dokument som enligt lag ska utgöra grunden för företagets arbete mot penningtvätt. Bedömningen ska identifiera och väga risker kopplade till produkter, tjänster, kunder, geografiska områden och distributionsätt. Trots detta framgår det i flera beslut att riskanalysen ofta är alltför generell, bristfälligt dokumenterad eller inte anpassad till den faktiska verksamheten. I vissa fall saknas nyckelfaktorer helt, och i andra har riskbedömningen inte uppdaterats i takt med att affärsmodellen förändrats.

Ett exempel är Goobit, där FI noterade att den allmänna riskbedömningen inte tog hänsyn till geografiska riskfaktorer trots att bolaget tillhandahåller tjänster globalt. Dessutom saknades analys av flera högriskkategorier, som visserligen beaktades i transaktionsövervakningen men inte i grundanalysen. FI konstaterade att Goobits riskbedömning därmed inte kunde ligga till grund för utformning av effektiva rutiner och åtgärder. Även ClearOn hade en otillräcklig riskbedömning, bolaget hade inte uppmärksammat omfattningen av sin kundbas, vilket ledde till att många kundrelationer helt föll utanför analysen. Swedbank, å sin sida, kritiserades för att den svenska verksamheten använde en riskklassificeringsmodell som inte var baserad på den gällande allmänna riskbedömningen. Detta innebar att kunder inte riskklassificerades i enlighet med identifierade produkt- och kundrisker, vilket stred mot grundkravet att klassificeringen ska ta sin utgångspunkt i den allmänna riskbilden och företagets kännedom om kunden.

En särskilt återkommande svaghet är just att kundriskklassificeringen inte är kopplad till den allmänna riskbedömningen, vilket strider mot penningtvättslagstiftningen. Kundklassificeringen är ett centralt verktyg i det riskbaserade angreppssättet, den avgör vilken nivå av kundkännedom som ska tillämpas, hur transaktioner ska övervakas och hur resurser ska prioriteras. I flera fall har FI funnit att företag inte klassificerat alla kunder, använt schablonartade mallar eller helt saknat modell för detta. ClearOn klassificerade exempelvis inte sina privatkunder alls, och andra företag, såsom Aros Kapital och Trustly, har haft för få risknivåer eller saknat koppling mellan klassificeringen och faktiska riskfaktorer. Goobit uppgav själva att deras kundklassificering inte utgick från bolagets riskbedömning, ett tydligt brott mot lagens krav.

I flera fall har FI funnit att företag inte klassificerat alla kunder, använt schablonartade mallar eller helt saknat modell för detta.

Ytterligare en aspekt som blivit allt mer framträdande i FI:s tillsyn är otillräcklig förståelse för hur distributionsmodellen påverkar penningtvättrisen. I beslutet mot Klarna framhöll FI att bankens modell med så kallade mor-handlare och underhandlare ökade risken för att produkterna skulle utnyttjas för penningtvätt. Trots att Klarna internt bedömt detta som en förhöjd risk, saknades en tillräcklig analys i den allmänna riskbedömningen, och det var oklart hur kontrollåtgärder anpassats till strukturen. Även i fallet med Trustly framkom liknande brister. Bolaget betraktade inte slutanvändarna av deras betaltjänst som sina egna kunder och hade därför inte tillämpat kundkännedom eller riskbedömning på dessa individer. FI bedömde att det förelåg en affärsförbindelse i lagens mening, vilket innebar att Trustly borde ha vidtagit samtliga AML-åtgärder för denna kategori.

Sammanfattningsvis visar FI:s beslut att många aktörer, oavsett storlek och verksamhetsinriktning, tenderar att behandla riskanalysen och kundklassificeringen som fristående formkrav snarare än som operativa kärnkomponenter i sin styrning. I praktiken fungerar dessa dokument ofta som pappersprodukter upprättade för att uppfylla regelverkets formella krav, men utan konkret genomslag i affärsbeslut, kontrollsystem eller resursfördelning. Den allmänna riskbedömningen är sällan integrerad i den löpande riskhanteringen och återfinns inte i företagets beslutsvägar, kontrollstrategier eller rapporteringslinjer. När detta sker urholkas syftet med ett riskbaserat angreppssätt. Kundklassificeringen blir ett frikopplat verktyg, övervakningen tappar träffsäkerhet och möjligheten att upptäcka eller förebygga penningtvätt försvagas.

FI:s tillsyn tyder också på att dessa brister inte enbart är operativa eller tekniska, utan i grunden handlar om styrning, förståelse och prioritering. När ledningen inte använder riskanalysen som beslutsunderlag, och kontrollfunktionerna inte förankras i verklig riskinsikt, blir AML-arbetet reaktivt snarare än strategiskt. Det är just denna avsaknad av intern förankring som återkommer i besluten oavsett om det gäller traditionella banker, betalningsinstitut eller kryptoplattformar. Därför handlar de återkommande bristerna inte om tillfälliga missar, utan om ett djupare strukturellt problem, att penningtvättrisker fortfarande hanteras parallellt med snarare än inom företagets styrning och kontroll.

3.2 KUNDKÄNNEDOM (KYC)

Finansinspektionen har i ett flertal beslut konstaterat omfattande brister i företags arbete med kundkännedom (KYC). Dessa brister sträcker sig från grundläggande identitetsverifiering till otillräcklig inhämtning av uppgifter om kundens verksamhet, syftet med affärsförbindelsen och den förväntade transaktionsprofilen. Sammantaget pekar besluten på att många aktörer inte har integrerat KYC som en kärnprocess i sin affärsmodell vilket lett till strukturella brister i regelföljningen.

1. Avsaknad eller otillräcklighet i dokumenterade rutiner

Flera företag har helt eller delvis saknat skriftliga instruktioner för hur kundkännedom ska tillämpas. FI har exempelvis konstaterat att ClearOn inte hade interna KYC-rutiner anpassade till sin riskprofil och verksamhetsvolym. I vissa fall hävdade företagen att externa manualer, IT-stöd eller ombudsinstruktioner kunde ersätta interna riktlinjer, något FI avfärdade med hänvisning till penningtvättslagstiftningens krav på dokumenterade, riskanpassade interna rutiner.

Liknande brister har även noterats hos Goobit och Safello, särskilt i verksamhetens uppstartsskede, då FI valde att förelägga förbättringsåtgärder istället för omedelbara sanktioner.

2. Ofullständig informationsinhämtning

En genomgående brist är att företag inte inhämtat tillräcklig information om sina kunder. Det gäller särskilt uppgifter om verklig huvudman, medborgarskap, syfte med affärsförbindelsen och förväntade transaktioner. FI konstaterade att Goobit inte frågat om förväntade volymer eller användning, vilket försvårade bedömningen av kundens riskprofil. Länsförsäkringar Bank och Swedbank har båda fått kritik för att dokumentationen av syfte och användning varit otillräcklig, trots att det utgör ett lagkrav vid kundkännedom. I flera fall har företag brutit i kontrollen av om kunder eller huvudmän varit bosatta i högriskländer, bland annat på grund av att uppgifter om medborgarskap saknats.

3. Brister i fördjupad kundkännedom och uppföljning

Flera beslut visar att företag saknar processer för att tillämpa fördjupad kundkännedom vid förhöjd risk. FI har i flera ärenden pekat på att bolag inte har rutiner för att vägra affärer eller avsluta affärsförbindelser vid otillräcklig information. I ett fall konstaterades att det saknades trösklar eller beslutspunkter för när transaktioner skulle blockeras eller granskas manuellt. SEB och Swedbank har båda fått anmärkningar kopplat till fördröjda eller otillräckliga åtgärder vid kända risker i utlandsverksamheter.

4. Överlåtelse av ansvar till ombud eller externa led

Ett återkommande tema, särskilt hos fintechbolag och betalningsinstitut, är att företaget förlitat sig på att andra aktörer t.ex. återförsäljare, plattformar eller ombud sköter delar av KYC-processen. FI har underkänt denna modell om det inte finns ett system för att kontrollera kvaliteten och säkerställa att kraven faktiskt uppfylls. I Klarnas och Trustlys fall har detta varit särskilt relevant i samband med analys av distributionsrisk, där avståndet till slutanvändaren medfört att kunden ibland inte identifierats eller kontrollerats tillräckligt noggrant.

Samtaget framgår att bristerna i kundkännedom inte enbart beror på enskilda tekniska fel eller bristfälliga IT-system. De speglar ofta en djupare organisatorisk svaghet där kundkännedom inte prioriterats som en kärnkomponent i affärsmodellen. I vissa fall tycks företag ha valt att minimera friktionen i onboarding-processer, till exempel genom att avstå från att ställa känsliga frågor om syfte eller transaktionsvolym, i hopp om att behålla kunder. I andra fall handlar det om resursbrist eller bristande kompetens kring hur KYC-kraven ska omsättas i praktiken. FI:s tillsyn visar dock tydligt att dessa luckor i kundkännedom lämnar företagen sårbara, både för penningtvättrisker och för regulatoriska ingripanden.

3.3 TRANSAKTIONSÖVERVAKNING OCH RAPPORTERING

Ett återkommande problemområde i FI:s tillsyn är svagheter i institutens förmåga att identifiera och rapportera misstänkta transaktioner. Bristerna gäller inte enbart frånvaro av övervakning, utan snarare hur ineffektivt eller felkalibrerat övervakningssystemet är utformat. FI har konstaterat att många företag använder standardssystem eller scenarioverktyg som inte är anpassade efter den egna verksamhetens riskprofil, vilket undergräver träffsäkerheten och försvårar prioritering av uppföljning.

I FI:s kartläggning av livförsäkringsföretag visade det sig att även när automatiserade övervakningssystem används, är scenariomodellerna ofta få till antalet, grovt formulerade eller inte relevanta för just försäkringsverksamhet. I vissa bolag fanns så få som 3 övervakningsscenarier, i andra upp till 48, men antalet genererade larm var antingen förvånansvärt lågt eller oöverblickbart stort. I nästan hälften av de granskade bolagen hade ingen misstänkt transaktion alls rapporterats till Finanspolisen under ett helt år, vilket FI tolkade som ett tecken på otillräcklig systemeffektivitet eller bristande uppföljning snarare än frånvaro av risk.

Liknande brister har framkommit i beslut mot flera banker. I fallet Länsförsäkringar Bank konstaterade FI att banken inte haft tillräckliga åtgärder för att övervaka "hög-hastighets-transaktioner" eller riskabla utlandsbetalningar i pågående kundrelationer. Swedbank fick särskilt allvarlig kritik för att transaktionsövervakningen i den svenska verksamheten var otillräcklig i förhållande till risknivå och verksamhetsomfattning, en bidragande orsak till den rekordstora sanktionsavgiften 2020.

3.3.1 Modellkalibrering, datagrund och validering - bortglömda komponenter

FI:s tillsyn visar att många företag misslyckas med att validera sina transaktionsövervakningsmodeller. Antingen saknas intern funktion för kvantitativ modellutvärdering, eller så valideras inte tröskelvärden och scenariologik systematiskt mot faktisk riskdata. I vissa fall har företag fortsatt använda scenarier som genererar antingen stora mängder falsklarm eller så få träffar att potentiell penningtvätt aldrig

identifieras. I båda fallen förlorar modellen sitt analytiska värde, vilket undergräver hela syftet med riskbaserad övervakning.

FI har också noterat att det i många fall saknas dynamisk koppling mellan övervakningen och annan riskinformation. Effektiv transaktionsövervakning ska inte vara ett fristående system, utan förses med input från kundriskklassificering, allmän riskbedömning och KYC-data. I flera fall saknas sådan integration helt. Ett företag kan därmed ha klassificerat en kund som högrisk, men transaktionerna från samma kund hanteras ändå enligt standardiserade övervakningsparametrar, vilket skapar ett glapp i riskstyrningen.

3.3.2 Organisatoriska brister och centraliserade strukturer

Ytterligare en orsak till bristerna är organisatorisk. FI har pekat på att vissa koncerner centraliserat AML-övervakningen till gruppnivå, medan dotterbolagen saknat tillräcklig insyn i vad som rapporteras. Det har lett till att lokala enheter inte själva gjort bedömningar eller rapporterat misstänkta transaktioner, vilket riskerar att information faller mellan stolarna. Om ett gruppövergripande system saknar realtids-feedback eller lokalt ansvar kan det dessutom dröja innan riskindikationer fångas upp eller förbli obeaktade helt.

Det finns också exempel där transaktionsövervakningen varit tekniskt implementerad men inte organisatoriskt prioriterad. FI har i flera fall sett att det saknas resurser, systemstöd eller kompetens för att analysera larm. Det leder till att larm ligger obehandlade, eller att analytiker fokuserar på irrelevanta signaler medan verkliga risker passerar obemärkta.

FI har också noterat att det i många fall saknas dynamisk koppling mellan övervakningen och annan riskinformation. Effektiv transaktionsövervakning ska inte vara ett fristående system, utan förses med input från kundriskklassificering, allmän riskbedömning och KYC-data. I flera fall saknas sådan integration helt. Ett företag kan därmed ha klassificerat en kund som högrisk, men transaktionerna från samma kund hanteras ändå enligt standardiserade övervakningsparametrar, vilket skapar ett glapp i riskstyrningen.

SAMMANFATTNING

Transaktionsövervakning är i dag en tekniskt och analytiskt krävande funktion. Den måste kalibreras med hjälp av faktisk riskexponering, kontinuerligt testas, valideras och anpassas till förändringar i verksamheten. Den måste också vara informationsmässigt integrerad med input från kundkännedom, riskklassificering och produktlogik samt organisatoriskt förankrad, med tydliga ansvarsförhållanden och kapacitet att agera. FI:s tillsyn visar att många institut ännu inte uppfyller dessa förutsättningar. Resultatet är övervakning som i praktiken är blind, antingen för att systemet inte larmar, eller för att larmen inte leder till åtgärd. I båda fallen uppstår allvarliga brister i skyddet mot penningtvätt.

3.4 STYRNING OCH INTERN KONTROLL

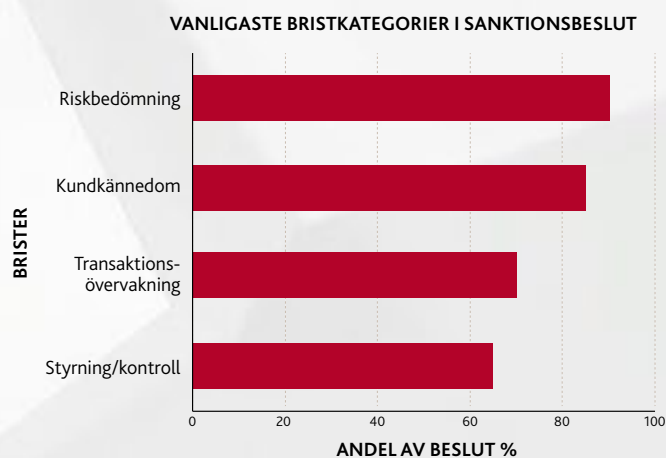
Den kanske mest genomgripande bristen som även förklarar varför ovanstående problem tillåts fortgå är svagheter i styrning och intern kontroll kring AML-arbetet. FI:s beslut lyfter ofta fram att företagsledning och styrelser inte tillräckligt styrt och kontrollerat arbetet mot penningtvätt. I flera fall har FI använt ord som "strukturella och återkommande brister på alla centrala områden", vilket understryker att problemen inte är isolerade utan tecken på systematiskt svag governance. Swedbank-fallet är belysande, den svenska utredningen slog fast att Swedbank haft stora brister i styrningen och kontrollen av AML-arbetet i de baltiska dotterbankerna. Banken uppvisade otillräcklig riskmedvetenhet i högsta ledningen och hade varken adekvata processer, rutiner eller kontrollsystem för att hantera penningtvätt-risken. Dessutom saknades det tillräckliga resurser i den baltiska verksamheten för att motverka penningtvätt, vilket pekar på att koncernledningen inte hade prioriterat området bemanningsmässigt. Även mindre banker har drabbats av liknande kritik: i tillsynen av JAK Medlemsbank (2020) och Länsförsäkringar Bank (2022) framkom att interna riktlinjer och kontroller kring riskanalys, modellvalidering och transaktionsövervakning varit bristfälliga eller obefintliga. FI noterade exempelvis att Länsförsäkringar saknade tillräckliga rutiner för validering och uppföljning av sitt övervakningssystem, en kontrollmekanism som borde ha fångat upp systemets brister. Vidare förekommer bristande utbildning och kompetens som en röd tråd. Redan 2008 konstaterade FI att Forex Bank inte hade tillräcklig utbildning av persona-

len om penningtvätsreglerna, och liknande indirekta tecken syns i senare ärenden där personal missat tydliga varningssignaler. Slutligen har vissa institut uppvisat en bristande transparens och regelefterlevnadskultur: FI:s utredning av Swedbank visade att banken känt till omfattande misstänkt penningtvätt i Baltikum men underlåtit att agera och till och med undanhållit information för FI under granskningens gång. Sådana exempel tyder på allvarliga kulturproblem och sänder en signal till hela branschen om vikten av ton från toppen.

Swedbank visade att banken känt till omfattande misstänkt penningtvätt i Baltikum men underlåtit att agera och till och med undanhållit information för FI under granskningens gång.

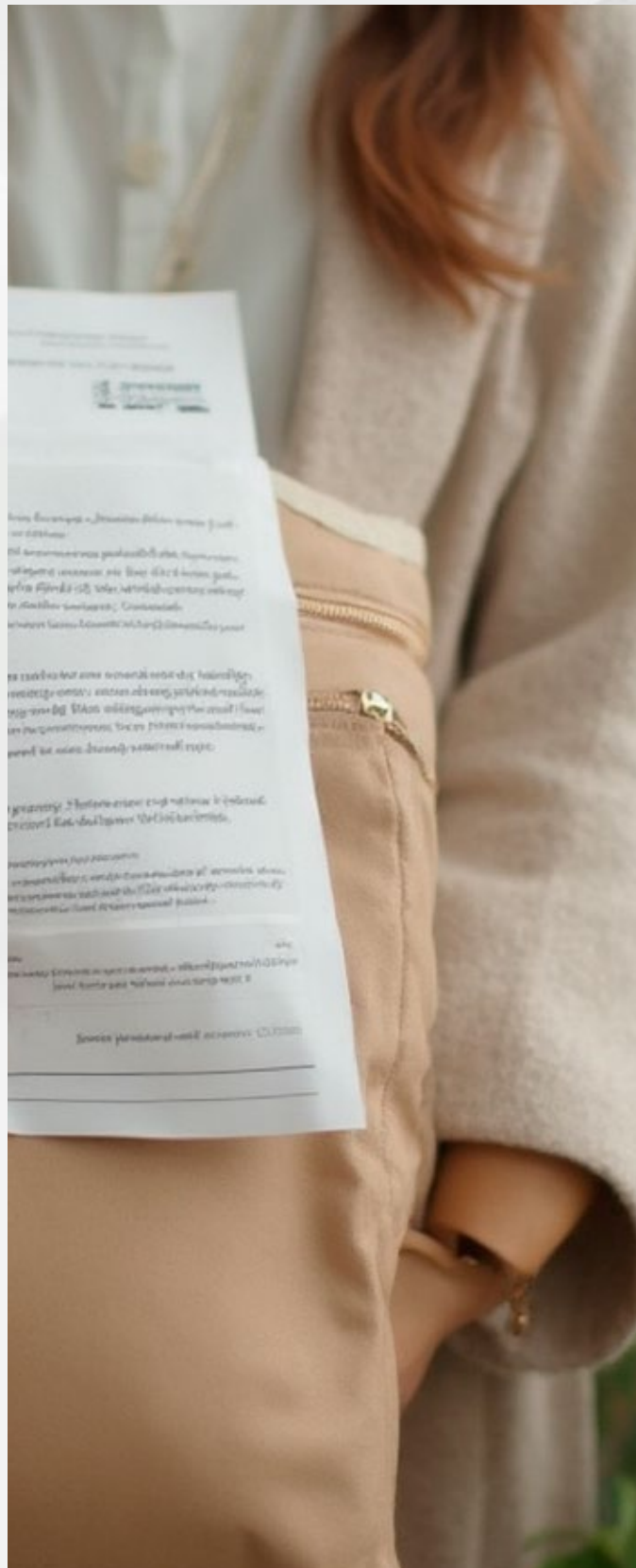
Återkommande brister inom styrning och intern kontroll antyder att penningtvätsfrågorna länge haft låg prioritet på ledningsnivå i delar av finanssektorn. Orsakerna varierar: I vissa fall har snabb affärstillväxt eller omstrukturering gjort att regelverkshanteringen hamnat på efterkälken. Forex Bank medgav exempelvis att när de gick från växlingskontor till bank 2003 hann inte interna rutiner och kunskapsöverföring med i samma takt. I större banker kan komplexa koncernstrukturer leda till otydligt ansvar, Swedbanks Baltikum-fadäs illustrerar hur lokala dotterbolag kunde bedriva högriskverksamhet utan att moderbankens kontrollmekanismer stoppade det. Det förefaller också finnas ett historiskt arv där många banker litade på sitt goda renommé och trodde sig ha "det händer inte oss"-immunitet, vilket gjorde att styrelser inte efterfrågade tillräcklig intern rapportering om penningtvättrisker. Först efter uppmärksammade skandaler (t.ex. internationella avslöjanden) kom dessa frågor högt på agendan. FI:s sanktionsärenden tyder på att flera ledningsgrupper reagerat reaktivt snarare än proaktivt, man åtgärdar brister först efter att FI ingripit, istället för att ha interna kontrollfunktioner som upptäcker och driver förbättring kontinuerligt.

Sammanfattningsvis är det tydligt att utan stark styrning, rätt resurser och en genuin regelefterlevnadskultur från toppen och ner riskerar samma typer av penningtvättsbrister att uppstå om och om igen hos olika aktörer. FI:s upprepade påpekanden och rekordhöga sanktionsavgifter de senaste åren signalerar just detta: att grundproblemen är av systemkaraktär och kräver att ledningen tar ett helhetsgrepp om AML-arbetet för att bryta mönstret av återkommande brister.



Figur 2: Vanligaste bristkategorierna i FI:s sanktionsärenden. Staplarnas längd indikerar andelen av besluten där respektive typ av brist har konstaterats (baserat på FI:s motiveringar i besluten). Riskbedömning och kundkännedom är de mest frekvent förekommande bristerna.

Figur 2 ovan sammanfattar de dominerande bristkategorier. Notera att bristerna ofta hänger samman t.ex. går en svag riskbedömning hand i hand med otillräcklig anpassning av såväl kundkännedomsåtgärder som transaktionsövervakning. FI påpekade 2018 att även om företag generellt blivit mer medvetna om penningtvättsregelverket och satsat mer resurser på området, behövdes fortsatta förbättringar på alla dessa centrala punkter. De återkommande tillsynsprojekten (se nästa avsnitt) bekräftar att dessa utmaningar kvarstod under den följande femårsperioden, om än med viss gradvis förbättring hos många aktörer.



4. FI:s tillsynsrapporter: sektorsvisa observationer

För att höja standarden i hela branschen har Finansinspektionen utöver individbaserade sanktioner också bedrivit kommunikativ tillsyn i form av tematiska kartläggningar. FI publicerar återkommande rapporter som sammanfattar iakttagelser och ger vägledning till marknaden. Två färskaste exempel är de tillsynsrapporter som kom i januari 2025 om livförsäkringsbolag respektive värdepappersbolag, där FI utvärderat hur dessa sektorer hanterar penningtvättsrisker.

Livförsäkringsföretag (FI Tillsyn Rapport 32, 2025): FI granskade 13 livförsäkringsbolags arbete mot penningtvätt under 2022. Rapporten fann att bolagen generellt behöver vidta ytterligare åtgärder för att minska risken att utnyttjas. Framför allt pekade FI på brister i riskbedömningen av produkter och tjänster, många livbolag hade inte fullt ut analyserat vilka av deras försäkringsprodukter som kan missbrukas för penningtvätt. Vidare varierade kvaliteten på kundkännedomsprocesserna; vissa bolag behövde skärpa kontrollen vid försäkringstagare med högre risk (t.ex. utländska kunder eller politiskt exponerade personer). Rapporten tog även upp utmaningar med distribution via förmedlare och tredje parter, där bolagen måste säkerställa att penningtvättskravet efterlevs i hela kedjan. FI noterade dessutom behov av stärkt intern kontroll och mer resurser hos vissa bolag för AML-arbetet. Positivt var att inga allvarliga överträdelse framkom som ledde till sanktion i detta segment, FI:s fokus låg på att förebygga risker genom dialog och vägledning.

Värdepappersbolag och banker med värdepappersrörelse (FI Tillsyn Rapport 31, 2025): En liknande kartläggning gjordes hos 15 aktörer inom värdepappersmarknaden. FI konstaterade att även dessa företag kan förbättra sina riskbedömningar, ofta var de alltför generella och inte anpassade till de specifika risker som värdepappersaffären medför. Det förelåg ingen samsyn i branschen; olika företag gjorde helt olika bedömningar av risknivåer för likartade kunder och

produkter. FI betonade att värdepappersmarknaden, med stora transaktionsvolymerna och internationell handel, kan utnyttjas i komplexa penningtvättsupplägg. Exempelvis kan kriminella köpa värdepapper med brottvinster för att "tvätta" pengarna. Därför förväntas företagen ha effekti-

Företagen har fått individuell feedback och i vissa fall förelägganden att åtgärda brister.

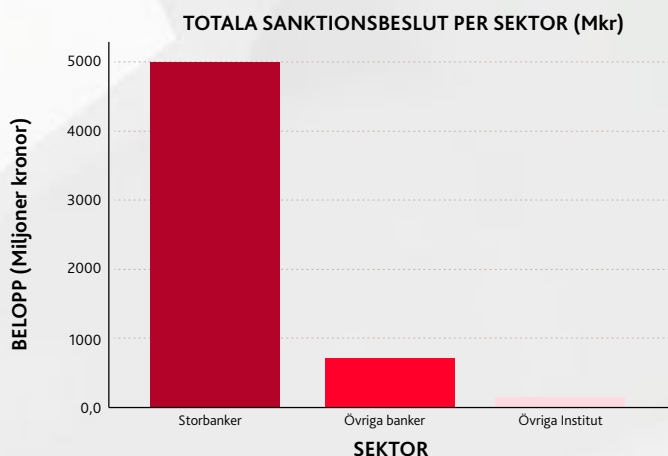
va system för att övervaka ovanliga handelsmönster och rapportera misstänkta affärer. FI:s rapport påminde om att flera värdepappersbolag behöver utveckla sina rutiner för löpande övervakning och se till att internrevision och regelverkslevnadsfunktion är tillräckligt involverade i AML-arbetet. Även här valde FI att kommunicera förväntningar snarare än att direkt sanktionera; inga sanktionsavgifter delades ut i denna insats, men företagen har fått individuell feedback och i vissa fall förelägganden att åtgärda brister.

Övriga tillsynsinsatser: FI analyserar årligen företagens egna återrapporteringar om penningtvättsarbetet. En rapport från 2022 sammanställde data från åren 2018 - 2021 och identifierade fortsatt förbättringspotential på områden som kundkontroll och rapporteringsdisciplin. Bland annat noterades att andelen företag som lämnar in den obligatoriska årsrapporten i tid ökade, men att vissa fortfarande brister vilket lett till förelägganden och ibland vite. FI använder sådan information för att riskklassificera företag och rikta sin tillsyn mot de största riskerna. Sammantaget visar FI:s samlade tillsynsarbete, både sanktioner och rapporter, att det finns sektorsvisa skillnader. Banker och betalningsinstitut har stått i första rummet vad gäller faktiska sanktioner, medan t.ex. livförsäkringsbolag hittills klarat sig utan böter men ändå fått tydliga förbättringskrav via FI:s rapporter.

5. Sanktionsavgifter fördelade per sektor

Hittills har banksektorn burit lejonparten av sanktionsavgifterna kopplade till penningtvätsregelverket. Storbankerna (Swedbank, SEB, Nordea, Handelsbanken) dominerar totalt sett, inte oväntat med tanke på deras storlek och de uppmärksammade fall som uppdragats. Mindre banker och kreditmarknadsbolag (inklusive sparbanker, nischbanker och liknande) har också drabbats av sanktioner men i betydligt lägre belopp. Betalningsinstitut, växlingskontor och fintech-bolag utgör en tredje kategori; här finns några relativt höga avgifter (t.ex. Trustly 130 Mkr, Klarna 500 Mkr) men många aktörer är små och hanterar mindre volymer, vilket återspeglas i lägre sanktionsbelopp.

utgör 500 Mkr. Betalningsinstitut och liknande står för en ännu mindre andel (cirka 150 Mkr totalt) exempelvis har två större betalningsförmedlare, Trustly och ClearOn, fått 130 Mkr respektive 14 Mkr i avgift, och ett kryptoväxlingsbolag (Goobit) 2 Mkr. Hittills (per 2024) har inga sanktionsavgifter utdömts inom försäkrings- eller värdepapperssektorn specifikt för penningtvätsregelverket. FI:s tillsynsrapporter indikerar dock att även dessa sektorer granskas noga och kan bli föremål för sanktion om brister inte åtgärdas framöver.



Figur 3: Totala sanktionsavgifter 2015 - 2024 per sektor (Mkr). "Storbanker" avser Swedbank, SEB, Nordea, Handelsbanken; "Övriga banker" innefattar övriga banker och kreditinstitut som fått sanktion (t.ex. sparbanker, nisch- och fintech-banker); "Övriga institut" avser betalningsinstitut, växlingskontor och liknande.

Av Figur 3 framgår att storbankerna står för den absolut största andelen av utdömda sanktionsbelopp, över 5 miljarder kronor, motsvarande cirka 85 - 90 % av totalsumman. Detta beror främst på de rekordstora böterna mot Swedbank och SEB år 2020. Övriga banker har tillsammans fått ca 600 - 700 Mkr i avgifter, varav en enskild aktör (Klarna)



6. Slutsatser

Granskningen av FI:s sanktionsbeslut och tillsynsrapporter inom penningtvättsområdet visar på en allt strängare tillsyn och en högre ambitionsnivå från myndighetens sida. Finansinspektionen har efter 2015 trappat upp sin kamp mot penningtvätt, med kulmen kring 2020 då globala skandaler utlöste rekordböter för svenska storbanker. Vanliga försyndelser har identifierats och kommunicerats tydligt: samtliga finansiella företag förväntas ha en genomarbetad riskbedömning, god kundkännedom, effektiv transaktionsövervakning och en stark intern kontrollkultur. Där detta åsidosatts har FI inte tvekat att ingripa med kraftiga sanktioner eller bindande förelägganden.

För företagen innebär utvecklingen att regelefterlevnad inom AML-området blivit en strategisk fråga i toppledning. Kostnaden, både i form av potentiella sanktionsavgifter och skadat anseende, av att inte ha robusta processer är i dag avsevärt högre än för 10 år sedan. Samtidigt ger FI viss vägledning genom sina rapporter, vilket indikerar att myndigheten önskar proaktivt höja lägstanivån i branschen. Företag som tar till sig av FI:s generella iakttagelser (t.ex. de brister som lyfts fram i tillsynsrapporterna) och som tidigt åtgärdar liknande svagheter i sin egen verksamhet, minskar risken att drabbas av framtida sanktioner.

Sammanfattningsvis har Finansinspektionens tillsyn inom penningtvättsområdet skärpts betydligt både vad gäller omfattningen av granskningar och de faktiska konsekvenserna för överträdelse. En stark signal har skickats till marknadens aktörer att regelefterlevnad och ett aktivt arbete mot penningtvätt inte är förhandlingsbart. Vi kan förvänta oss att FI fortsätter på den inslagna vägen med höga krav, och att penningtvättsregelverket förblir ett av de mest prioriterade tillsynsområdena även under kommande år.



7. Framtidens AML-tillsyn: AMLA och den nya europeiska strukturen

EU:s nya myndighet för bekämpning av penningtvätt och finansiering av terrorism, AMLA (Anti-Money Laundering Authority), innebär ett avgörande steg mot mer enhetlig, kraftfull och riskbaserad tillsyn inom unionen. AMLA inrättas genom förordning (EU) 2024/1620, som antogs i maj 2024 och träder i kraft den 1 juli 2025. Myndigheten ska ha sitt säte i Frankfurt och förväntas inleda operativ tillsynsverksamhet under 2026.

AMLA kommer att få direkt tillsynsansvar över ett urval av högriskaktörer inom den finansiella sektorn, inklusive större banker, betaltjänstleverantörer och kryptotjänsteföretag. Urvalet sker utifrån unionsgemensamma riskkriterier, där samtliga medlemsstater förväntas bidra med minst en tillsynsenhet i ett initialt urval om upp till 40 aktörer. Utöver detta får AMLA ett brett mandat att samordna, harmonisera och utveckla tillsynen inom EU. Myndigheten ska bland annat:

- Fastställa bindande tekniska standarder (RTS) inom områden som riskbedömning, kundkännedom (KYC), tredjepartsförlitande, filialverksamhet i tredjeland, outsourcing och rapportering.
- Utfärda sanktionsavgifter på upp till 10 procent av ett företags totala årliga omsättning vid överträdelser av AML-regelverket.
- Övervaka nationella tillsynsmyndigheter och säkerställa enhetlig tillämpning av AML/CFT-regler inom hela unionen.

AMLA:s mandat signalerar en tydlig ambitionshöjning vad gäller krav på modellvalidering, datakvalitet, spårbarhet och systemintegration. Särskilt fokus riktas mot att säkerställa att riskbedömningar, kundklassificeringar och transaktionsövervakning inte hanteras i separata system eller enheter, utan är samordnade i ett gemensamt riskramverk med löpande återkoppling. Dokumentation och förmåga att motivera modellval, tröskelvärden och kontrollåtgärder blir

centralt, liksom insyn i outsourcing- och distributionskedjor.

Parallellt med utvecklingen på EU-nivå sker även en breddning av den svenska penningtvättstillsynen. Nationella tillsynsorgan som Finansinspektionen, Länsstyrelserna, Revisorsinspektionen och Advokatsamfundet har under senare år intensifierat granskningen av verksamhetsutövare utanför finanssektorn exempelvis fastighetsmäklare, revisorer, advokater, bolagsbildare och varuhandlare. AMLA kommer inte att ha direkt tillsyn över dessa kategorier, men myndigheten får ett uttryckligt mandat att samverka med nationella tillsynsorgan för att främja harmoniserad tillämpning av regelverket även inom icke-finansiella sektorer.

Det är också viktigt att se AMLA i ljuset av de övriga delar som ingår i EU:s nya AML-paket. Den nya förordningen om bekämpning av penningtvätt (AMLR) kommer att bli direkt tillämplig i alla medlemsländer från den 10 juli 2027, vilket innebär att företag måste anpassa sig till ett enhetligt och detaljstyrt regelverk på EU-nivå. Samma dag ska även det sjätte AML-direktivet (AMLD6) vara införlivat i nationell lagstiftning. Tillsammans med AMLA markerar dessa regelverk ett paradigmskifte i EU:s syn på AML/CFT från decentraliserad efterlevnad till integrerad styrning, kontroll och tillsyn på unionsnivå.

Sammanfattningsvis innebär den nya AML-strukturen att tillsynen blir både djupare genom skarpare krav på riskhantering, dokumentation och systemintegration och bredare, genom sektorsövergripande harmonisering och ett närmare samspel mellan EU och nationella myndigheter. För svenska verksamhetsutövare betyder detta att AML-arbetet inte längre bara är en fråga om formell efterlevnad, utan om verklig riskförståelse, affärsstyrning och långsiktig förtroendehantering.

Denna rapport baseras uteslutande på offentligt tillgängliga beslut och rapporter från Finansinspektionen och andra tillsynsmyndigheter. Alla omnämnda företag förekommer i dokumenterade tillsyns- eller sanktionsärenden, som redovisas i referenslistan. Syftet är att belysa återkommande mönster i tillsynspraxis, inte att bedöma enskilda aktörers nuvarande verksamhet eller regelefterlevnad. Informationen har kontrollerats mot källorna med största möjliga noggrannhet. BDO ansvarar inte för förändringar som kan ha skett efter respektive beslutsdatum.

Referenser

- Finansinspektionen (2013).

Beslut: Nordea Bank AB - Anmärkning och straffavgift 30 miljoner kronor (FI Dnr 12-7237, 16 april 2013) [fi.se](#)

- Finansinspektionen (2013).

Beslut: Forex Bank AB - Varning och straffavgift 50 miljoner kronor (FI Dnr 13-980, 22 maj 2013) [fi.se](#) [sverigesradio.se](#).

- Finansinspektionen (2015).

Pressmeddelande: Nordea får varning och straffavgift; Handelsbanken får anmärkning (19 maj 2015) [fi.se](#).

- Finansinspektionen (2018).

FI Tillsyn Rapport 1: Erfarenheter från penningtvätts-tillsynen 2016 - 2017 (12 april 2018)

- Finansinspektionen (2020a).

Beslut: Swedbank AB - Varning och sanktionsavgift 4 000 Mkr (FI Dnr 19-22127, 19 mars 2020) [fi.se](#).

- Finansinspektionen (2020b).

Beslut: Skandinaviska Enskilda Banken AB - Anmärkning och sanktionsavgift 1 000 Mkr (FI Dnr 19-12288, 25 juni 2020) [fi.se](#).

- Finansinspektionen (2020c).

Beslut: JAK Medlemsbank - Anmärkning och sanktionsavgift 1,6 Mkr (FI Dnr 19-12288, 18 juni 2020) [fi.se](#).

- Finansinspektionen (2022a).

FI Tillsyn - Analys av penningtvättsrapporteringen 2018 - 2021 (Rapport publicerad 14 juni 2022)

- Finansinspektionen (2022b).

Beslut: Trustly Group AB - Varning och sanktionsavgift 130 Mkr (FI Dnr 21-8391, 22 februari 2022) [fi.se](#).

- Finansinspektionen (2022c).

Beslut: ClearOn AB - Varning och sanktionsavgift 14 Mkr (FI Dnr 20-21809, 22 februari 2022) [fi.se](#).

- Finansinspektionen (2022d).

Beslut: Länsförsäkringar Bank - Anmärkning och sanktionsavgift 90 Mkr (FI Dnr 21-20800, 14 december 2022) [fi.se](#).

- Finansinspektionen (2023a).

FI Tillsyn Rapport 31: Hantering av penningtvättrisker i värdepappersrörelsen (31 januari 2025)

- Finansinspektionen (2023b).

FI Tillsyn Rapport 32: Livförsäkringsföretagens hantering av risker för penningtvätt (31 januari 2025)

- Finansinspektionen (2023c).

Beslut: Aros Kapital AB - Varning och sanktionsavgift 45 Mkr (FI Dnr 22-14442, 13 december 2023) [fi.se](#).

- Finansinspektionen (2023d).

Beslut: Goobit AB - Anmärkning och sanktionsavgift 2 Mkr (FI Dnr 21-289, 21 juni 2023) [fi.se](#).

- Finansinspektionen (2024).

Beslut: Klarna Bank AB - Anmärkning och sanktionsavgift 500 Mkr (FI Dnr 22-13340, 11 december 2024) [fi.se](#).

- Reuters (2015). "Lenders Nordea, Handelsbanken fined over money laundering rules" - **Reuters News, 19 May 2015** [reuters.comi-law.com](#).

- Sveriges Radio (2013). "Forex får straffavgift på 50 miljoner" - **Ekot, 22 maj 2013** [sverigesradio.se](#)

- Sak & Liv (2023). "Swedbank får anmärkning av FI och sanktionsavgift på 850 Mkr" - **Nyhetsartikel, 15 mars 2023** [sakochliv.se](#).

- Dagens industri (2023). "Klarna får böter på en halv miljard - överträtt penningtvättsregler" - **Di.se, 11 dec 2024** [efn.se](#).



www.bdo.se