Nationell riskbedömning 2023/2024 – Neobanker

EN RAPPORT AV: Bolagsverket, Brottsförebyggande rådet, Ekobrottsmyndigheten, Fastighetsmäklarinspektionen, Finansinspektionen, Kronofogdemyndigheten, Länsstyrelsen i Skåne län, Länsstyrelsen i Stockholms län, Länsstyrelsen i Västra Götalands län, Polismyndigheten, Revisorsinspektionen, Skatteverket, Spelinspektionen, Sveriges advokatsamfund, Säkerhetspolisen, Tullverket samt Åklagarmyndigheten

Utgivare: Polismyndigheten
Diarienummer: A340.719/2024
Version: Reviderad version, maj 2024
Tryck: Polisens tryckeri Stockholm, augusti 2024
Grafisk form: Blomquist Communication, blomquist.se

Sammanfattning

Det här är Samordningsfunktionens fjärde nationella riskbedömning av penningtvätt och finansiering av terrorism i Sverige. Rapporten är avgränsad till att handla om digitala finansiella tjänster med specifik inriktning på tjänster erbjudna av neobanker. Riskbedömningen 2023/2024 syftar till att identifiera möjliga hot, sårbarheter och risker som digitala finansiella tjänster erbjudna av neobanker kan innebära för bekämpningen av penningtvätt eller terrorismfinansiering.

Termen neobank har använts åtminstone sedan mitten av 2010-talet för att beskriva fintechbolag som utmanar traditionella banker, bland annat genom att fokusera på innovation, rörlighet och snabb implementering av ny teknik. I denna rapport används begreppet neobank om en verksamhet som erbjuder liknande tjänster och produkter som traditionella banker, men som primärt har sin närvaro på internet och som erbjuder sina tjänster via appar och webbplatser. Neobanker inriktade mot företag erbjuder ofta även bokförings- och faktureringstjänster. Neobanker kan även erbjuda konkurrenskraftiga priser med bland annat lägre avgifter. Detta har medfört att neobanker blivit attraktiva på den finansiella marknaden och att framväxten av neobanker har ökat under senare år. I slutet av 2023 fanns det cirka 30 verksamhetsutövare under Finansinspektionens tillsyn som motsvarar ovanstående definition av neobanker.

Neobanker kan utnyttjas för penningtvätt och finansiering av terrorism eftersom de tjänster som vissa neobanker erbjuder möjliggör viss anonymitet till följd av lägre grad av kontroll, vilket bedöms vara attraktiva för kriminella aktörer. Neobanker förekommer i Ekobrottsmyndighetens förundersökningar där anonymiserade tjänster innebär att de används för många transaktioner och stora belopp, ofta för penningtvätt av brottsvinster från skattebrott och avlöning av svart arbetskraft, samt i Skatteverkets skatteutredningar som ett sätt att dölja inkomster från beskattning. Även Säkerhetspolisen ser att neobanker förekommer i ökande utsträckning i dess operativa arbete.

Hotet och sårbarheten bedöms på en fyrgradig skala (1–4 där 4 är högst). Risken för penningtvätt och finansiering av terrorism bedöms sedan som en sammanvägning av hot och sårbarheter, även detta på en fyrgradig skala (1–4). Hotet för penningtvätt och finansiering av terrorism för neobanker bedöms vara högt (4). Sårbarheten bedöms vara betydande (3), den näst högsta nivån. Bedömningarna baseras på ett antal identifierade hot och sårbarheter, exempelvis det stora antalet inblandade parter och jurisdiktioner i samband med transaktioner, svårigheter avseende spårbarhet av transaktioner, avsaknad av fysiska möten i samband med verifikations- och kundkännedomsprocessen samt möjligheterna att dölja verklig kontohavare, avsändare och mottagare genom bland annat utnyttjande av kontomålvakter.

Baserat på de hot och sårbarheter som identifierats bedöms risken för neobanker också vara betydande (3). En konsekvens av att neobanker erbjuder vissa tjänster som kan används för penningtvätt och finansiering av terrorism riskerar att skada förtroendet för det finansiella systemet och neobanker som företeelse. Andra konsekvenser är att upptäckt och lagföring av penningtvätt och finansiering av terrorism försvåras, vilket i sin tur kan leda till lägre lagföring, samt att skatteutredningar kan förhindras vilket har som konsekvens minskade skatteintäkter om inte rätt beskattning kan göras. Den yttersta konsekvensen av finansiering av terrorism är genomförda terrordåd.

Denna rapport avslutas med ett antal rekommendationer, bland annat att kunskapen om neobanker och deras risker behöver öka men också ett antal rekommendationer om förbättrat informationsutbyte och rapportering till Finanspolisen och Skatteverket, förbättrade kundkännedomsprocesser samt att utöka rapporteringskravet avseende klientmedelskonton.


£250.50
Cryptocurrency Price
Since last week

Innehåll

1. Inledning

Det här är Samordningsfunktionens fjärde nationella riskbedömning av penningtvätt och finansiering av terrorism i Sverige. Rapporten handlar om digitala finansiella tjänster och är avgränsad till att handla om neobanker och de tjänster och produkter dessa erbjuder och den risk för och konsekvenser av penningtvätt och finansiering av terrorism som följer av detta.

Ett riskbaserat förhållningssätt i arbetet mot penningtvätt och finansiering av terrorism är viktigt för att uppnå en fungerande och effektiv regim där olika delar av samhället samverkar. I Sverige omfattas flera olika typer av aktörer där tillsynsmyndigheter, brottsbekämpande myndigheter och verksamhetsutövare (privata aktörer) är de främsta. Bekämpningen av penningtvätt och finansiering av terrorism sker inte enbart nationellt utan även internationellt, bland annat genom samarbetet inom organisationen Financial Action Task Force (FATF) samt på EU-nivå genom lagstiftning, riktlinjer och rekommendationer.

Av förordningen (2009:92) om åtgärder mot penningtvätt och finansiering av terrorism framgår att Samordningsfunktionen löpande ska identifiera, kartlägga och analysera riskerna och metoderna för penningtvätt och finansiering av terrorism i Sverige. Dessutom ska Samordningsfunktionen sammanställa, årligen eller efter nya eller förändrade risker, uppdatera och i lämplig utsträckning offentliggöra nationella riskbedömningar för penningtvätt respektive finansiering av terrorism.

1.1 Syfte och mål

Området bank- eller finansieringsrörelse ingick i 2020/2021 års nationella riskbedömning.[1] Även om neobanker inte explicit nämns i den tidigare riskanalysen görs bedömningen att de ingår i samma sektor eftersom de bedriver bankliknande verksamhet. I den tidigare riskbedömningen lyftes exempelvis möjligheten till anonymitet upp som en risk kopplad till bank- eller finansieringsrörelsen, exempelvis genom användande av målvakter, bulvaner eller förfalskad dokumentation. Att kriminella aktörer snabbt kan genomföra transaktioner genom flera produkter beskrevs som ytterligare en risk kopplad till sektorn. De risker som då tydliggjordes visar på behovet av en djupare förståelse av detta specifika område och dess risker.

Den nationella riskbedömningen 2023/2024 syftar till att identifiera möjliga hot, sårbarheter och risker som de digitala produkter och finansiella tjänster som neobanker erbjuder kan innebära. Målet med riskbedömningen 2023/2024 är att formulera riskreducerande rekommendationer utifrån de identifierade hoten, sårbarheterna och riskerna.

1 Rapport, Samordningsfunktionen (2021) *Nationell riskbedömning av penningtvätt och finansiering av terrorism i Sverige 2020/2021.*

1.2 Samordningsfunktionen

Inom Polismyndigheten ska det finnas en samordningsfunktion för åtgärder mot penningtvätt och finansiering av terrorism.[2] Samordningsfunktionen består av följande 16 myndigheter: Bolagsverket, Brottsförebyggande rådet (Brå), Ekobrottsmyndigheten, Fastighetsmäklarinspektionen, Finansinspektionen, Kronofogdemyndigheten, Länsstyrelsen Skåne, Länsstyrelsen Stockholm, Länsstyrelsen i Västra Götaland, Polismyndigheten, Revisorsinspektionen, Skatteverket, Spelinspektionen, Säkerhetspolisen, Tullverket, Åklagarmyndigheten samt av Sveriges Advokatsamfund. Riskbedömningen är ett resultat av medlemmarnas gemensamma arbete.

Arbetet med årets riskbedömning har främst skett i en mindre projektgrupp bestående av Polismyndigheten genom Finanspolisen, Finansinspektionen, Ekobrottsmyndigheten, Skatteverket och Brottsförebyggande rådet.

1.3 Avgränsning

Denna rapport är avgränsad till att handla om neobanker, deras konstruktion och de tjänster de erbjuder. Det finns ingen entydig eller legal definition på vad en neobank är. I denna riskanalys omfattar begreppet neobank verksamheter som bedriver bank- eller bankliknande verksamhet men som primärt har sin närvaro på internet och som erbjuder sina tjänster via appar och webbplatser. En neobank har, i motsats till traditionella banker, i regel inga fysiska besökskontor.

De verksamheter som ingår i definitionen behöver inte nödvändigtvis ha banktillstånd utan kan utgöras av bland annat betalningsinstitut eller institut för elektroniska pengar (nedan kallat e-pengainstitut). Det avgörande för att ingå i definitionen är istället vilka produkter och tjänster som verksamheten erbjuder, vilka ofta ligger nära traditionella bankverksamheters produkter och tjänster, oaktat tillståndstyp.

1.4 Metod

Den nationella riskbedömningen har utgått från FATF:s metod för att göra en riskbedömning av hotet för penningtvätt och finansiering av terrorism.[3] Rapporten är baserad på kvantitativa data och kvalitativa resonemang utifrån de deltagande myndigheternas expertkunskaper.

1.5 Målgrupp

Mottagare av riskbedömningen är Regeringskansliet, Samordningsfunktionens medlemmar och verksamhetsutövare som direkt och indirekt omfattas av riskbedömningen.

1.6 Regelverken

Penningtvätt och finansiering av terrorism regleras både i administrativa och straffrättsliga regelverk. Det administrativa regelverket, lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism (PTL), är centralt och ska förebygga och motverka att finansiell verksamhet och annan näringsverksamhet utnyttjas för penningtvätt och finansiering av terrorism. Det straffrättsliga regelverket syftar till att lagföra personer som utfört penningtvätt eller finansiering av terrorism och omfattas främst av lagen (2014:307) om straff för penningtvättsbrott och lagen (2022:666) terroristbrottslag.

2 Förordning (2009:92) om åtgärder mot penningtvätt och finansiering av terrorism.

3 Se FATF:s webbplats för mer information, fatf-gafi.org

2. Neobanker

2.1 Vad är en neobank?

Termen neobank har använts åtminstone sedan mitten av 2010-talet för att beskriva fintech-bolag som utmanar traditionella banker, bland annat genom att fokusera på innovation, rörlighet och snabb implementering av ny teknik. För att möta kundernas behov och preferenser introducerar neobanker ofta nya funktioner, produkter och tjänster betydligt snabbare än traditionella banker. Genom neobankernas lägre kostnader för fysisk infrastruktur (exempelvis genom att inte tillhandahålla besökskontor) kan de ofta även erbjuda konkurrenskraftiga priser med bland annat lägre avgifter. Detta har medfört att neobanker blivit attraktiva på den finansiella marknaden och att framväxten av neobanker har ökat under senare år.

För att starta en neobank med hemvist i Sverige krävs tillstånd från Finansinspektionen. Neobanker är också skyldiga att följa finansiella regelverk. De måste skydda kunddata, följa penningtvättsregelverket och upprätthålla robusta åtgärder för att trygga säkerheten för transaktioner och kundinformation.

Endast institut med banktillstånd får kalla sig ”bank”, men då det inte finns någon legal definition av neobank får även aktörer utan banktillstånd använda begreppet neobank. En skillnad är att en ”bank” måste vara ansluten till minst ett generellt betalningssystem, antingen via clearingsystem som Bankgirot eller via kortsystem som Visa och Mastercard. Samtidigt är det möjligt för en verksamhet utan banktillstånd att samarbeta med en verksamhet som har banktillstånd och därmed erbjuda fler tjänster.

I slutet av 2023 fanns det enligt Finansinspektionen bedömningen ungefär 30 banker, betalningsinstitut och e-pengainstitut som alla kan anses utgöra svenska neobanker utifrån den definition av neobanker som ligger till grund för denna rapport. Dessa 30 neobanker har tillstånd hos Finansinspektionen och ligger under myndighetens tillsyn. Svenska konsumenter kan dock bli kunder hos utländska neobanker som har tillstånd hos ett EU-land för att kunna erbjuda sina produkter och tjänster på den europeiska marknaden. Europeiska neobanker registrerade i andra länder, men som är aktiva i Sverige, ligger inte under svenska Finansinspektionens tillsyn.

Med utgångspunkt i den definition av neobanker som ligger till grund för rapporten omfattar ovan nämnda 30 neobanker bland annat följande typer av verksamheter.

1. **Neobanker med banktillstånd**, vilka har startats som helt digitala banker och har därmed aldrig haft några fysiska besökskontor. Den här typen av neobank erbjuder vanligtvis ett brett produktutbud och är i många avseenden väldigt lika traditionella banker vad gäller produkter och tjänster.

2. **Neobanker som är ett betalningsinstitut**, som exempelvis erbjuder betalkort och genom sitt gränssnitt möjliggöra insättningar och uttag på kortet inom ramen för sitt tillstånd. I det fall neobanken även vill tillhandahålla krediter eller sparprodukter kan det göras med samarbetsavtal med en bank med erforderliga tillstånd, genom ett s.k. white labeling-upplägg.

3. **Neobanker som är e-pengainstitut**, vilka många gånger är inriktade mot företagskunder såväl inom som utanför Sverige. Utöver utgivning av elektroniska pengar kan en sådan neobank tillhandahålla betalnings-transaktioner genom kreditutrymme, företagskonton, betalkort, och faktureringstjänster.

2.2 Hur blir man kund i en neobank?

Neobanker präglas ofta av en hög grad av teknisk innovation som möjliggör snabba onboardingprocesser.[4] En skillnad mellan traditionella banker och neobanker är just hur snabbt en ny kund kan öppna ett konto även om båda måste följa samma regelverk när det gäller kundkännedomsprocesser.[5]

Att bli kund och kunna använda konton i neobanker är vanligtvis en enkel tvåstegs-process. Det första steget är att registrera sig som kund vilket ofta går snabbt och kräver bara ett mobilnummer eller en e-postadress. Just snabbheten och enkelheten lyfts ofta fram som en konkurrensfördel. Det andra steget är verifiering av kundens uppgifter. Det steget består oftast av att kunden skickar in en digital kopia av en identitetshandling och ett foto av sig själv. Hos vissa neobanker tillämpas inte tvåstegsprocess, utan identifieringen görs enbart via e-legitimation. I båda fallen saknar processen fysiska möten mellan neobanken och kunden. En traditionell bank har möjlighet att kalla kund till ett fysiskt kundmöte för att verifiera kunduppgifter vilket neobanker saknar förutsättningar till, i och med att neobanker i regel saknar fysiska besökskontor.

Processen för att bli företagskund varierar mycket, där den mest förenklade processen går ut på att företrädare för företaget enbart krävs på en e-postadress för att kunna bli kund hos en neobank. Erfarenheter från tillsyn och annan myndighetsinformation har visat att det även förekommer neobanker vars processer för potentiella företagskunder bland annat innefattar identifiering av firmatecknare, verifiering av verklig huvudman och kontroll av företagsuppgifter mot externa register.

4 Med onboardingprocess menas tillvägagångssättet för att bli verifierad som kund i en bank eller andra finansiella institut.

5 Kundkännedomsprocess är den process som genomförs av verksamhetsutövare för att identifiera sina kunder och bedöma deras riskprofil. Det är lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism som ställer krav på en sådan process.

2.3 Produkter och tjänster

Neobankernas produkter och tjänster erbjuds endast digitalt. Konton, betalkort och krediter utgör några av de vanligaste tjänsterna på många neobanker. Ofta erbjuder neobanker både fysiska och virtuella betalkort. Virtuella betalkort fungerar som fysiska betalkort, men kortuppgifterna finns endast tillgängliga digitalt. Virtuella betalkort kan göras tillgängliga för en kund direkt efter att denne har registrerat sig som kund, men innan de av kunden lämnade uppgifterna har verifierats av verksamhetsutövaren. Vissa neobanker erbjuder också omedelbara kontoöppningar utan exempelvis inkomstkrav, samt tillgång till betaltjänster innan kundens uppgifter har verifierats.

Investeringsrådgivning, finansiell översikt, olika former av investeringar i aktier eller ädelmetaller, växling mellan valutor och hantering av kryptovalutor utgör ytterligare exempel på tjänster som tillhandahålls. Flera neobanker började som handelsplattformar för kryptovalutor och erbjuder sina kunder kryptovalutaplånböcker och möjlighet att koppla betalkort till kryptovalutaplånboken. Ofta kan man också flytta kryptovalutor inom neobanken och till och från externa plånböcker.

Vissa neobanker erbjuder utökade tjänster, exempelvis så kallade gemensamma betalkonton där flera personer är kontohavare. De kan bland annat använda betalkort kopplade till kontot, dela upp och fördela betalningar samt göra snabba överföringar till andra konton i samma neobank. Överföringar kan exempelvis genomföras genom scanning av QR-koder eller genom att ange mottagarens e-postadress eller ett användarnamn. Några neobanker ger även kunder möjlighet att koppla upp sina betalkort mot olika betallösningar såsom Google Pay eller Apple Pay. Neobankers tjänster och erbjudanden finns ytterligare beskrivet i Finanspolisens rapport om neobanker.[6]

De tjänster som vissa neobanker inte kan erbjuda bland annat på grund av begränsningar i det aktuella tillståndet, kan erbjudas genom samarbetsavtal med andra leverantörer genom så kallade white labeling-upplägg (se avsnitt 2.5 om White labeling). Exempelvis har ett betalningsinstitut inte tillåtelse att erbjuda inlåning genom sparkonton inom ramen för det tillstånd som Finansinspektionen beviljar i enlighet med lagen om betaltjänster. Istället kan de erbjuda sparprodukter genom ett samarbetsavtal med en bank, som betalningsinstitutet kan förmedla sparkunder till. Andra exempel är att externa parter tillhandahåller betalkort eller kryptovalutaplånböcker.

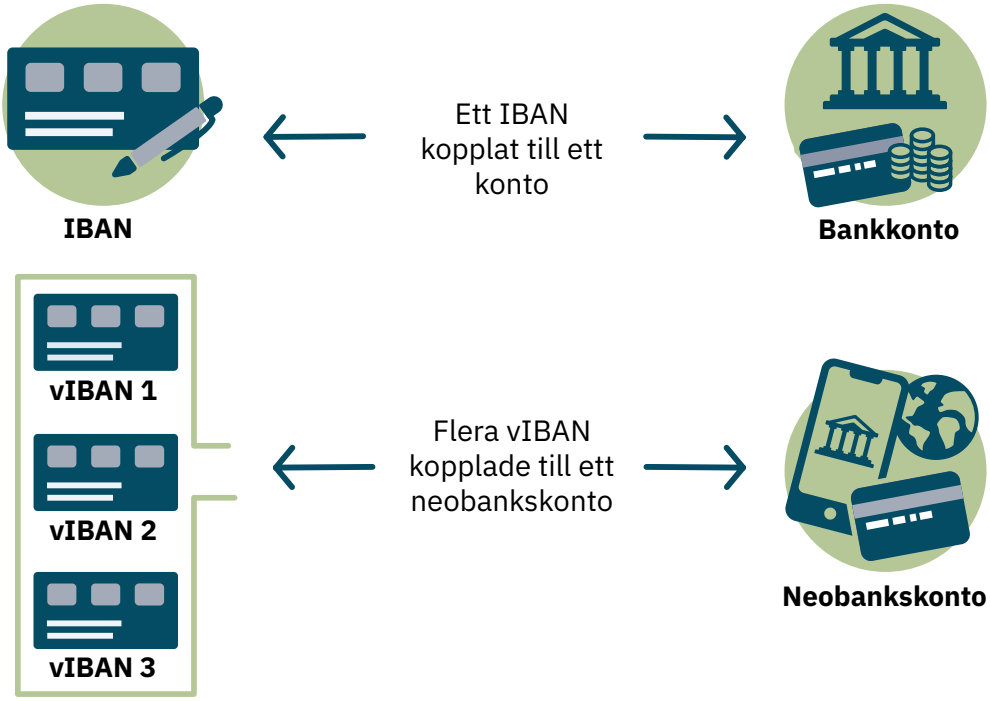
Företagskunder är ett attraktivt segment och flera neobanker tillhandahåller därför lösningar särskilt inriktade mot företag. Utvecklingen av antalet neobanker som riktar sig till endast företagskunder är snabbväxande. Det finns dels svenska neobanker av detta slag, men även en del utländska som både är etablerade i Sverige och riktar sig mot den svenska marknaden. Skillnaden mellan neobanker inriktade mot företag jämfört med neobanker inriktade mot privatpersoner ligger främst i betalningsvolymerna i de transaktioner som företagskunderna genomför samt storleken på kreditutrymmet som erbjuds företagskunder jämfört med privatpersoner. Ytterligare en skillnad är att företagskunder erbjuds tilläggstjänster som bland annat bokföring, faktureringstjänster och virtuella IBAN.

6 Rapport, Finanspolisen (2022) *Neobanker*.

2.4 Virtuella IBAN

International Bank Account Number (IBAN) är en global standard för att identifiera bankkonton och används främst vid internationella betalningar. Neobanker skapar inte sällan virtuella bankkonton för sina kunder. Virtuella IBAN (fortsättningsvis kallat vIBAN) är ett indentifikationssystem som tilldelar dessa virtuella bankkonton en unik IBAN-kod. vIBAN används som en identifierare för det virtuella bankkontot och underlättar genomförandet av transaktioner. En viktig skillnad mellan traditionella IBAN och vIBAN är att varje IBAN normalt sett matchas med endast ett bankkonto, vilket innebär att det bara finns ett enda bankkonto kopplat till varje enskilt IBAN-nummer. För vIBAN däremot kopplas normalt flera nummer till samma bankkonto (figur 1). Denna typ av konto beskrivs närmare i stycke 5.5.6.

Figur 1. IBAN och vIBAN och hur dessa kopplas till olika konton.



2.5 White labeling

Så kallad white labeling förekommer inom många olika sektorer och innebär att företag köper in och marknadsför redan utvecklade produkter som sina egna, under eget varumärke och med egna villkor. Inom den finansiella sfären används det vanligtvis av finansiella institut som använder bankers API:er[7] för att utveckla egna plattformar för finansiella tjänster och produkter, med hjälp av de licensierade bankernas befintliga infrastruktur. Det är särskilt förekommande bland fintechbolag och neobanker utan egna banktillstånd.

Neobanker som saknar egna banktillstånd och som är uppbyggda som så kallade white label-banker har alltså samarbetsavtal med etablerade banker med tillstånd och som bistår med de regulatoriska och juridiska aspekterna av samarbetet. Sådana neobanker, som många gånger utgörs av betalningsinstitut eller e-pengainstitut, får därmed möjlighet att erbjuda produkter som faller utanför ramen för det egna tillståndet.

Finansinspektionen har genom erfarenheter i tillsynen noterat att det blivit vanligare att finansiella företag använder sig av den typen av samarbetslösningar för att erbjuda sina kunder produkter som det egna företaget inte har tillstånd för att tillhandahålla. Genom samarbetsavtal med etablerade banker kan sådana neobanker under det egna varumärket erbjuda exempelvis sparprodukter, som enligt svensk lagstiftning enbart kan erbjudas av banker med banktillstånd. I marknadsföringen är det många gånger inte uppenbart för kundmålgruppen att det är någon annan bank som kunden de facto kommer att ingå avtal med. Ett annat exempel kan vara att ett företag som saknar tillstånd för kreditförmedling ingår ett samarbetsavtal med en kreditgivare och upplåter sin plattform för kreditförmedling. Beroende på hur samarbetsavtalet är utformat parterna emellan kan företagen åta sig att utföra delar av exempelvis kundkännedomsprocesser eller kreditprövningsprocesser åt varandra. Ur ett penningtvättsperspektiv väcker upplägg av det här slaget frågor om bland annat riskägande och ansvarsfördelning i kundkännedomsprocesser och transaktions-monitorering, i och med att samarbetsavtal och förmedling av bankliknande tjänster idag inte är specifikt reglerat enligt svensk lag.

7 Enligt Skatteverkets definition: Förkortningen API står för Application Program Interface. Det är ett numera standardiserat sätt att överföra information som vi använder dagligen, kanske ofta utan att veta om det. Det är exempelvis API:er som förser våra mobilappar med allt från väderprognoser till träningsscheman, samt bokföringssystem med saldon från en bank.

3. Neobankers förekomst i utredningar

Neobanker förekommer i Ekobrottsmyndighetens förundersökningar. Neobanker med ett stort antal kunder utgör av naturliga skäl den största delen, men i förundersökningarna förekommer även neobanker i varierande storleksordning. Neobankerna i förundersökningarna är därtill registrerade i en rad olika länder, både i Sverige och utomlands. Neobanker som förekommer i svenska utredningar är dock till övervägande del utländska neobanker. Flera utredningar och rapporter har visat att företag ofta används som brottsverktyg inom organiserad brottslighet för att begå ekonomisk brottslighet och tvätta pengar.[8] Neobanker som är direkt inriktade mot företag är också relativt vanligt förekommande i förundersökningarna.

I förundersökningarna förekommer neobankerna på samma sätt som traditionella banker, det vill säga att personer och företag har konton genom vilka de skickar och tar emot pengar. Utredningarna visar att neobanker används i penningtvättsupplägg där brottsvinster förs över till neobankskonton, antingen direkt eller via vanliga bankkonton eller via olika betalplattformar. Därefter förs brottsvinsterna vidare till neobankskonton som antingen innehas av huvudmännen i brottsupplägen eller av andra personer. Det handlar ofta om många transaktioner och stora belopp och neobanker utgör ofta första steget i en penningtvättsprocess. Brottsvinsterna kan sedan användas för konsumtion eller investeringar. Många neobanker tillhandahåller även handel med kryptovalutor vilket ger ytterligare möjligheter att försvåra spårandet av brottsvinster.

Tillvägagångssätten för att tvätta brottsvinster förändras och utvecklas i takt med nya betallösningar och aktörer på marknaden. Finanspolisens analyser visar att kriminella aktörer är flitiga användare av neobanker[9] i syfte att bland annat variera sina penningtvättupplägg, skikta pengar och sprida tillgångar.

Skatteverket har i skatteutredningar och i skattebrottsutredningar uppmärksammat att neobanker används i samband med skatteundandragande. Bygg och handel utgör vanligt förekommande branscher i utredningarna. Skatteundandragande kan i de fallen gå till på olika sätt, men samtliga har den gemensamma nämnaren att ett eller flera neobankskonton använts i brottsupplägget. I ärenden har det bland annat handlat om anställda från andra EU-länder eller tredjeland som är anställda av utländska underentreprenörer verksamma i Sverige, men som inte har anmält att de är aktiva i Sverige. Det innebär att företagen är okända för svenska myndigheter. Ersättningen för de svartanställdas arbete har i ett första steg betalats in till den utländska underentreprenören som därefter har fört över lönen till anställdas neobankskonton, utan att ha betalat erforderliga avgifter (skatteundandragande).

8 Brå 2015:22 Penningtvätt och annan penninghantering. Kriminella, svarta och grumliga pengar i legal ekonomi, Brå 2016:10 Kriminell infiltration av företag, Brå 2019:17 Penningtvättsbrott. En uppföljning av lagens tillämpning, SOU 2023:34 Bolag och brott– några åtgärder mot oseriösa företag.

9 Rapport, Finanspolisen (2021) *Finanspolisens årsrapport 2021.*

Det förekommer även exempel på att personer som är obegränsat skattskyldiga[10] i Sverige har fått sina löner från utländska arbetsgivare insatta på konton i utländska neobanker. Detta utan att några kontrolluppgifter har lämnats in till Skatteverket i Sverige.

I så sådana fall finns det en stor risk att ersättningar inte beskattas korrekt. I en skatteutredning har exempelvis en svensk person, utvandrad och bosatt i ett annat EU-land, tagit emot belopp från ett svenskt företag för utfört konsultarbete. Betalning för tjänsterna har satts in direkt på ett konto hos en utländsk neobank, och beloppen har inte redovisats i personens inkomstdeklaration i Sverige. Inom OECD och EU finns regleringar om automatiskt utbyte av uppgifter om finansiella konton för skatteändamål mellan skatteförvaltningar i länder, så kallade CRS-uppgifter och DAC2-uppgifter.[11] Inom ramen för CRS och DAC2-regelverket ska finansiella institut i de olika länderna rapportera konton som innehas av personer och företag med skatterättslig hemvist i annat land. Skatteverket har uppmärksammat att vissa länder inte klassificerar neobanker som sådana finansiella institut som ska rapportera finansiella konton, vilket innebär att syftet med regelverket kringgås. Det finns därmed dels en risk att skatt undandras, dels att penningtvätt inte uppmärksammas av Skatteverket.

Säkerhetspolisens bedömning är att neobanker uppträder i ökande grad bland personer som förekommer i Säkerhetspolisens underrättelseverksamhet. Möjligheten till anonymitet genom lägre grad av kontroll samt möjligheten att göra pengar tillgängliga omedelbart är en viktig faktor i det ökande användandet. Ett konkret exempel är en person som misstänks planera ett terrorattentat som använde en större internationell neobank för att personer i andra länder skulle kunna ta emot pengar. Personen satte in pengar på sitt konto och personer som hade möjlighet att göra uttag från kontot gjorde det i andra länder, både genom kortköp och kontantuttag. I detta fall rörde det sig om ett högriskland dit de flesta svenska banker inte utför transaktioner. Pengarna bedömdes gå till resor, men även till mat och uppehälle för individer involverade i attentatsplanering.

Erfarenheter från Finansinspektionens tillsyn av institut som likt neobanker drivs av teknologisk utveckling och som bedöms vara förenade med liknande risker har bland annat visat på bristfälliga åtgärder för kundkännedom som inte har bedömts vara adekvata givet den förhöjda inneboende risk för penningtvätt och finansiering av terrorism som den typen av verksamhet anses vara förenade med.

Bristfälliga åtgärder för kundkännedom, i kombination med de digitala banktjänsternas flexibilitet och smidighet som möjliggör genomförande av mångfaldiga transaktioner varje dag, medför förhöjda risker för såväl penningtvätt och finansiering av terrorism, som för andra typer av brott som exempelvis bedrägerier.

10 För fysiska personer finns det i 3 kap. 3 § Inkomstskattelagen tre fristående kriterier för att vara obegränsat skattskyldig i Sverige. Dessa kriterier är: bosatt i Sverige, stadigvarande vistelse i Sverige och väsentlig anknytning till Sverige. Obegränsad skattskyldighet innebär att man är skattskyldig i Sverige för alla sina inkomster i Sverige och från utlandet. Det finns dock undantag från skattskyldigheten såväl i intern rätt, till exempel sexmånadersregeln, som i skatteavtal.

11 CRS står för Common Reporting Standard och är OECD:s rapporteringsnorm för utbyte av upplysningar. DAC2 är EU:s motsvarighet till det.

I Brås rapport avseende bedrägerier framhålls att en digital bank- och betalmarknad möjliggör bedrägerier. Bankärenden som genomförs digitalt och som i regel är obevakade av bankpersonal, bedöms utgöra en naturlig förutsättning för flera typer av bedrägerier. För att öka konsumentskyddet fick Finansinspektionen i oktober 2023 i uppdrag av regeringen att granska hur betaltjänstleverantörerna arbetar för att förhindra bedrägerier.[12] Finansinspektionen ser särskilt allvarligt på utvecklingen av bedrägerierna på betalningsmarknaden, där social manipulation används för att lura brottsoffer och stora summor tillfaller kriminella ekonomin.

Samtidigt som en digital bank- och betalmarknad har bidragit till smidiga och snabba betalningslösningar har det också inneburit nya sätt för kriminella att utföra bedrägerier och snabbt tvätta och gömma vinsterna från bedrägerierna. Bedrägerier drabbar många och har över tid ökat i omfattning, Under 2022 polisanmäldes drygt 180 000 bedrägerier, vilket kan jämföras med drygt 50 000 anmälningar år 2000[13] med bedömda brottsvinster på cirka 5,8 miljarder kronor 2022. Bedrägerier bedöms vara ett av de mest vinstdrivande brotten som individer och grupper inom organiserade kriminella miljöer kan engagera sig i[14] och brottsvinster från bedrägerier bidrar till kriminella nätverks ekonomiska förutsättningar och kan återinvesteras i annan brottslighet. Brottsvinsterna bedöms kunna utgöra en strategisk resurs för de olika kriminella nätverk som begår brotten.

12 Regeringens uppdrag till Finansinspektionen att motverka bedrägerierna, FI2023:02625.
13 Rapport, Brottsförebyggande rådet (2023) *Bedrägerier mot privatpersoner.*
14 Rapport, Polismyndigheten (2021) *De dödliga bedrägerierna.*

4. Rättslig reglering

4.1 Företag med tillstånd från Finansinspektionen

För att driva ett företag som erbjuder finansiella tjänster krävs som huvudregel tillstånd från Finansinspektionen. Företaget som beviljats tillstånd står under Finansinspektionens tillsyn. Finansinspektionens tillsyn av företagen sker utifrån en bedömning av risken i olika verksamheter och utifrån hur stora de negativa konsekvenserna för samhället eller för konsumenterna blir om riskerna realiseras. Vilka specifika krav som ställs på verksamheten och vad Finansinspektionen utövar tillsyn över regleras i de olika så kallade rörelselagarna som är regler för specifika verksamhetstyper. Därutöver står i princip samtliga företag med tillstånd under Finansinspektionens penningtvättstillsyn i enlighet med penningtvättslagen samt i enlighet med myndighetens penningtvättsföreskrifter (FFFS 2017:11). Nedan följer en redogörelse av de verksamhetstillstånd som Finansinspektionen utfärdar och som förknippas med neobanker.

4.1.1 Bankrörelse och finansieringsrörelse

Ett företag som vill bedriva bank- eller finansieringsrörelse får sin ansökan prövad i enlighet med bestämmelserna i lagen (2004:297) om bank- och finansieringsrörelse, samt Finansinspektionens föreskrifter. En bankrörelse är en rörelse som tillhandahåller betalningsförmedling via generella betalsystem och mottagande av medel som efter uppsägning är tillgängliga för fordringsägaren inom högst 30 dagar. Med begreppet finansieringsrörelse avses en rörelse som har till ändamål att ta emot återbetalningspliktiga medel från allmänheten och lämna kredit, ställa garanti för kredit eller i finansieringssyfte förvärva fordringar eller upplåta lös egendom till nyttjande (leasing). Utöver reglerna i penningtvättslagen har banker och finansieringsrörelser även en rad skyldigheter, bland annat vad gäller kapitalkrav, kapitalbas och konsumentskydd.

4.1.2 Betaltjänster

Företag som tillhandahåller betaltjänster ska som huvudregel ha tillstånd för det i enlighet med lagen (2010:751) om betaltjänster (LBT)). I 1 kap. 2 § LBT listas de åtta olika betaltjänster ett finansiellt företag kan ha tillstånd för att tillhandahålla. Ett företag kan tillhandahålla flera betaltjänster samtidigt, men behöver ansöka om tillstånd för samtliga. I likhet med banker och kreditmarknadsbolag har betalningsinstitut en rad skyldigheter bland annat vad gäller kapitalkrav, kapitalbas och konsumentskydd att uppfylla.

Som nämnts finns det totalt åtta olika betaltjänster som finansiella företag kan ansöka om tillstånd för. Med utgångspunkt i definitionen av neobanker listas här de betaltjänster som bedöms vara relevanta för riskbedömningen av neobanker. Dessa olika betaltjänster definieras i 1 kap. 2§ LBT.

- Insättning och uttag av kontanter
- Genomförande av betalningstransaktioner
- Utgivning av betalningsinstrument
- Penningöverföring

4.1.3 Elektroniska pengar

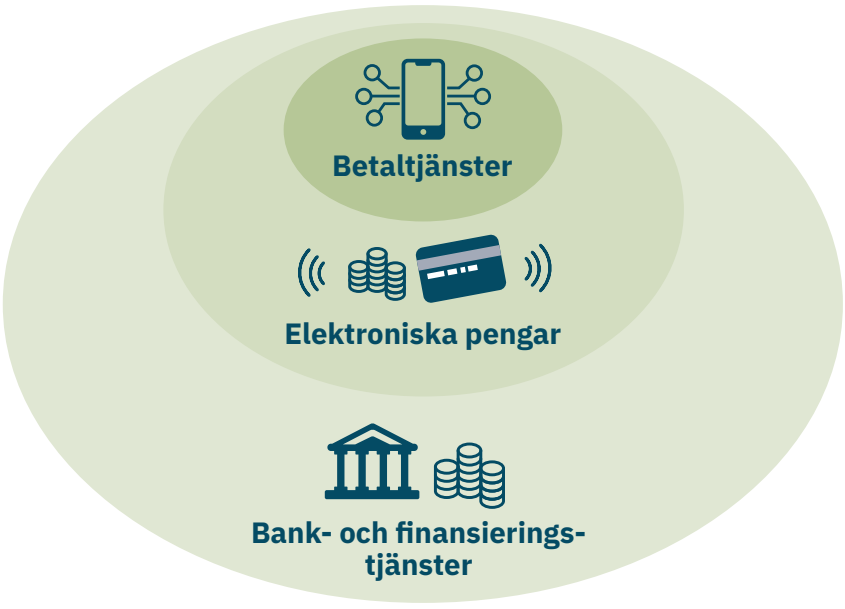
Finansiella företag som avser att ge ut elektroniska pengar behöver ha ett tillstånd från Finansinspektionen i enlighet med lagen (2011:755) om elektroniska pengar (LEP). Med elektroniska pengar avses ett elektroniska förvarat penningvärde som representerar en fordran på utgivaren, som ges i utbyte mot medel i syfte att genomföra betalningstransaktioner enligt LBT och som godtas som betalningsmedel av andra än utgivaren.

Banker, kreditmarknadsbolag, betalningsinstitut och institut för elektroniska pengar ska årligen inkomma med information till Finansinspektionen. Det är en del av de tillsynsaktiviteter som Finansinspektionen genomför för att se till att verksamhetsutövarna uppfyller de villkor som uppställs i rörelselagarna och i penningtvättslagen.

4.1.4 Konsumtion av tillstånd

Tillstånden för att driva av bank eller finansieringsrörelse, ge ut elektroniska pengar och tillhandahålla betaltjänster är i viss mån överlappande. Lagen om bank- och finansieringsrörelse konsumerar både lagen om elektroniska pengar och lagen om betaltjänster. Detta innebär att ett finansiellt företag med tillstånd att bedriva bank eller finansieringsrörelse även får ge ut elektroniska pengar och tillhandahålla betaltjänster utan att ansöka om detta. Det är dock krav på att företaget informerar Finansinspektionen om dess avsikt i god tid innan tillhandahållandet av den nya tjänsten inleds. Lagen om elektroniska pengar konsumerar i sin tur lagen om betaltjänster, vilket medför att ett företag med tillstånd att ge ut elektroniska pengar även får tillhandahålla betaltjänster givet att det informerar Finansinspektionen innan påbörjandet. Ett företag med tillstånd att tillhandahålla betaltjänster kan dock inte driva bank eller finansieringsrörelse eller ge ut elektroniska pengar.

Figur 2. Visualisering av konsumtion av tillstånd.



4.2 Företag med tillstånd från utländska tillsynsmyndigheter inom EES

Vissa finansiella företag med säte i andra länder inom EES har möjlighet att bedriva verksamhet på den svenska marknaden. Detta gäller för bland annat banker, e-pengainstitut och betalningsinstitut. Ett grundläggande krav är att företaget har ett verksamhetstillstånd utfärdat av den behöriga myndigheten i landet i vilket företaget har sitt säte. Företaget kan sedan underrätta hemlandsmyndigheten om avsikten att tillhandahålla tjänster i Sverige. Utländska företag kan bedriva verksamhet i Sverige antingen genom att erbjuda sina tjänster genom så kallad direktpassportering där de riktar sig mot den svenska marknaden, eller genom att etablera en filial i Sverige. För e-pengainstitut och betalningsinstitut finns också möjligheten att anlita ombud i Sverige. Finansinspektionen underrättas av den utländska tillsynsmyndigheten. Om ansökan avser ett e-pengainstitut eller ett betalningsinstitut som vill anlita ombud eller etablera en filial ska Finansinspektionen informera om alla rimliga skäl till farhågor i samband med det avsedda anlitandet av ett ombud eller etablerandet av en filial, när det gäller penningtvätt eller finansiering av terrorism. Beslutet om godkännande av verksamheten i Sverige fattas av den utländska behöriga myndigheten, vilken också har det primära ansvaret för tillsynen över företagets arbete mot penningtvätt och finansiering av terrorism om verksamheten sker genom direktpassportering eller genom anlitande av ombud. Sker verksamheten genom filial i Sverige har Finansinspektionen tillsyn över filialens arbete mot penningtvätt och finansiering av terrorism.

4.3 Penningtvättsregelverket och Finansinspektionens penningtvättstillsyn

En övervägande majoritet av de företag som har tillstånd eller registrering hos Finansinspektionen, inbegripen bank, e-pengainstitut samt betalningsinstitut behöver följa penningtvättsregelverket och står under Finansinspektionens penningtvättstillsyn. De regelverk som omfattas och som dessa företag behöver följa utöver PTL är Finansinspektionens föreskrifter (FFFS 2017:11) om åtgärder mot penningtvätt och finansiering av terrorism (penningtvättsföreskrifterna), samt Europaparlamentets och rådets förordning (EU) 2015/847 av den 20 maj 2015 om uppgifter som ska åtfölja överföringar av medel och om upphävande av förordning (EG) nr 1781/2006 (WTR). De olika rättsakterna brukar gemensamt benämnas det administrativa penningtvättsregelverket.

Det administrativa penningtvättsregelverket är ett riskbaserat regelverk vilket innebär krav på att de som behöver följa regelverket själva har kunskaper om riskerna för penningtvätt och finansiering av terrorism. Regelverket ställer vidare krav på att verksamhetsutövaren ska kunna motverka dessa risker i sin verksamhet genom att vidta riskbaserade åtgärder för att motverka att verksamheten utnyttjas för penningtvätt och finansiering av terrorism. Vilka åtgärder som behöver vidtas beror på vilka specifika risker som verksamheten är utsatt för med utgångspunkt i att de största resurserna ska läggas inom den del av verksamheten där riskerna bedöms vara som allvarligast.

Utöver ett riskbaserat förhållningssätt innehåller det administrativa penningtvättsregelverket en rad olika handlingsdirigerande krav på verksamhetsutövarna. Exempelvis ställs krav på att upprätta en allmän riskbedömning, upprätta rutiner och riktlinjer för bland annat kundkännedom, genomföra övervakning och rapportering, genomföra riskbedömning av kunder som ska utgå från den allmänna riskbedömningen samt krav på att vidta kundkännedomsåtgärder.

Regelverket uppställer även krav på att verksamhetsutövaren löpande kontrollerar kunder och deras transaktioner. En verksamhetsutövare får inte etablera en affärsförbindelse med en kund om det finns misstanke om att tjänsterna kommer att användas för penningtvätt eller finansiering av terrorism. En transaktion får inte genomföras om det kan misstänkas att den utgör ett led i penningtvätt eller finansiering av terrorism, eller om det inte finns tillräcklig kännedom om kunden och saknas möjlighet att övervaka och bedöma kundens aktiviteter. Misstänkta transaktioner och aktiviteter ska alltid rapporteras till Finanspolisen.

Verksamhetsutövare som står under Finansinspektionens penningtvättstillsyn är skyldiga att följa det administrativa penningtvättsregelverket och att tillåta att inspektionen granskar att det följs. Finansinspektionen har möjlighet att genomföra ett antal olika tillsynsåtgärder för att kontrollera efterlevnaden av regelverket. Vid konstaterade brister är det ytterst de olika rörelselagarna som bestämmer vilken typ av ingripandemöjligheter som inspektionen har. Några av de vanligt förekommande åtgärder som Finansinspektionen kan vidta är föreläggande om att vidta rättelse, sanktionsavgift och ytterst – vid särskilt allvarliga överträdelser – att återkalla tillståndet eller registreringen.

4.4 EBA:s riktlinjer

Kreditinstitut och finansiella institut träffas även av de riktlinjer för användning av lösningar för etablering av affärsförbindelser med nya kunder på distans[15] som den europeiska bankmyndigheten (EBA) publicerat. Riktlinjerna innehåller bland annat åtgärder som företagen ska vidta i samband med att de antar eller ser över lösningar för etablering av affärsförbindelser med nya kunder på distans. Exempelvis bör företagen införa och upprätthålla riskbaserade policyer och rutiner för kundkännedom i situationer när kunder etableras på distans. Dessa bör innehålla b.la. de situationer när lösningen för etablering av affärsförbindelser med nya kunder på distans kan användas, med hänsyn till de riskfaktorer som har identifierats och bedömts i b.la den allmänna riskbedömningen. Även uppgifter om vilka kontroller företaget gör för att säkerställa att den första transaktionen med en ny kund inte genomförts förrän alla inledande kundkännedomsåtgärder har vidtagits bör framgå.

Ska ett företag införa en ny lösning för distansetablering av kunder bör företaget göra en bedömning av b.la. hur lösningen kommer att påverka risken för penningtvätt eller finansiering av terrorism samt göra tester för att bedöma risker för bedrägerier och identitetsmissbruk. Även företagets riskreducerande åtgärder bör bedömas.

15 EBA/GL/2022/15 Riktlinjer för användning av lösningar för etablering av affärsförbindelser med nya kunder på distans i enlighet med artikel 13.1 i direktiv (EU) 2015/849.

4.5 Rapportering till Finanspolisen

En viktig skyldighet för dessa neobanker, med tillstånd i Sverige, är att utan dröjsmål rapportera misstänkta fall av penningtvätt eller finansiering av terrorism i sin verksamhet till Finanspolisen, som är Sveriges FIU (Financial Intelligence Unit). De svenska verksamhetsutövare som i denna rapport kategoriserats som neobanker stod 2023 för strax under 7 procent av totala antalet misstankerapporter till Finanspolisen[16]. Av de 30 neobankerna hade 11 banktillstånd och de stod för 77 procent av misstankerapporterna från neobankerna. Vissa neobanker inkom med få eller inga rapporter. Några verksamhetsutövare förekommer i betydligt högre grad i andras misstankerapporter jämfört med vad de själva rapporterar. Neobanker, precis som andra finansiella institutioner, har en rapporteringsplikt endast i de länder där de är registrerade. Inom EU kan neobanker ofta agera fritt inom den gemensamma marknaden för varor och tjänster. Detta innebär att neobanker ska rapportera misstänkta fall av penningtvätt eller finansiering av terrorism till den FIU där neobanken är registrerad. Om personer eller företag som förekommer i rapporter är kopplade till Sverige, ska den aktuella FIU i det landet vidarebefordra informationen till Finanspolisen. Det omvända scenariot gäller om en utländsk medborgare eller ett företag som är kund hos en neobank registrerad i Sverige förekommer i en rapport.

16 För jämförande statistik se Finanspolisens årsrapport 2023. Som referens till 7 procent så är det något mindre än vad spelbranschen rapporterar (9 procent) och en tiondel av inrapporteringen från samtliga banker (70 procent).

5. Risk- och konsekvensanalys

5.1 Definitioner av hot, sårbarhet och konsekvens

Enligt FATF kan en risk ses som en funktion av tre faktorer: hot, sårbarhet och konsekvens. En riskbedömning för penningtvätt och finansiering av terrorism är en produkt eller process baserad på en metod som beslutas av de berörda parterna. Följande definitioner bygger på FATF:s begreppsförklaringar.

Begreppet hot syftar på en person, grupp, eller verksamhet som kan skada till exempel staten, samhället eller ekonomin. Hotet kan avse kriminella aktörer och deras medhjälpare samt tillgångar och verksamheter. Hot fungerar ofta som en viktig utgångspunkt för att utveckla en förståelse för risken för penningtvätt och finansiering av terrorism. För att kunna göra riskbedömningen är det därför viktigt att ha kännedom om den övergripande kedjan. För penningtvätt innebär det att det är nödvändigt med en förståelse dels för de brott som genererar brottsvinsterna, dels själva processen med att tvätta brottsvinsterna. För terrorfinansiering behövs en förståelse både för medlens ursprung och för hur de används för att finansiera terrorism.

Begreppet sårbarhet syftar på de omständigheter som kan utnyttjas av den organisation eller de individer som utgör ett hot eller som kan stödja eller underlätta deras verksamhet. Sårbarhet är i detta sammanhang de faktorer som utgör svaga punkter i olika system för bekämpning eller kontroll av penningtvätt och finansiering av terrorism. Det kan också röra sig om egenskaper hos ett visst land, en viss bransch, finansiell produkt eller typ av tjänst som gör den intressant för personer som vill tvätta pengar eller finansiera terrorism.

Begreppet konsekvens syftar på den effekt eller skada som penningtvätt och finansiering av terrorism kan orsaka. Detta inbegriper den bakomliggande brottslighetens eller terrorismens påverkan på finansiella system och institut, liksom på ekonomin och samhället i stort. Penningtvätt och finansiering av terrorism medför konsekvenser som kan påverka befolkningen, särskilda grupper, företagsklimatet, nationella och internationella intressen samt finanssektorns rykte och attraktionskraft i ett land på både kort och lång sikt. En riskbedömning bör alltså inkludera en uppskattning av hot, sårbarheter och konsekvenser.

Eftersom det är svårt att avgöra eller uppskatta konsekvenserna av penningtvätt och finansiering av terrorism är det allmänt accepterat att en sådan analys inte nödvändigtvis måste gå på djupet, och att länder i stället kan välja att fokusera på att skaffa sig en helhetsbild av olika hot och sårbarheter. Det viktiga i riskbedömningen är att ha en metod för att bedöma vilka risker som är större än andra, vilket i sin tur gör det lättare att avgöra vilka åtgärder som behövs mest.

5.2 Utgångspunkter för bedömningar

Neobank som institution innebär flera sårbarheter och hot som sammantaget medför risk för att neobanker kan komma att utnyttjas för penningtvätt och finansiering av terrorism. I detta kapitel bedöms neobankers exponering emot dessa risker gemensamt utifrån både penningtvätt och finansiering av terrorism. Detta görs enligt följande utgångspunkter:

- Hot riktas mot sektorn av aktörer som vill utnyttja neobanker för penningtvätt och finansiering av terrorism, och bedöms enligt skalan 1–4, där 4 är den högsta nivån.
- Sårbarhet är begränsningar i sektorns förmåga att förhindra penningtvätt och finansiering av terrorism på en aggregerad nivå, och bedöms också enligt skalan 1–4, där 4 är den högsta nivån.

Hot och sårbarhet avgör sammantaget den övergripande risknivån för penningtvätt och terrorfinansiering genom neobanker. Numeriskt anges nivån som ett genomsnitt av dessa två faktorer. Först redovisas en riskanalys baserat på bedömningar av förekommande sårbarheter och hot för neobanker, därefter analyseras de konsekvenser som penningtvätt och finansiering av terrorism genom neobanker kan ge upphov till i samhället.

Dessa bedömningar har gjorts utifrån inrapporterade data till Finanspolisen respektive Finansinspektionen, samt information från Ekobrottsmyndigheten och Skatteverket. Vid tiden för publiceringen av riskanalysen har Finansinspektionens temaundersökning avseende neobankers efterlevnad av penningtvättsregelverket[17] inte avslutats, varför bedömningarna främst har baserats på tidigare erfarenheter från tillsyn av institut som likt neobanker drivs av teknologisk utveckling och som bedöms vara förenade med liknande risker. Vidare har Finansinspektionen kunnat göra vissa uppskattningar av riskerna ur ett sektorsövergripande perspektiv utifrån inrapporterade data och övrig myndighetsinformation.

5.3 Hot- och riskbedömning för banksektorn från NRA 2020/2021

I den nationella riskanalysen för 2020/2021 behandlades den finansiella sektorn och en del av den är bank- och finansieringsrörelsen. Främst behandlades affärsbanker, det vill säga. aktiebolag som har fått tillstånd av Finansinspektionen att bedriva inlåningsverksamhet. Banksektorn är den sektor där penningtvätt och finansiering av terrorism kan få störst konsekvenser på ett nationellt plan. De traditionella bankerna har vidtagit långtgående åtgärder för att minska riskerna, men samtidigt är hotnivån hög då nästan alla transaktioner berör sektorn i något skede.

Hotet mot bank- eller finansieringsrörelse bedömdes vara högt (4) och för betalningsinstitut och e-pengainstitut bedömdes det vara betydande (3). Sårbarheten för bank- eller finansieringsrörelse bedömdes vara medel (2) och för betalningsinstitut och e-pengainstitut bedömdes den vara betydande (3). Risken i banksektorn bedömdes därför vara betydande (3). För sektorerna betalningsinstitut och e-pengainstitut klassades risken för penningtvätt och finansiering av terrorism som betydande (3). Neobanker finns både som banker, med banktillstånd, och som betalningsinstitut och e-pengainstitut, varför riskbedömningen tar sin utgångspunkt i riskanalysen av dessa sektorer.

17 Finansinspektionens temaundersökning av tre neobanker inleddes i november 2023.

5.4 Hot kopplade till neobanker

5.4.1 Högriskkunder

De traditionella bankerna har vidtagit långtgående åtgärder för att minska riskerna för penningtvätt och finansiering av terrorism, exempelvis genom att bygga ut monitoreringssystem och neka högriskkunder att bli eller fortsätta vara kunder hos dem. Enligt flera myndigheter har det omfattande arbetet mot penningtvätt och finansiering av terrorism sannolikt lett till att högriskkunder söker sig till andra aktörer eftersom behovet av transaktioner i penningtvättssyfte kvarstår. Neobanker bedöms vara attraktiva för kriminella aktörer som är i behov av att tvätta pengar, bland annat på grund av snabbheten i transaktioner, att det är relativt lätt att bli kund (både i eget namn och genom bulvaner) samt möjligheten att dölja verkliga avsändare och mottagare.

Det finns flera exempel på kriminella aktörer som efter att ha nekats att bli kund eller avslutats som kunder hos traditionella banker därefter har öppnat konton i neobanker. Det förekommer även att kriminella aktörer har många konton i flera olika neobanker. Detta görs både i eget namn och i bulvaners namn. Den sårbarhet som främst utnyttjas är möjligheten att kringgå den verifieringssprocess som görs av kundens uppgifter och därigenom dölja den verklige kontohavaren.

5.4.2 Företag som brottsverktyg

Företag som brottsverktyg har uppmärksammats i flera utredningar och problemet med målvakter är idag stort.[18] Många av riskerna gällande företagstransaktioner är desamma för storbankerna och neobankerna. Det är inte ovanligt att företag genomför stora transaktioner, men neobanker ger som tidigare nämnts möjlighet till anonymiserade transaktioner genom lägre grad av kontroll. Det finns därför en risk att företag som används i penningtvätt och finansiering av terrorism kommer använda konton i neobanker istället för i traditionella banker, framför allt på grund av enkelheten och snabbheten i transaktioner och att det kan vara lättare att dölja vem som verkligen företräder företaget och hanterar kontot. I Ekobrottsmyndighetens förundersökningar kan redan idag ses att företag använda i brottslig verksamhet använder konton i neobanker.

Ett verkligt exempel är ett svenskt aktiebolag där styrelsen inför en konkurs byts ut till personer som är målvakter. Därefter försätts företaget i konkurs men företaget fortsätter dock att handla med fordon i utlandet och får betalningar för dessa insatta på ett neobankskonto. Företaget har även haft konto i en annan neobank där miljonbelopp har gått in och sedan förts vidare. Ett annat verkligt exempel är där brottsvinster från bedrägerier förs från svenska företagskonton i traditionella banker till utländska företagskonton och därifrån vidare till neobankskonton där gärningspersonerna kan tillgodogöra sig dem genom till exempel betalkort. Andra exempel är där brottsvinster från skattebrott tvättas genom transaktioner till neobankskonton och vidare till andra konton eller till olika betalkort.

Finanspolisen bedömer att mörkertalet i att upptäcka, åtgärda och rapportera företag som används för att tvätta pengar är stort och att detta utgör en allvarlig sårbarhet i samhällets försvar mot penningtvätt.[19] Att information om misstänkta transaktioner inte kommer till Finanspolisens kännedom ökar detta mörkertal då kartläggningar av penningtvätt försvåras. Om företag som utnyttjas i brottslig verksamhet i större utsträckning använder neobanker riskerar detta mörkertal att öka ytterligare.

18 SOU 2023:34 Bolag och brott – några åtgärder mot oseriösa företag.
19 Rapport, Finanspolisen (2022) *Finanspolisens årsrapport 2022*.

5.4.3 Transaktioner till högriskländer

Många neobanker agerar på en världsmarknad vilket innebär att de också kan vara attraktiva för finansiering av terrorism, detta genom möjligheten att genomföra transaktioner till högriskländer som traditionella banker inte utför transaktioner till. Grupper och personer som finansierar terrorism strävar också efter anonymitet och så liten spårbarhet som möjligt, vilket riskerar att göra neobanker attraktiva för finansiering av terrorism.

5.5 Sårbarheter hos neobanker

5.5.1 Generellt om neobankers sårbarheter

För brottslig verksamhet som genererar brottsvinster i form av pengar behövs någon form av penningtvätt för att dölja brottsvinsternas ursprung, försvåra spårningen av dem och slutligen integrera dem tillbaka in i det ekonomiska systemet alternativt återinvestera dem i brottslig verksamhet. Kontanter är fortfarande ett vanligt inslag i brottslig verksamhet, exempelvis i samband med betalning av narkotika eller avlöning av svart arbetskraft, men användandet av digitala betalningsmedel ökar som en följd av den generellt tilltagande digitaliseringen i samhället.

Det innebär att neobanker riskerar att bli ett vanligare verktyg i brottslig verksamhet framöver, framför allt genom enkelheten och hastigheten i digitala transaktioner samt möjligheten till anonymitet som kan göra det lättare för kriminella att flytta och dölja brottsvinster. En ökad möjlighet att använda finansiella tjänster digitalt utan ett fysiskt möte, med helt digitala verifieringsprocesser, möjliggör en högre grad av anonymisering och öppnar bland annat upp för risken för kontomålvakter.

I den nationella riskanalysen för 2020/2021 konstateras att användning av digitala bank- och penningöverföringstjänster underlättar insamling och överföring av pengar. Enkelhet, hastighet och större anonymitet är några av de inbyggda sårbarheter som gör att neobanker också tilltalar personer med avsikt att genomföra transaktioner i terrorfinansieringssyfte. Detta är också något som Ekobrottsmyndigheten observerat då neobanker ofta utgör första steget i en penningtvättsprocess.

Pengarnas ursprung spelar inte någon roll ur ett straffrättsligt perspektiv vad gäller terrorfinansiering, men grupper och personer som finansierar terrorism strävar ändå efter anonymitet och så lite spårbarhet som möjligt. På så sätt är merparten av de sårbarheter som beskrivits avseende penningtvätt även relevanta för finansiering av terrorism. Särskild vikt spelar möjligheten att kunna transferera pengar till högriskländer snabbt med bedömd lägre grad av kontroll än i en traditionell bank. Minskad spårbarhet gör att brotten blir svårare att både upptäcka och utreda. Det är inte ovanligt att en neobank är registrerad i ett land, men erbjuder sina tjänster till i vissa fall en världsmarknad, vilket försvårar rapporteringen av misstänkta transaktioner och möjligheten för brottsbekämpande myndigheter att ha ett nära samarbete med verksamhetsutövaren.

5.5.2 Många olika parter

Många neobanker som är verksamma på den svenska marknaden är utländska finansiella institut som har tillstånd i andra länder. Det innebär att personer i Sverige kan vara kunder i neobanker registrerade i andra länder. Om dessa inte har en filial i Sverige har Finansinspektionen ingen tillsyn över dem och de är undantagna rapporteringsplikten som ska göras till Finansinspektionen. Det innebär att kvaliteten på tillsynen av dessa neobanker är beroende av utländska tillsynsmyndigheter. Utländska neobanker kan också ha bristande kännedom om enskilda kunders finansiella beteenden på den svenska marknaden jämfört med den marknaden man vanligtvis verkar på. Det kan ha som konsekvens att högriskkunder kan söka sig till

neobanker som inte har kännedom om svenska förhållanden och vad som anses vara riskbeteende i en svensk kontext. Tillgång till och förståelse av svenska register för att utföra kundkännedom kan också vara bristande hos utländska neobanker.

Det är tidskrävande att begära ut information och få svar på begäran från andra länder i samband med förundersökningar och skatteutredningar. Ett svar från ett land kan exempelvis ge information om att överföringar skett till konton i andra länder, varför ny begäran om internationell rättshjälp till andra länder ofta är nödvändig. Det finns exempel från förundersökningar och skatteutredningar där förfrågningar har gjorts i flera led för att kunna spåra transaktioner. Att externa parter kan hantera olika funktioner som erbjuds av neobanker, exempelvis utgivning av betalkort, kan också försvåra möjligheten att spåra transaktioner. Att ansvaret för olika funktioner fördelas på olika aktörer gör också att transaktioner därför kan bli svårare att spåra. Detta har även observerats av Ekobrottsmyndigheten som ofta får förfrågningar från andra länder gällande svenska medborgare som är kontohavare i neobanker och förekommer i dessa länders förundersökningar.

Ett verkligt exempel som belyser dessa svårigheter berör en förfrågan avseende en person som är kund i en neobank i ett annat land än Sverige. I det fallet svarar den aktuella neobanken att kunden är ett e-pengainstitut och att den brottsutredande myndigheten behöver kontakta dem. När kontakt tas med e-pengainstitutet, i ytterligare ett annat land, blir svaret att e-pengainstitutet har en underleverantör och att den efterfrågade slutkunden är kund hos en ytterligare verksamhetsutövare i ett tredje land.

Bankärenden som genomförs digitalt och i regel är obevakade av bankpersonal bedöms utgöra en förutsättning för flera typer av bedrägerier. Det alltmer fragmenterade förloppet i transaktionerna, där förloppet är uppdelat med ett flertal olika aktörer inblandade som bara har kontroll över det steg i kedjan de själva hanterar och att ingen aktör har hela bilden, försvårar identifierandet av bedrägliga transaktioner.

5.5.3 Gränsöverskridande verksamhet – olika kontrollorgan eller bristande kontroll

Neobanker ska, som tidigare beskrivits, rapportera misstänkta transaktioner till det landets FIU (motsvarande den svenska Finanspolisen) som de är registrerade i. Det innebär till exempel att en misstänkt transaktion från ett konto i en neobank som är registrerad i ett annat land än Sverige, men som innehas av en svensk medborgare, ska rapporteras till det aktuella landets FIU. Detsamma gäller för utländska medborgare som är kunder i svenska neobanker.

Utländska aktörer som verkar i Sverige har en begränsad uppgiftsskyldighet som i princip är helt beroende av egenrapportering. Skatteverkets beskattningsverksamhet har begränsade möjligheter att göra generella inhämtningar från utländska aktörer. Brottsutredande myndigheter och Skatteverkets beskattningsverksamhet kan därtill ha problem att få svar på förfrågningar från vissa jurisdiktioner. Att många olika jurisdiktioner är inblandade kan också leda till att kontrolluppgifter inte lämnas till Skatteverket avseende transaktioner till och från utlandet, eller att information rapporterad till den FIU där neobanken är registrerad inte förs vidare till svenska Finanspolisen. Brister i rapportering innebär att informationen inte kommer till svenska myndigheters kännedom.

Kontrolluppgifter avseende utlandsbetalningar till och från Sverige är en del av Skatteverkets kontrollmaterial som ökar möjligheterna att spåra pengar och att hitta oredovisade inkomster. Det finns indikationer på att det finns brister i kontrolluppgifterna avseende överföringar från svenska banker och finansiella institutioner till utländska neobanker. Bland annat finns det exempel där en svensk neobank lämnat kontrolluppgifter avseende utlandsbetalningar, på totalt sett betydande belopp, till

en neobank i ett annat EU-land, utan att de slutliga mottagarna av betalningarna har angetts. I sådana fall saknas transparens vilket innebär att det finns stor risk för att det inte uppmärksammas att det är pengar som tvättats genom neobankerna och att mottagarna är kopplade till kriminell verksamhet. Det finns även indikationer på att finansiella institut underrapporterar utlandskontrolluppgifter till Skatteverket.

5.5.4 Verifiering av kunder och kundkännedomsprocessen

I den nationella riskanalysen för 2020/2021 konstaterades att det finansiella systemet är beroende av hög tilltro till grundidentifiering av en persons identitet. Det innebär att förekomsten av målvakter och att andras identiteter utnyttjas är särskilt problematiskt för den svenska penningtvättsregimen. Neobanker ska genomföra kundkännedomsåtgärder på sina kunder. Kundkännedomsprocesserna och kraven på dokumentation kan skilja sig åt mellan olika neobanker, men i takt med att processen att skapa konto och bli kund förenklas och blir snabbare kan kvalitén i kundkännedomen också påverkas.

En påtaglig sårbarhet i neobankers verifierings- och kundkännedomsprocesser är att identifieringen inte sker i samband med ett fysiskt möte. En verifieringsprocess som bygger på digitala möten består istället ofta av att kunden skickar in bestyrkta kopior på en id-handling och ett foto på sig själv. Möjligheterna att utnyttja andras identitetshandlingar är dock många. Att förfalska id-handlingar är relativt enkelt, och det finns även nätbaserade tjänster som öppet annonserar att de mot betalning hjälper kunder att kringgå verifieringsprocessen.

Även om e-legitimationer används finns det exempel på att e-legitimationer har kringgåtts i samband med verifieringsprocesser. En särskilt viktig aspekt, och en allvarlig sårbarhet som öppnar upp för ett flertal möjliga bedrägerier, är inloggning och digitala signeringar av uppdrag (godkännanden av transaktioner). En annan sårbarhet, som utnyttjas i bedrägerier, är möjligheten att från banken utfärda en ny mobil e-legitimation till en ny enhet som sedan kan användas i samband med inloggning och signering av uppdrag.[20] Ett konkret exempel är en dom från Allmänna reklamationsnämnden som beskriver hur en gärningsperson i ett bedrägeri fick en annan person att installera en e-legitimation i sitt namn på gärningspersonens enhet där denne sedan använde e-legitimationen för att öppna ett konto i en neobank och sedan föra över pengar dit från personens konto.

Inom EU finns eIDAS[21] men det adresserar inte de grundläggande sårbarheterna hos e-legitimationer: att säkerställa grundidentiteten på personen som har fått en e-legitimation utfärdad och att säkerställa att den som använder den verkligen är den som e-legitimationen utfärdats till.

5.5.5 Frågan om kundrelationer och ansvarsfördelning

Den typ av samarbetsavtal verksamhetsutövare emellan genom white labeling-upplägg, som möjliggör att vissa verksamhetsutövare kan erbjuda produkter och tjänster som annars faller utanför verksamhetsutövarens egna tillstånd (se avsnitt 2.5), leder inte sällan till frågor om bland annat riskägande och ansvarsfördelning i kundkännedomsprocesser och transaktionsmonitoreringen. Det leder i sin tur till oklara gränsdragningar för vem som äger kundrelationen och därmed står för risken för bland annat penningtvätt eller finansiering av terrorism. Samarbetsavtal av detta slag är idag inte specifikt reglerat enligt svensk lag, varför en gränsdragningsproblematik avseende kundrelationer och ansvarsfördelning kan uppstå.

20 Rapport, Brottsförebyggande rådet (2023) *Bedrägerier mot privatpersoner*.

21 eIDAS: Regulation on electronic identification and trust services, Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

5.5.6 Brister i transparens

I den nationella riskanalysen för 2020/2021 gjordes observationen att teknikutvecklingen skapar nya utmaningar. Nya betallösningar och deras konstruktion gör att det skapas möjligheter att dölja transaktioner och tillgångar, vilket försvårar upptäckt och kontroll. Det gör också transaktioner snabbare.

Vissa neobanker använder sig av så kallade virtuella bankkonton. Dessa kan liknas vid klientmedelskonton, det vill säga neobanken har ett konto hos en bank med tillgodohavanden för flera av sina kunder. Varje kunds tillgodohavanden hålls i ordning av neobanken via olika liggare. Exempelvis: neobanken ser ut som en traditionell bank gentemot slutkunden, men när kunden X sätter in pengar på sitt konto neobanken, som vanligtvis är kopplat till ett betalkort, finns pengarna egentligen på bank B på ett konto där innehavaren är neobanken (på samma konto ligger även innehav för andra kunder). Denna typ av konton försvårar spårbarheten av medel för bankerna samt deras monitorering. Dessutom kan det leda till felaktiga motpartsuppgifter i penningtvättsregistret vid misstankerapportering.

Lag (2020:272) om konto- och värdefackssystem omfattar kreditinstitut, utländska kreditinstitut med filial i Sverige, värdepappersbolag samt utländska värdepappersbolag med filial i Sverige. Med kreditinstitut avses bank och kreditmarknadsföretag, vilka har tillstånd för att bland annat tillhandahålla inlåningskonton. Således omfattas de flesta svenska neobanker inte av lagen och inkluderas inte i Mekanismen[22]. Det är en teknisk plattform framtagen av Skatteverket för att brottsutredande myndigheter samt Skatteverkets beskattningsverksamhet och Kronofogdemyndigheten snabbt kan få tillgång till uppgifter om vilka konton en person eller företag innehar eller har fullmakt för hos ovan nämnda institut. Mekanismen gör det också möjligt att fastställa vem, vilka personer eller vilket/vilka företag som innehar ett visst bankkonto eller värdefack. I dagsläget är omkring 120 institut anslutna till Mekanismen. Att neobanker som inte är bank- och kreditmarknadsföretag inte inkluderas innebär att en sökning i Mekanismen på personer, ett företags organisationsnummer eller personnummer på företrädare inte ger träff på konton hos många svenska neobanker. Effekten och risken är att sökta tillgångar inte upptäcks och förblir dolda för myndigheter.

Verksamhetsutövare med svenskt banktillstånd ingår i Mekanismen vilket gör att myndigheter vid sökning kan hitta specifika kontohavare hos verksamhetsutövaren. Däremot ingår inte verksamhetsutövare utan svenskt banktillstånd, så som till exempel utländska neobanker eller svenska neobanker utan tillstånd att tillhandahålla inlåningskonton, i Mekanismen. Om en neobank utan svenskt banktillstånd innehar klientmedelskonton hos en verksamhetsutövare med banktillstånd kommer enbart information om neobankens klientmedelskonto att kunna hittas; information om vilka kunder som har ett innehav hos neobanken i fråga kommer däremot inte att kunna sökas fram. Kunders innehav på neobankers klientmedelskonton kan bland annat avse medel som i ett senare led ska tillgängliggöras på betalkort, företagskonto eller sparkonto hos någon annan verksamhetsutövare med vilken neobanken har ett samarbetsavtal.

Ett exempel: Person A har ett konto hos en svensk bank med banktillstånd och ett konto hos en neobank som inte har svenskt banktillstånd. Vid sökning på personen i Mekanismen kommer bara det första kontot att hittas, inte det andra. Detta beror på att neobanken där person A har ett konto i sin tur har ett klientmedelskonto i den svenska banken och den svenska banken saknar uppgifter om vilka kunder som

22 Konto- och värdefackssystem (Mekanismen), mer information om Mekanismen finns på Skatteverkets webbplats.

har vilka medel på klientmedelskontot. Person A.s innehav i neobanken befinner sig således ett steg bortom de konton Mekanismen kan söka fram.

Varje medlemsstat i EU ska ha ett kontor för återtagande av brottsutbyte för att snabbt kunna spåra brottsvinster utanför det egna landets landsgränser utan att behöva begära rättslig hjälp. ARO (Asset Recovery Office) har tillgång till Mekanismen, vilket förenklar och snabbar på möjligheten att få kännedom om var eventuella brottsvinster finns inom EU. Att inte alla neobanker är anslutna till Mekanismen försvårar därför att snabbt kunna spåra brottsvinster.

För företag med bankgiro via neobanker finns brister i hur data och kontouppgifter registrerats och hanteras. Neobanken uppges ofta som primär organisation knutet till företagskonton eller bankgironummer istället för den faktiska innehavaren. Hos Bankgirots söktjänst för bankgironummer framgår detta då till exempel en sökning på ett företags organisationsnummer inte ger träff. Problematiken har flera följdeffekter såsom felaktigheter i data hos banker och i penningtvättregistret, vilket påverkar möjligheten till monitorering av misstänkta transaktioner.

Det finns en sårbarhet i informationsdelningen rörande transaktioner mellan olika verksamhetsutövare i transaktionskedjan, vilket tas upp i Finanspolisen rapport om neobanker.[23]

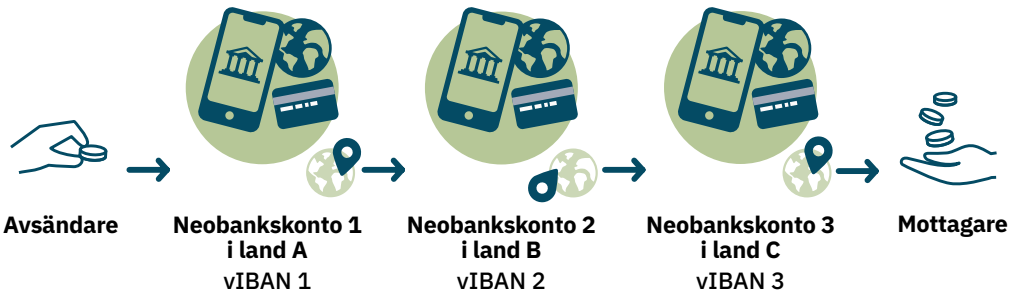
Det gäller inte minst vid insättningar till ett konto hos neobanker där såväl avsändande respektive mottagande bank samt neobanken ifråga har begränsad information om mottagare och avsändare. Vid en kortinsättning sker transaktionen vanligen genom ett gränssnitt via neobanken. När pengarna går till en neobanks klientmedelskonto hos en mottagande bank ser avsändande bank inte vem som är kontoinnehavare hos neobanken. Neobanken kan i sin tur ha begränsad information om vem betalkortet tillhör och således vem avsändaren är. Flera neobanker har i tillägg möjlighet för andra personer än kontoägaren att göra betalningar med kort till en annan persons konto.

Europol har i sin hotbedömning av finansiell och ekonomisk brottslighet för 2023[24] identifierat att vIBAN missbrukas av kriminella då de möjliggör snabba internationella betalningar som maskerar identiteten på huvudkontot, utfärdaren och ursprungslandet. På grund av strukturen kring vIBAN finns det teoretiskt inte någon gräns för antalet mellanhänder mellan banken och slutkunden (figur 3). Det utnyttjas i den kriminella ekonomin för att tvätta pengar och upprätthålla en parallell ekonomi. Kriminella kan exempelvis utföra transaktioner via en stor mängd virtuella bankkonton och betalningar till olika länder. De kan på så sätt enkelt sprida sina tillgångar över många virtuella bankkonton och försvåra spårning av pengaflöden. Detta gör det svårare att upptäcka och spåra misstänkta transaktioner och medför extra steg i finansiella utredningar. Detta försvårar arbetet mot penningtvätt och för brottsbekämpande myndigheter på grund av brist på transparent information och möjligheten att dölja transaktioner.

23 Rapport, Finanspolisen (2022) *Neobanker.*

24 Rapport, Europol (2023) *The Other Side of the Coin – Analysis of Financial and Economic Crime.*

Figur 3. Olika vIBAN i en serie transaktioner.



5.6 Risk- och konsekvensanalys

Risken för penningtvätt och finansiering av terrorism bedöms som en sammanvägning av hot och sårbarheter.

I den nationella riskanalysen för 2020/2021 bedömdes hotet för penningtvätt och finansiering av terrorism i banksektorn vara högt (4). Nästan all penningtvätt berör banksektorn på något sätt och neobanker är en del av banksektorn vilket innebär att hotet för penningtvätt för neobanker bedöms vara detsamma som för banksektorn som helhet, högt (4).

Bedömningen baseras på att behovet av transaktioner i penningtvättssyfte och finansiering av terrorism kvarstår, men när högriskkunder stängs ute från traditionella banker söker de sig sannolikt till andra lösningar eftersom behovet kvarstår. De möjligheter att dölja kontohavare, avsändare och mottagare samt spåra transaktioner som identifierats gör neobanker attraktiva för högriskkunder. Dessa möjligheter gör att även hotet från företag att använda i penningtvätt ingår i bedömningen då det riskerar bli svårare att upptäcka penningtvätt och finansiering av terrorism genom företag. De många inblandade parterna gör att antalet misstänkta transaktioner som kommer till Finanspolisens kännedom riskerar minska ytterligare vilket leder till att mörkertalet ökar ännu mer, men även att Skatteverkets beskattningsverksamhet försvåras. Möjligheten att göra transaktioner till högriskländer ingår också i bedömningen.

I den nationella riskanalysen för 2020/2021 bedömdes sårbarheten hos banksektorn som helhet för penningtvätt och finansiering av terrorism vara medel (2) och för sektorerna betalningsinstitut, betaltjänstleverantör och utgivare av elektroniska pengar bedömdes den vara betydande (3).

Sårbarheten för neobanker för penningtvätt och finansiering av terrorism bedöms vara betydande (3), det vill säga den näst högsta nivån. Bedömningen baseras på att neobanker bedöms i viss mån ha större likheter med betalningsinstitut, betaltjänstleverantör och utgivare av elektroniska pengar då inte alla har banktillstånd, men också de identifierade sårbarheterna: det stora antalet inblandade parter och jurisdiktioner i samband med transaktioner, svårigheter avseende spårbarhet av transaktioner, avsaknad av fysiska möten i samband med verifikations- och Känn din kund-processen, samt möjligheterna att dölja verklig kontohavare, avsändare och mottagare.

I den nationella riskanalysen för 2020/2021 bedömdes risken för penningtvätt och finansiering av terrorism i banksektorn och för sektorerna betalningsinstitut, betaltjänstleverantör och utgivare av elektroniska pengar vara betydande (3).

Neobanker finns både som banker med banktillstånd, som betalningsinstitut och betaltjänstleverantör samt som e-pengainstitut. Risken för neobanker bedöms därför också vara betydande (3). Bedömningen baseras på de hot och sårbarheter som identifierats, framförallt hotet från högriskkunder och svårigheterna att spåra transaktioner, möjligheterna att dölja verklig kontohavare, avsändare och mottagare samt möjligheten att göra transaktioner till högrisländer. Den kan förändras över tid beroende på till exempel förändrade kundkännedomsprocesser, ändrade och mer tillförlitliga verifieringsprocesser eller förbättrat informationsutbyte, men även ett över tid ökat användande av neobanker och andra elektroniska betalningslösningar.

Banksektorn är den sektor där penningtvätt kan få störst konsekvenser på ett nationellt plan[25]. De traditionella bankerna har vidtagit långtgående åtgärder för att minska riskerna, men samtidigt är hotnivån hög då nästan all penningtvätt berör sektorn i något skede. Penningtvätt i banksektorn som helhet riskerar att påverka förtroendet för det finansiella systemet och skada Sveriges anseende internationellt. Finansiering av terrorism har samma konsekvenser men även den yttersta konsekvensen av genomförda terrordåd.

Neobanker ingår i banksektorn men de egenskaper, sårbarheter och hot som har identifierats i denna rapport (enkelhet och snabbhet i transaktioner, många parter och jurisdiktioner inblandade samt möjligheterna att dölja verkliga kontohavare, avsändare och mottagare) har delvis andra konsekvenser. Användandet av neobanker för penningtvätt och finansiering av terrorism riskerar att skada förtroendet för det finansiella systemet och neobanker som företeelse, men Sveriges anseende internationellt i lägre grad. För Sverige är en konsekvens av hot och sårbarheter mot och hos neobanker att de riskerar att försvåra upptäckt och lagföring av penningtvätt och finansiering av terrorism. Det kan leda till lägre lagföring men även försvåring av skatteutredningar vilket har som konsekvens en minskning av skatteintäkter om inte rätt beskattning kan göras.

25 Rapport, Samordningsfunktionen (2021) *Nationell riskbedömning av penningtvätt och finansiering av terrorism i Sverige 2020/2021*.

6. Rekommendationer

Kompetenshöjning

Det finns ett generellt behov att öka kunskapen om riskerna i neobanker hos svenska verksamhetsutövare och myndigheter som i sitt arbete kommer i kontakt med dessa. Kompetenshöjningen bör syfta till att öka medvetenheten om bland annat neobankers processer för kundkännedom och användandet av e-legitimation i dessa. Behovet av de kompetenshöjande insatserna bör analyseras utifrån respektive verksamhets uppdrag.

Utländska neobanker

Sverige bör verka för förbättring av informationsutbyte för svenska myndigheter om svenska kunder i utländska neobanker. Det bör även inkludera åtgärder för att förbättra spårbarheten i transaktioner och motverka brister i motpartsuppgifter.

Produkter och tjänster

Produkter och tjänster som inte kan erhållas från vissa neobanker, eftersom de faller utanför verksamhetsutövarens egna tillstånd, kan istället erbjudas genom white labeling-upplägg med samarbetsavtal med andra leverantörer, vanligtvis traditionella banker. Det bör dock göras en översyn av den svenska lagstiftningen vad gäller möjligheten att erbjuda produkter och tjänster som faller utanför det egna tillståndet i och med den gränsdragningsproblematik avseende kundrelationer och ansvarsfördelning som sådana samarbetsavtal många gånger ger upphov till.

Verifiering

Verifikationsprocesser som sker på distans bör i möjligaste mån vara utformade för att minska risken för kontomålvakter och användandet av stulna och förfalskade identiteter, exempelvis genom ökad användning av e-legitimation. Sverige bör därför verka för att e-legitimationer inom EU i så stor omfattning som möjligt ska användas vid verifiering av kunder och dess godkännande av transaktioner.

Internationellt samarbete

Ett stärkt internationellt samarbete är en grundförutsättning för att motverka penningtvätt och finansiering av terrorism via neobanker. Då det föreligger brister i delgivningen och hanteringen av misstankerapporter mellan FIUs rekommenderas Finanspolisen att vidta proaktiva åtgärder i att förbättra situationen. Genom en ökad interaktion och informationsutbyte kan Finanspolisen dessutom spela en aktiv roll i att förbättra både kvaliteten och kvantiteten i rapporteringen från neobanker.

Rapporteringsskyldigheten

Olika länder tolkar regelverken inom CRS och DAC2 olika. Det leder till otydligheter vad gäller om neobanker i andra länder omfattas av rapporteringsskyldigheten av uppgifter om finansiella konton. I dagsläget innebär detta en diskrepans mellan länder och det finns risk för att kriminella aktörer skaffar konton i neobanker registrerade i länder som gör tolkningen att neobanker inte omfattas av CRS och DAC2-rapportering, i syfte att undkomma skatt eller tvätta pengar. Sverige bör därför lyfta frågan om harmonisering av rapporteringsskyldigheten för finansiella institut inom OECD och EU.

Skatteverket

Det finns indikationer på underrapportering av utlandskontrolluppgifter till Skatteverket, men i nuläget finns det inga sanktioner kopplade till brister eller utelämnande av uppgifterna. Skatteverket bör lyfta frågan om förutsättningar finns för att påföra sanktionsavgift till ett finansiellt institut vid sent inkomna, ofullständiga eller uteblivna kontrolluppgifter (KU80/81). Uppgifterna bör även lämnas på ett av Skatteverket fastställt formulär.

Mekanismen

Svenska neobanker som inte har tillstånd att tillhandahålla inlåningskonton omfattas inte av kravet på rapportering av konton till Mekanismen. Dessa verksamhetsutövare tar emellertid emot medel från sina kunder, som hamnar på klientmedelskonton hos traditionella banker. Att innehavet tillhörande neobankernas kunder på dessa klientmedelskonton inte går att söka fram i Mekanismen försvårar möjligheten att spåra transaktioner samt hitta och återta brottsvinster. Det bör utredas om det finns förutsättningar att utöka rapporteringskravet avseende kontoinnehavare så att även neobankernas kunder med konton hos dem eller i andra banker där neobankerna har klientmedelskonton eller liknande omfattas. I samband med en sådan utredning bör även vIBAN och identifiering av virtuella bankkonton hos neobanker inkluderas.

SAMORDNINGSFUNKTIONEN MOT PENNINGTVÄTT OCH FINANSIERING AV TERRORISM