

Neobanker

En rapport om neobanker och deras risker relaterade till penningtvätt och finansiering av terrorism



PMY Rapport

Polismyndigheten, Nationella operativa avdelningen, maj 2022



Utgivare: Polismyndigheten, Nationella operativa avdelningen, Box 12256, 106 75 Stockholm
Dnr: A235.498/2022, Saknr: 423
Omslagsfoto: MostPhotos
Upplaga: Internet
Datum:2022-05-16

Innehåll

Innehåll	3
Sammanfattning	4
Inledning	5
Syfte och metod	6
1 Beskrivning av neobanker.....	7
1.1 Banker, betaltjänster och elektroniska pengar	7
1.2 Neobankernas tjänster och erbjudanden	9
1.3 Exempel på neobanker	11
2 Risker för penningtvätt och terrorfinansiering	13
2.1 Neobankernas internationella struktur	13
2.2 Falsa identiteter, identitetsstöld och målvakter	14
2.3 Insättning på konton hos neobanker	15
2.4 Den dolda ekonomin.....	17
2.5 Finansiering av terrorism	18
3 Tillvägagångssätt för penningtvätt och terrorfinansiering	19
3.1 Skiktning	19
3.2 Användning av kryptovalutor	19
3.3 Spridda tillgångar.....	20
3.4 Snabba återbetalningar av lån eller krediter.....	20
3.5 Indikatorer och tillvägagångssätt som föranlett misstankerapporter	20
3.6 Terrorfinansiering	22
4 Misstankerapporter	23
4.1 Kön och ålder.....	23
4.2 Kopplingar till annan brottslighet	24
4.3 Kopplingar till kriminella grupperingar.....	25
5 Slutsatser.....	26
6 Tänkbara åtgärder	27
6.1 Neobanker riktade mot företagskunder.....	27
6.2 Internationellt samarbete.....	27
6.3 Mekanismen.....	27
6.4 eID	28

Sammanfattning

En neobank kan enkelt beskrivas som en helt digital bank där användaren kan utföra alla sina tjänster via en mobilapp eller genom ett webbgränssnitt. Digitaliseringen av ekonomin gör att efterfrågan och utbudet av dessa banker växer, idag finns ungefär 250 sådana företag globalt. Det är sannolikt att neobanker är en växande verksamhet där kriminellas användning i penningtvättsupplägg kommer att öka framgent och följa den allmänna tekniska utvecklingen.

Betalinstitut, e-pengainstitut och en del banker benämns ofta som neobanker. Neobank är inte en juridisk term, betydelsen av ordet är ”ny bank”, där neo står för *nytt/modifierat* på latin. Utvecklingen inom området går mot att neobankerna utökar sina erbjudanden genom nya licenser, uppköp av andra bolag eller via samarbeten med andra bolag. Flera neobanker går även längre och skaffar sig en egen banklicens. De fortsätter dock att platsa in i benämningen neobanker. Flertalet neobanker har en kundbas även utanför det land där de har sin registrering. Neobanker kan erbjuda många tjänster och produkter som en traditionell bank gör, men har ofta smidigare och mer användarvänliga lösningar än vad traditionella banker har. Detta har medfört att neobanker blivit attraktiva på den finansiella marknaden, och framväxten av neobanker har ökat under senare år.

Neobanker och deras tjänster är dock också attraktiva för kriminella aktörer som utnyttjar dessa kanaler för att tvätta sina svarta pengar eller för att finansiera allvarlig och grov brottslighet, såsom finansiering av terrorism. Transaktioner via neobanker är smidiga, snabba och gränsöverskridande, samtidigt som det finns möjlighet för kriminella aktörer att utnyttja konton hos neobanker för att agera dolt samt handla med och konsumera kryptovalutor. Underrättelser vittnar om kriminella aktörer som flitiga användare av neobanker. Totalt 39 % av de personer som blivit inrapporterade av både neobanker och traditionella banker¹ förekommer i andra typer av underrättelser med kopplingar till grov och organiserad brottslighet. Till stor del rör det kriminella grupperingar i utsatta områden som är aktiva i narkotika- och våldsbrottslighet.

¹ Misstankerapporter från traditionella banker avser misstänkta personer vars transaktioner inkluderat transaktioner till och/eller från en neobank.

Inledning

Behovet av förenklade betallosningar, digitala möjligheter och skraddarsyddas tjänster blir allt större, både i Sverige men även globalt. Framväxten av så kallade Fintech-bolag har ökat under de senaste åren, där neobankers utgör en del. En onlinedatabas listar över 246 neobankers globalt varav 76 stycken i Europa.²

Neobankers är helt digitala och kan ha en gränsöverskridande verksamhet som innebär att deras kundbas breder ut sig utanför det land där de är registrerade. Neobankers erbjuder en användarvänlig upplevelse, innovativa lösningar, lägre kostnader och aktiv marknadsföring, vilket gjort att deras tjänster ökat bland allmänheten. Denna kundbas ser ut att öka under kommande år.

Neobankers och traditionella bankers erbjuder i mångt och mycket liknande tjänster och delar därför på många risker för penningtvätt och finansiering av terrorism. Samtidigt är kunskapen om och inblicken i neobankers begränsad hos brottsutredande myndigheter. Underrättelser visar på att kriminella aktörer är kunder hos neobankers och innehavare av deras betalkort. Således föreligger det en risk för att neobankers kan användas som ett led i en penningtvättskedja eller vid finansiering av terrorism.

² <https://neobanks.app/>

Syfte och metod

Syftet med denna rapport är att ge ökad förståelse samt ny och kompletterande information om neobanker genom att

- Ge en kunskapshöjande beskrivning av vad neobanker är,
- Beskriva risker för penningtvätt och finansiering av terrorism,
- Beskriva tillvägagångssätt där neobanker utnyttjas för penningtvätt och finansiering av terrorism.

Analysen bygger i huvudsak på data ur penningtvättsregistret mellan åren 2020–2021 i form av misstankerapporter från svenska neobanker och traditionella banker. Rapporterna från traditionella banker innefattar transaktioner till och från en eller flera neobanker. Vidare har kompletterande data hämtats från utländska neobankers misstankerapporter. Cirka 2 600 personer som rapporterats till Finanspolisen har utgjort underlag för analysen i denna rapport. Andra underrättelser som rör penningtvätt och terrorfinansiering via neobanker har inkluderats i analysen samt underrättelseinformation om de personer som misstankerapporterats. Dialog har även förts med andra myndigheter och företag, både svenska och utländska.

Då antalet rapporter från utländska verksamhetsutövare är få har detta medfört att analysen behövt begränsas. Neobanker riktade enbart mot företagskunder har inte analyserats inom ramarna för denna rapport. Neobanker kan ha en god förmåga att upptäcka penningtvätt och finansiering av terrorism, denna förmåga kan skilja sig åt mellan olika neobanker och ämnet diskuteras inte i denna rapport.

1 Beskrivning av neobanker

En neobank är enkelt beskrivet en digital bank där användaren kan utföra alla sina tjänster via en mobilapp eller genom ett webbgränssnitt. Neobank är inte en juridisk term, betydelsen av ordet är ”ny bank”, där neo står för *nytt/modifierat* på latin. Även om många av de finansiella tjänsterna som en neobank erbjuder är liknande de hos en traditionell bank, är neobankerna ofta mer användarvänliga och kan utmana traditionella banker på grund av bland annat lägre kostnader och användarvänliga tjänster.

Vilka tjänster som erbjuds kan variera från neobank till neobank. Oftast rör det sig om bolag som börjat med enstaka tjänster för att sedan utöka sitt produkt- och tjänsteutbud stegvis. De flesta neobanker erbjuder främst konton, kort samt krediter, ofta genom partnerskap med en traditionell bank. Andra uppskattade tjänster kan exempelvis vara sparhjälp och finansiell översikt. Neobanker kan även utöka sina erbjudanden genom nya licenser, uppköp av andra bolag eller via samarbeten med andra bolag. Flera neobanker går även längre och skaffar sig en egen banklicens, de fortsätter dock platsa in i benämningen neobanker.

1.1 Banker, betaltjänster och elektroniska pengar

Betalinstitut, e-pengainstitut och en del banker tillskrivs ofta namnet neobanker. Det är förekommande att en del neobanker går in i partnerskap med traditionella banker för att kunna erbjuda tjänster och produkter som de i annat fall inte hade kunnat erbjuda.

Bolag behöver söka tillstånd hos Finansinspektionen eller motsvarande myndighet i ett annat land, att få bedriva sin verksamhet. I följande text beskrivs de olika tillstånden som finns för en verksamhet som bedrivs i Sverige. Tillståndet visar vilken verksamhet som får bedrivas och vilka krav som ställs på tex styrning och kontroll i bolaget. För bolag som är registrerade i annat land inom EU finns det liknande tillstånd.

Tillstånd att bedriva bankrörelse

Förutsättningarna för att få driva bank- och finansieringsrörelse framgår av lagen (2004:297) om bank- och finansieringsrörelse och förordningen (2004:329) om bank- och finansieringsrörelse. I bankrörelse ingår att förmedla betalningar via generella betalsystem och att ta emot pengar på konto. I finansieringsrörelse ingår näringsverksamhet där ändamålet bland annat är att ta emot återbetalningspliktiga medel från allmänheten samt lämna

krediter. Banker och kreditmarknadsföretag får ge ut elektroniska pengar inom ramen för sitt befintliga tillstånd.³

Tillstånd att ge ut elektroniska pengar

För att få ge ut elektroniska pengar krävs ett tillstånd av Finansinspektionen enligt lagen (2011:755) om elektroniska pengar. Likt för betaltjänster är det möjligt att ansöka om att undantas från tillståndsplikt bland annat om den planerade verksamheten har sådan begränsad omfattning att genomsnittligt utestående skulder hänförliga till elektroniska pengar aldrig överstiger fem miljoner euro, och kallas då för registrerad utgivare istället för institut för elektroniska pengar. Ett institut för elektroniska pengar eller en registrerad utgivare får också tillhandahålla betaltjänster enligt lagen (2010:751) om betaltjänster.

Elektroniska pengar definieras i lagen⁴ som ett elektroniskt förvarat penningvärde som:

- representerar en fordran på utgivaren,
- ges ut i utbyte mot medel i syfte att genomföra betalningstransaktioner enligt lagen (2010:751) om betaltjänster, och
- godtas som betalningsmedel av andra än utgivaren.

Tillstånd att tillhandahålla betaltjänster

För att tillhandahålla en eller flera betaltjänster krävs tillstånd i enlighet med lagen (2010:751) om betaltjänster. Om genomsnittet av de totala betalningstransaktionerna under de senaste 12 månaderna inte överstiger ett belopp motsvarande 3 miljoner euro per månad kan man ansöka om att undantas tillståndsplikt och istället registreras som betaltjänstleverantör. Med betaltjänster avses bland annat tjänster som möjliggör insättningar och uttag av kontanter till och från ett betalkonto samt de åtgärder som krävs för förvaltning av kontot, penningöverföring och genomförande av betalningstransaktioner. Det finns åtta kategorier av tillstånd som bolagen kan ansöka om, som avgör vilka betaltjänster som kan erbjudas.⁵

³ 2 kap. 2 § första stycket först punkten Lag (2011:755) om elektroniska pengar.

⁴ Lagen (2011:755) om elektroniska pengar.

⁵ [Lagen om betaltjänster 1 kap. 2 §](#)

1.2 Neobankernas tjänster och erbjudanden

Nedan listas exempel på tjänster och erbjudanden som neobanker erbjuder.⁶ Många traditionella banker har anpassat sig efter konkurrensen från neobanker genom att utveckla sina egna tjänster och erbjudanden. Listan nedan är således inte kännetecknande enbart för neobanker.

Snabbt och effektivt skapande av betalkonto

Det går snabbt och enkelt att öppna ett betalkonto. Oftast skapas kontot redan inom ett par minuter direkt i mobilen.

Betalkort

En neobank erbjuder oftast ett kostnadsfritt basutbud där det ingår ett betalkonto med tillhörande betalkort, som bland annat kan användas utomlands med låga eller inga kostnader för valutaväxling. Om kunden vill ha fler fördelar kopplade till sitt betalkonto och betalkort finns det avgiftsbelagda premium-konton att välja mellan. Neobanker erbjuder oftast både fysiska och virtuella betalkort. Virtuella betalkort fungerar på liknande sätt som fysiska betalkort, men kortuppgifterna finns bara tillgängliga digitalt.

Mobilapp

Mobilapparna erbjuder olika funktioner, bland annat:

- Möjlighet att spärra och låsa upp sitt betalkort direkt i mobilappen.
- Möjlighet att föra över pengar internt till andra konton inom neobanken alternativt till andra banker.
- Tjänsten ”Köp nu betala senare” börjar bli vanligt förekommande.⁷

Budgetering och överblick

Kunden kan föra över pengar från sina andra bankkonton till sitt konto hos neobanken, och på så sätt skapa sig en god överblick över sitt sparande och sina kostnader samt budgetera för kostnader.

Gemensamt betalkonto

Det fungerar som ett vanligt betalkonto, men flera personer kan stå som ägare och ha ett varsitt betalkort kopplat till kontot. Alternativt kan det vara en person som står som ägare till betalkontot, och som kan bjuda in andra personer till kontot.

⁶ Exempelen som listas gäller inte för samtliga neobanker på den svenska marknaden, utbudet kan skilja sig åt. De avser en generell beskrivning av ett tjänste- och produktutbud som oftast ingår.

⁷ <https://www.cnn.com/2021/09/10/monzo-and-revolut-to-enter-buy-now-pay-later-market.html>.

Dela på kostnader

En betalning/ett kortköp kan enkelt delas mellan flera personer förutsatt att de är kunder inom samma neobank. Kunden väljer en betalning och hur den ska fördelas, exempelvis i lika stora delar, procentdel eller summa och sänder en förfrågan till utvalda kontakter i appen.

Överföringar

Överföringar kan ske snabbt till andra personer inom samma neobank, genom att exempelvis scanna en QR-kod, skicka pengar till personer i telefonens kontaktlista eller genom att ange en e-mailadress alternativt användarnamn som är kopplat till mottagarens konto hos neobanken.

Erbjudanden och bonusar

För att attrahera nya kunder erbjuder neobanker ofta bonusar i form av till exempel startkapital vid nyregistreringar eller bonusar vid rekrytering av vänner. Det kan även förekomma erbjudanden om rabatter hos andra bolag som neobankerna samarbetar med.

Digitala betaltjänster

En del neobanker stödjer numera att deras kunder kopplar sina betalkort till en betallösning. Tre av de största tjänsterna som erbjuder mobila betalningar kopplade till kort via telefon och med en så kallad ”Pay” funktion är Google Pay, Apple Pay och Samsung Pay. I princip kan de flesta betalkort kopplade till något av de tre största kortnätverken (VISA, Mastercard, American Express) anslutas till ovan lösningar.

Kryptovalutor

Att tillhandahålla handel för kryptovalutor är något som ökar hos neobanker. Ett flertal neobanker har sitt ursprung i kryptovalutor, exempelvis som handelsplattformar, och har sedan utökat sitt kunderbjudande med fler tjänster.

Många neobanker tillhandahåller sina kunder plånböcker för kryptovalutor samt lösningar för överföringar mellan dessa. Kunder har således möjlighet att flytta kryptovalutor till och från externa plånböcker (egna eller andras). Ofta erbjuds numera också betalkort kopplade till kryptotillgångarna. Köp kan göras för Fiat valuta och kortet krediteras sedan av kryptotillgången genom en växling. Utvecklingen av betalkort kopplade till kryptotillgångar är ett område som kortnätverk (exempelvis VISA och Mastercard) satsar på, med bland annat målet att tillhandahålla snabbare eller direkt inlösen av kryptotillgångar.

Det finns neobanker som erbjuder handel med kryptovaluta endast inom sin egen plattform. Det medför att det inte går att överföra kryptovaluta mellan

exempelvis en extern plånbok och kontot hos neobanken. Liksom hos traditionella banker skiljer sig ställningstagandet åt huruvida handel med kryptovalutor tillåts, det kan förekomma utan restriktioner hos en del medan en annan del blockerar penningöverföringar till vissa handelsplattformar.

1.3 Exempel på neobanker

Det finns ett stort antal neobanker. En onlinedatabas listar över 246 neobanker globalt varav 76 stycken i Europa. I Europa har de flesta neobanker sina huvudkontor i England och Frankrike, följt av Tyskland och Schweiz.⁸

Svenska medborgare kan bli kunder hos dessa neobanker, om neobankerna har tillstånd hos ett EU land för att kunna erbjuda sina produkter och tjänster på den europeiska marknaden utan att behöva ansöka om enskilda tillstånd hos övriga länder, via så kallad "passporting".⁹

Att skapa en neobank behöver inte vara komplicerat. Det finns ett ökat antal bolag som erbjuder tjänster med byggblock för ändamålet. Banking as a service (BaaS), open banking och platform banking är några snarlika men skilda koncept av lösningar för företag. PrePay Solutions¹⁰ (PPS EU) och det svenska bolaget Vilja¹¹ är exempel på bolag som erbjuder sådana tjänster.

För att ge exempel på olika sorters neobanker presenteras en kort lista nedan på neobanker som tillhandahåller sina produkter och tjänster i Sverige.

Neobank	Kommentar
Wise (tidigare Transferwise)	Registrerade i Belgien.
Monese	Har sitt huvudkontor i England, men har egen EU-licens. Efter Brexit har de ingått samarbete med e-pengainstitutet PPS EU i Belgien och erbjuder därigenom sina tjänster och produkter på den europeiska marknaden.
Bunq	Registrerade i Nederländerna. Har banklicens. Första Fintech-bolaget att gå med i TIPS, EU-systemet för direktöverföringar mellan banker.

⁸ <https://neobanks.app/>

⁹ <https://www.eba.europa.eu/regulation-and-policy/passporting-and-supervision-branches>

¹⁰ <https://www.pps.edenred.com/>

¹¹ <https://viljasolutions.com/>

Fidor Bank	Registrerade i Tyskland – en av de första neobankerna (år 2009). Har banklicens.
Nuri (tidigare Bitwala)	Registrerade i Tyskland, kontolösning via Solarisbank AG. Erbjuder bland annat handel med virtuell valuta, plånböcker för kryptovaluta.
Paysend	Har ingen egen EU licens, samarbetar med Easy Payment and Finance (EP, S.A) registrerade i Spanien.
Gimi	Registrerade i Sverige och erbjuder betalkort via PFS Card Services (Irland). Erbjuder förbetalda kort där marknadsföringen riktar sig till barn och deras föräldrar.
Northmill Bank	Registrerade i Sverige. Har banklicens.
N26	Registrerade i Tyskland. Har banklicens.
Klarna Bank	Registrerade i Sverige. Har banklicens. Används främst för att genomföra betalningar vid shopping, men erbjuder även sparkonton och kort bland annat.
P.F.C.	Registrerade i Sverige.
Revolut	Grundades i England, men idag rapporteringspliktiga i Litauen. Har banklicens.
Rocker	Registrerade i Sverige.
Lunar Bank	Registrerade i Danmark. Har banklicens.

Neobanker riktade mot företagskunder

SME (small and medium-sized enterprises), det vill säga små och medelstora företag, uppskattas täcka 99 % av företagen inom EU.¹² För många neobanker är detta ett attraktivt segment och flera neobanker (t.ex. Revolut och Lunar Bank) tillhandahåller därför lösningar för såväl privatkunder som företagskunder. Utvecklingen av antalet neobanker som riktar sig till endast företagskunder är snabbväxande. Det finns både svenska neobanker av detta slag, men även en del utländska som både är etablerade i och riktar sig mot den svenska marknaden. Några exempel på denna typ av neobanker är Qonto, Tide, Holvi, Pleo samt Mynt.

¹² https://ec.europa.eu/growth/smes/sme-definition_en

2 Risker för penningtvätt och terrorfinansiering

I detta avsnitt beskrivs en del risker för penningtvätt och terrorfinansiering kopplade till neobankers. Neobankers tillhör Fintechsektorn, för vilken Finanspolisen tidigare har gjort en utförlig beskrivning av risker och hur de riskerna kan motverkas. Då flertalet av dessa risker även gäller för neobankers rekommenderas för ytterligare beskrivning att ta del av publikationerna från Black Wallet projektet.¹³

2.1 Neobankernas internationella struktur

Neobankers begränsas inte av en kundbas i det egna landet eftersom de kan ha kunder internationellt. För svenska medborgare innebär det att de kan vara kunder hos en utländsk neobank, varvid de kan utföra transaktioner i Sverige via sitt betalkort men transaktionerna utförs rent tekniskt i det land där neobanken är registrerad. Neobankers är, liksom andra finansiella institut, rapporteringspliktiga i det land där de är registrerade. Detta kan bli problematiskt ur ett penningtvätts- och terrorfinansieringshänseende eftersom en svensk medborgare kan genomföra misstänka transaktioner via ett betalkort utfärdat av exempelvis en dansk neobank där de danska myndigheterna är de som underrättas om misstanken. Samma scenario gäller om en utländsk medborgare skulle vara kund hos en svensk neobank.

Om samarbetet mellan myndigheter i olika länder inte fungerar effektivt och ingen vidareberapportering sker av utländska medborgare riskerar länder att ha begränsad kunskap om sina medborgares ekonomiska förhållanden utomlands.

Ingen svensk tillsyn

Många neobankers som är verksamma på den svenska marknaden är utländska finansiella institut som har erhållit tillstånd i ett annat EU-land. Finansinspektionen har inte någon tillsyn över neobankers som inte har en filial i Sverige men som istället erbjuder sina tjänster via ”passporting”. Neobankers som inte har en filial i Sverige är även undantagna den periodiska rapporteringsplikten som ska göras till Finansinspektionen. Detta medför att kvalitén och omfattningen på tillsynen är beroende av den utländska tillsynsmyndighetens förmåga.

Begränsad marknads- och kundkännedom

En neobank kan som tidigare nämnts ha kunder i många länder. En hypotes är att en neobank har fokus främst på den inhemska marknaden i det land

¹³ Publikt material finns tillgängligt på Finanspolisens hemsida.

den fick tillstånd och då även risker förknippade till den marknaden, samtidigt som det kan finnas en begränsad eller försvårad möjlighet för neobanken att inhämta och tillgodogöra sig tillräckligt med information om sina utländska kunder.

Olika marknader har i stort liknande risker, men de kan också skilja sig åt från land till land. Skillnaderna kan bestå i avvikande områden i form av utsatta områden, kriminella nätverk, brottstyper som utmärker sig i vissa länder, korruption och andra risker som kan vara bra för en verksamhetsutövare att känna till för att kunna anpassa sin monitorering. Sammanfattningsvis innebär det att utländska neobanker kan ha en begränsad kunskap om den svenska marknaden såväl som den svenska kriminella kontexten.

2.2 Falska identiteter, identitetsstöld och målvakter

Likt andra finansiella institut, är neobanker skyldiga att följa penningtvättsreglverket och genomföra kundkännedomsgärder på sina kunder.

Generellt går det relativt snabbt att registrera ett konto hos en neobank. Detta är dessutom något som neobanker lyfter i sin marknadsföring. Processen för att skapa ett nytt konto tar ett par minuter.¹⁴ Kundkännedomprocesserna kan skilja sig åt mellan olika neobanker, men i takt med att skapandeprocessen för kontot effektiviseras kan kvalitén också påverkas. Det finns misstankerapporter som bekräftar att falska identiteter använts vid registrering av konton hos neobanker.

Det föreligger risk för att en kriminell aktör kan utnyttja en målvakt för att skapa ett konto hos en neobank. Åtkomsten till kontot överförs till den kriminella aktören därefter. Det finns underrättelser som styrker att kriminella aktörer använder sociala medier så som Snapchat och Instagram för att locka och rekrytera målvakter mot betalning. Personerna uppmanas att ha tillgång till svenska identitetshandlingar, mobiler med simkort samt en mejladress för att sedan ladda ner neobanksappar.

Många utländska neobanker har för närvarande en registreringsprocess där kunden lämnar ifrån sig personuppgifter och viss dokumentation. Risken med att göra detta kan medföra en ökad risk för identitetsstöld, då informationen kan hamna i orätta händer. Som privatperson kan man idag inte veta med säkerhet om någon skapat diverse konton hos finansiella institut med ens personuppgifter.

¹⁴ <https://www.lunar.app/se/ladda-ner>, <https://get.n26.com/>, <https://getpfc.com/sv/hem/>.

2.3 Insättning på konton hos neobanker

Det finns ett antal olika sätt för en kund hos en neobank att göra insättningar på sitt konto. Nedan beskrivs några av dem samt en del risker kring de olika metoderna. Att sätta in pengar på sitt konto benämns hos neobankerna som ”top-up”. I vissa fall kan top-ups utföras av andra personer än kunden. Utöver nedan olika sätt är insättningar i form av överföringar från spel- och kryptoplattformar också förekommande.

En risk gällande insättningar på konto till neobanker är att transaktionen kan ske via en kedja av olika verksamhetsutövare. Det finns en risk för att information om en transaktionskedja går förlorad eftersom transaktionen passerar flera verksamhetsutövare som har tillgång till olika delar av transaktionskedjan.

Kontanter

Majoriteten av neobankerna har inte stöd för direktinsättningar av kontanter, men det finns en del neobanker som erbjuder det och då ofta via samarbeten med en tredjepart. Genom att i appen skapa en streckkod/QR-kod för en kontantinsättning kan man sätta in kontanter via ett stort utbud av butiker och kiosker.¹⁵ Kontantinsättningar kan också ske via en penningöverförare genom att ange ett IBAN-nummer. En kontant betalning av en kreditkortsräkning är också ett möjligt tillvägagångssätt att betala med kontanter.

En ytterligare möjlighet är om kunden har ett kreditkort utgivet av en traditionell bank. Då kan en top-up till en neobank hamna på en räkning som betalas kontant. Exempelvis kan en Revolutkund göra en top-up på sitt konto genom att betala med ett kreditkort som är utgivet av Swedbank, för att sedan betala räkningen kontant genom Kassagiro.

Swish

Snabba insättningar med Swish erbjuds via en del neobankers gränssnitt. Detta gäller för närvarande främst svenska bolag men även en del andra bolag riktade mot den svenska marknaden.

Hos den aktuella neobanken väljer användaren belopp samt att insättningen ska ske via Swish. Swish-appen öppnas och överföringen godkänns och utförs. Pengarna hamnar hos en mottagande bank på ett klientmedelskonto tillhörandes neobanken. Den mottagande banken ser dock inte vem som är kontoinnehavare av det konto hos neobanken som ska krediteras med

¹⁵ <https://n26.com/en-es/blog/cash26> , <https://www.viacash.com/>, <https://www.bunq.com/benefits/withdraw-deposit>, <https://www.fidor.de/en/mobile-payment/fidor-cash>

swishinsättningen. Den avsändande banken har i sin tur inte heller några uppgifter om mottagaren.

Det skiljer sig alltså åt vad olika parter i transaktionskedjan kan se för information gällande en transaktion. Det innebär att neobanken inte heller har tillgång till all information. Neobanken vet vilket konto hos dem som ska krediteras med en insättning och de vet vem som är kontoinnehavare av det kontot, men de har inte tillgång till information om vem som är avsändare. Neobankens möjligheter att verifiera om det är den egna kunden som är avsändare av transaktionen och om swishnumret tillhör den egna kunden är alltså begränsade. Hur mycket information som Swish har tillgång till avseende detta transaktionsflöde är inte utrett.

I dagsläget går det inte att koppla Swish till ett konto hos en neobank, med andra ord kan Swishtransaktioner inte dras från ett konto hos en neobank.

Betalkort

En insättning kan ske direkt via betalkort, men det finns en del kort som i vissa fall inte stöds.

Neobankens kund initierar en korttransaktion genom ett gränssnitt via neobanken som kan ske direkt. Då pengarna oftast går till neobankens 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.

Kontoöverföring

Hos en del neobanker får kunden ett IBAN-nummer kopplat till sitt konto. Kontoöverföringar kan då genomföras från annan bank via SEPA och SWIFT, en transaktion som normalt sett tar ett par dagar att genomföra om det är en internationell transaktion.

Som beskrivet tidigare gällande både insättningar med Swish och betalkort, har avsändande respektive mottagande banker samt neobanken ifråga begränsad information om mottagare och avsändare. Samma gäller även för insättningar via kontoöverföring

Förbetalda engångskort

Insättningar med hjälp av förbetalda engångskort går att göra på konton hos en del neobanker.¹⁶ De förbetalda engångskorten ska i de flesta fall vara utställda av MasterCard eller Visa och dessa går exempelvis att köpa på Pressbyrån, 7Eleven och i andra liknande butiker. Fördelen med förbetalda

¹⁶ Webmoney - <https://www.wmtransfer.com/eng/information/short/index.shtml>, Paypal - <https://www.businessinsider.com/how-to-add-gift-card-to-paypal?r=US&IR=T>

engångskort för en kriminell aktör är att användaren kan vara anonym då kortet inte kan kopplas till en person och köpet kan göras med kontanter. Risk finns således för att förbetalda engångskort kan köpas för kontanta brottsvinster och pengarna görs sedan tillgängliga på konton hos neobanker för att exempelvis föras vidare för att ackumulera större summor hos en och samma mottagare.

En förbestämd summa är dock redan insatt på de förbetalda engångskorten, vilket begränsar möjligheten för den kriminella aktören att själv bestämma vilken summa som ska sättas in på kortet. Däremot finns det en möjlighet att köpa flera förbetalda engångskort med hjälp av målvakter, utspritt över olika butiker och dagar för att skingra misstanke från butiksbiträdet.

2.4 Den dolda ekonomin

Det finns risk för att kontot hos neobanken nyttjas för att upprätthålla en parallell ekonomi som är dold för den egna traditionella banken och för brottsutredande myndigheter. Genom banköverföringar till ett IBAN-konto hos en neobank kan insättningar förekomma i form av löneutbetalningar¹⁷ samt överföringar från andra personer. Insättningar i form av överföringar mellan kunder inom neobanken är ofta också enkla att genomföra.

Exempelvis kan en kriminell aktör ha en inkomst i form av lön eller bidrag som varje månad betalas in på dennes konto hos en traditionell bank. Via detta konto genomförs betalningar för hyra, fasta utgifter och diverse betalningar som förefaller normala. Den traditionella banken har ingen anledning att misstänka någon kriminell verksamhet. Den kriminella aktören använder dock sitt konto hos en neobank för att dölja och använda brottsligt förvärvade pengar. Inkomst som kommer från ett icke deklarerat arbete överförs till aktörens konto hos neobanken varje månad. Aktören kan få tillgång till de oskattade pengarna via det betalkort som tillhör kontot, och kan därigenom konsumera pengarna. Då pengarna inte passerar aktörens primära bankkonto hos den traditionella banken, kan den traditionella banken inte upptäcka den dolda ekonomin som aktören innehar hos en neobank. På samma sätt är det inte möjligt för neobanken att få vetskap om aktörens övriga inkomster som innehåses på det primära bankkontot, och misstänker därför inte heller att insättningarna på neobankens konto sannolikt härrör från kriminell verksamhet.

¹⁷ <https://www.revolut.com/en-BE/help/adding-money/with-bank-transfer/can-i-get-my-salary-paid-into-my-revolut-account>

2.5 Finansiering av terrorism

På grund av användarvänligheten avseende vissa tjänster och möjligheten att enkelt hantera ett stort antal konton kan neobanker vara ett redskap för terrorfinansiering. Snabba, gränsöverskridande och delvis dolda transaktioner och konton är attraktiva vid finansiering av terrorism. På så vis skiljer sig inte riskerna för terrorfinansiering från de risker gällande penningtvätt som beskrivs i denna rapport.

3 Tillvägagångssätt för penningtvätt och terrorfinansiering

I följande kapitel beskrivs en del tillvägagångssätt för penningtvätt via neobanker och avslutningsvis tillvägagångssätt för terrorfinansiering via neobanker. Informationen är hämtad från misstankerapporter som inkommit till Finanspolisen från både neobanker och traditionella banker samt annat underrättelsematerial.

3.1 Skiktning

Möjlighet att följa pengar som kommer från brottslig verksamhet försämras genom att pengarna skiktas genom olika neobanker. En stor del av inkomna misstankerapporter bekräftar detta tillvägagångssätt.

Pengar som härrör från brottslig verksamhet, som i många fall har handlat om bedrägeribrott, mottas på en aktörs bankkonto hos en traditionell bank. Pengarna skickas omgående vidare till konton hos en eller flera neobanker, där de oftast tas ut kontant via bankomater eller sänds vidare till exempelvis ytterligare en neobank eller kryptoplattform.

De inblandande verksamhetsutövarna har begränsade möjligheter och resurser att se den fullständiga transaktionskedjan och transaktionsflöden.

3.2 Användning av kryptovalutor

Användning av kryptovalutor direkt via betalkort är en möjlighet som en del neobanker erbjuder.

Ett modus som noterats är att brottsvinster i kryptovaluta överförs till en kryptoplånbok kopplad till ett betalkort som tillhör en neobank. Betalkortet används vid köp i butiker eller liknande, och kryptovalutan omvandlas till fiatvaluta vid köptillfället. Den kriminella aktören kan via detta förfarande konsumera sina brottsvinster.

Vidare kan ovannämnda betalkort möjliggöra för en kriminell aktör att föra över den vinst som gjorts på kryptovaluta från sin kryptoplånbok och som därefter kan användas vid köp i butik. Den som har gjort en vinst på kryptovalutor ska betala 30 procent i skatt på vinsten, och den som sålt, bytt eller betalat med kryptovalutor ska redovisa detta till Skatteverket i samband med

deklarationen.¹⁸ Eftersom det oftast åligger den egna personen att ta upp eventuella vinster i sin deklaration, kan det leda till ökad risk för skattefusk.

3.3 Spridda tillgångar

Underrättelser vittnar om en utbredd förekomst bland kriminella av att ha betalkort kopplade till neobank. Att sprida sina tillgångar genom att vara kund i flera olika banker, däribland neobank, är ett sätt att undgå upptäckt, vilket noteras som ett tillvägagångssätt i underrättelser.

Som exempel på förekomsten hade en utländsk neobank drygt 160 000 kunder i Sverige år 2020. Sverige utmärkte sig i ett nordiskt sammanhang med stor omsättning. Kontantuttagen i vissa områden utmärkte sig, särskilt i storstäder och i vissa utsatta områden.¹⁹ En stark representation av aktörer som blivit misstankerapporterade av neobanken i fråga ägnar sig åt narkotikahandel.

3.4 Snabba återbetalningar av lån eller krediter

Lån tas i syfte att amortera lånet med pengar som kommer från brottslig verksamhet.

Upplägget är att lån eller krediter som tas hos en neobank återbetalas inom kort tid, både med höga amorteringsbelopp och snabba återbetalningar som kan ske av låntagaren själv eller av andra personer. Detta är ett tillvägagångssätt som uppmärksammas i tidigare fall, exempelvis gällande amortering av billån eller andra lån hos traditionella banker.

3.5 Indikationer och tillvägagångssätt som föranlett misstankerapporter

Vid inrapportering till Finanspolisen ska rapportören ange en eller flera indikatorer som föranlett misstanken. Indikatorerna kan ge en insikt i tillvägagångssätt för penningtvätt och terrorfinansiering.

Enligt de misstankerapporter som undersöktes inom ramarna för denna rapport med kopplingar till neobank ser fördelningen i kategorierna ”produkter och tjänster” samt ”kundkännedom” ut enligt nedan.

¹⁸<https://www.skatteverket.se/privat/skatter/vardepapper/andratillgangar/kryptovalutor.4.15532c7b1442f256bae11b60.html>.

¹⁹ Information framtagen ur en gemensam analys mellan Finanspolisen och neobanken i fråga.

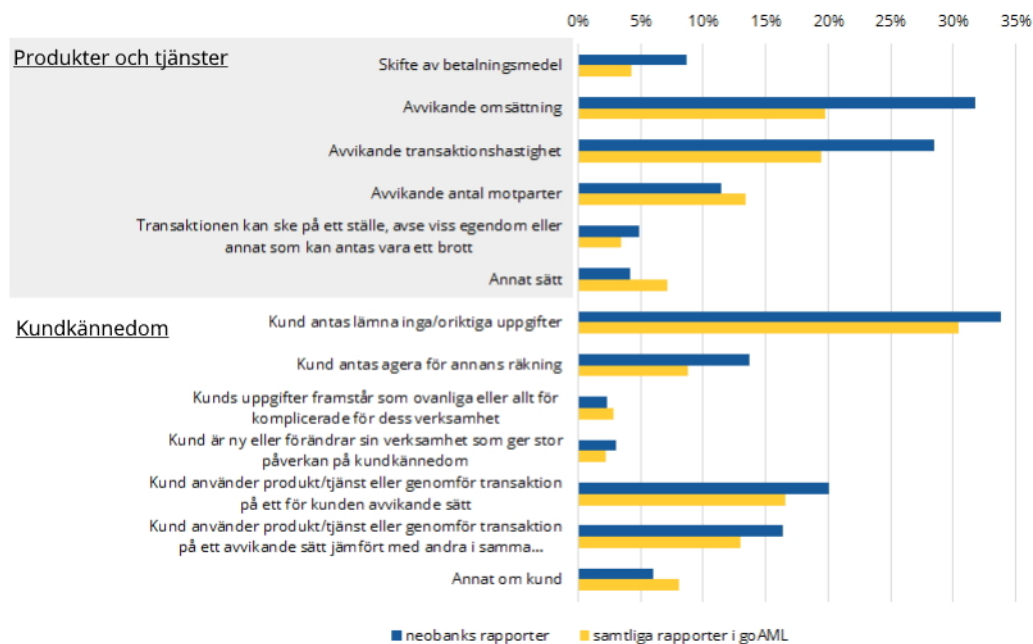


Diagram 1 Indikatorer från verksamhetsutövare

I kategorin ”produkter och tjänster” utmärker sig indikatorerna avseende *betalningsmedel*, *avvikande omsättning* och *avvikande transaktionshastighet* i jämförelse med samtliga misstanke rapporter. Detta indikerar att misstanke rapporter med kopplingar till neobankers i större utsträckning har en avvikande omsättning och avvikande transaktionshastighet. Resultatet av indikatorerna i denna kategori stärker tesen att neobankers används av kriminella då det ger dem möjlighet till snabba transaktioner och därför kan skicka svarta pengar enklare.

I kategorin ”kundkännedom” utmärker sig tre indikatorer. Här har rapportörerna i högre grad reagerat på att kunden lämnat oriktiga underlag eller inga alls, att kunden är ny eller förändrat sin verksamhet samt att kunden antas agera åt någon annan. Detta styrker hypotesen att det förekommer målvaktskonton i högre grad relaterat till neobankers, något som också tagits upp tidigare i rapporten.

Sammanfattningsvis visar indikatorerna från rapporter kopplade till neobankers på en större misstankegrad grundad på snabba transaktioner (skiktningar), att kund antas agera åt någon annan och avvikande omsättningar, till skillnad från indikatorer avseende totala antalet misstanke rapporter.

3.6 Terrorfinansiering

Misstankerapporter som inkommit rörande finansiering av terrorism står för 2 % av den totala inrapporteringen av neobanker. Siffran ligger i nivå med den totala inrapporteringen från samtliga rapportörer gällande finansiering av terrorism.

Ett exempel på tillvägagångssätt är att en kriminell aktör mottar insamlingar via Swishinsättningar, kontantinsättningar samt insättningar från utlandet på sitt bankkonto hos en traditionell bank. En del av den mottagna summan överförs i ett senare skede till en eller flera olika neobanker, och den andra delen av summan används för köp av kryptovalutor, resor, klockor och smycken samt till kontantuttag utomlands. Den överförda summan till neobanker används i sin tur också för kontantuttag utomlands, där kontanterna sedan kan föras vidare till ett riskområde ockuperat av terroristorganisationer.

4 Misstankerapporter

I detta avsnitt presenteras statistik som är hämtad från misstankerapporter som Finanspolisen mottagit från neobanker och även rapporter från traditionella banker där transaktioner till och/eller från neobanker beskrivits i misstanken. Utifrån dessa ges en överblick över de inrapporterade personernas kön, ålder samt kopplingar till annan brottslig verksamhet. Det är 2 619 personer inkluderade.

Det är viktigt att lyfta fram att på grund av hur data registreras har det inte varit möjligt att kunna identifiera vilka personer som varit misstänkta och vilka som ingått i rapporten enbart för att de blivit utsatta på ett eller annat sätt, exempelvis bedrägeri.²⁰ Fördelningen av kön och ålder visar således en gemensam bild av kriminella aktörer och eventuella brottsoffer, medan kopplingen till annan brottslig verksamhet visar en statistisk bild av de personer som faktiskt förekommer i andra underrättelser som rör annan brottslig verksamhet eller kriminella grupperingar.

Antalet inkomna misstankerapporter i urvalet ligger på en nivå kring 80 misstankerapporter per månad. Misstankerapporter från svenska neobanker är också inkluderade och står för cirka 5 % av misstankerapporterna.

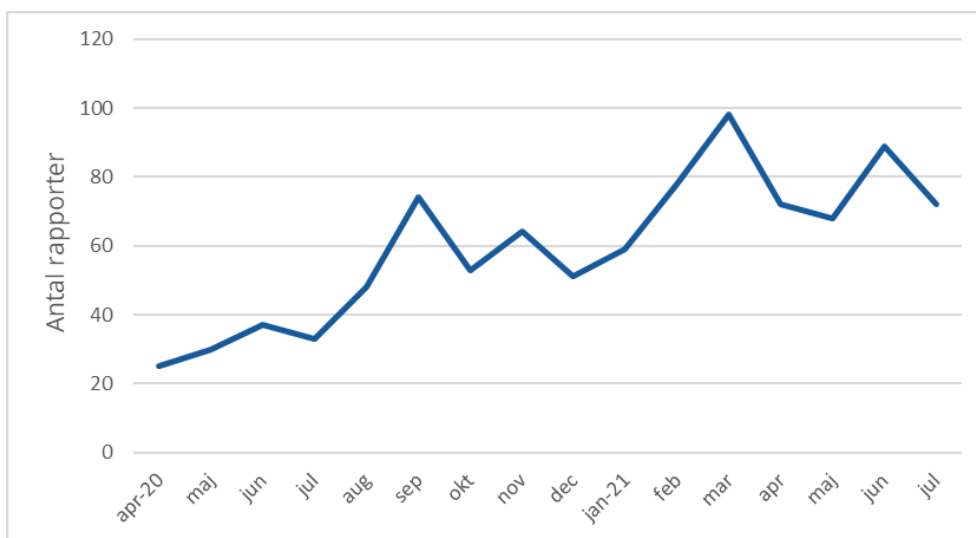


Diagram 2 Antalet inkomna misstankerapporter över tid

4.1 Kön och ålder

Av de 2 619 personer som ingått i mottagna misstankerapporter har 713 varit kvinnor och 1 906 män, det vill säga 27 % kvinnor och 73 % män. Majoriteten av personerna är födda under 1980 eller 1990-talet. Diagrammet

²⁰ Misstankerapporter som granskats är av typen STR (Suspicious Transaction Report).

nedan visar fördelningen i ålder avseende nämnda personer, de fem mest förekommande årtiondena är presenterade.

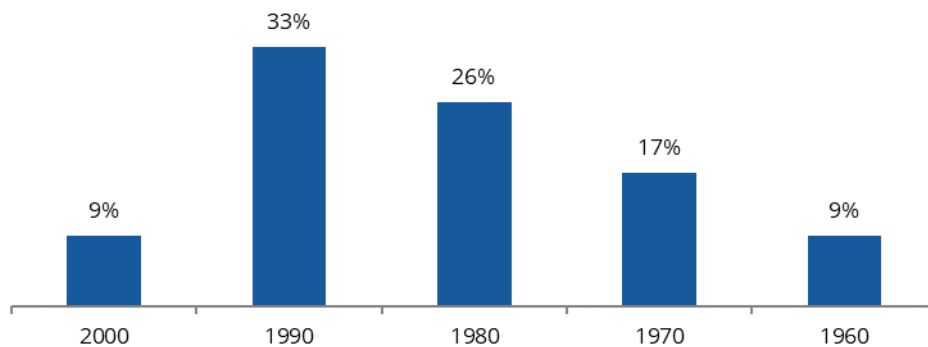


Diagram 3 Inrapporterade personers fördelning av ålder

Av de inrapporterade som även förekommer i andra underrättelser är överrepresentationen av män något större (82 %). Majoriteten av personerna är fortfarande födda under 1990-talet (41 %) följt av personer födda under 1980-talet (28 %).

4.2 Kopplingar till annan brottslighet

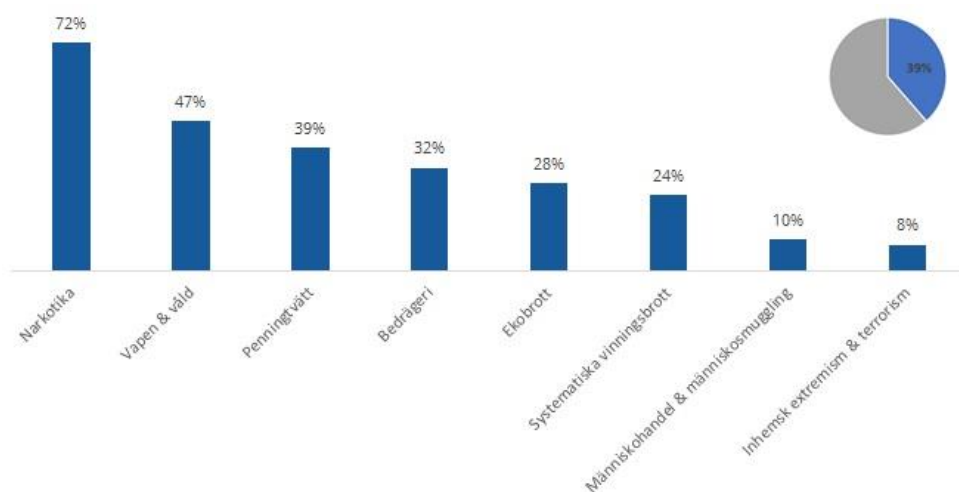


Diagram 4 Andel av personerna som förekommer i underrättelse efter koppling till vissa andra brottsområden. En person kan vara kopplad till flera olika brottsområden, vilket gör att antalet förekomster inom alla brottsområden är fler än antalet personer.

Det finns en tydlig koppling till allvarlig och organiserad brottslighet för de inrapporterade personerna genom att 1 010 personer (39 %) förekommer med minst en underrättelse inom allvarlig eller organiserad brottslig verksamhet.

Flest kopplingar finns till narkotika, penningtvätt, vapen och våld samt bedrägerier. Kategorin penningtvätt innebär att brottsvinster kommer från annan brottslig verksamhet, men där det inte framgått vilken brottslighet som föregått penningtvätten. Brottsområden med en koppling på under 2 % är

inte med i diagram 4. De kategorierna är exempelvis korruption, miljöbrott, sexualbrott mot barn samt IT-brott.

4.3 Kopplingar till kriminella grupperingar

Av de personer som förekommer i underrättelser kan 91 personer (9 %) mer tydligt kopplas till en kriminell gruppering eller nätverk antingen genom att personen ingår i grupperingen eller för att i någon utsträckning har eller har haft en koppling till den.²¹

Grovt sorterat finns tydligast kopplingar till lokala kriminella nätverk. Dessa nätverk kännetecknas av att de i huvudsak har anknytning till ett specifikt geografiskt område, där de har en stark kriminell påverkan även om deras kriminella verksamhet sällan är begränsad till det geografiska området. Majoriteten av dessa är verksamma inom *utsatta områden* och en större andel av dessa nätverk ägnar sig åt narkotikabrottslighet.²²

Andra underrättelser bekräftar att medlemmar i lokala kriminella nätverk är användare av neobanker. Det förekommer underrättelser om kriminella aktörer vars kontoutdrag visar på frekventa transaktioner till och från konton hos neobanker, samt kriminella aktörer som vid stopp och kontroll av fordon eller vid husrannsakan har haft betalkort från olika neobanker.

²¹ Personer som står/stått i konflikt med den kriminella grupperingen eller endast setts ihop med grupperingen vid något tillfälle har exkluderats från analysen.

²² Rapport: *Kriminella nätverk inom den organiserade brottsligheten*, 2019, s. 14

5 Slutsatser

- Neobanker utnyttjas av kriminella för att hantera och tvätta pengar från brottsvinster, vilket inte minst gäller kriminella grupperingar i utsatta områden som är aktiva i narkotika- och våldsbrottslighet.
- Det finns en sårbarhet i informationsdelningen rörande transaktioner mellan olika verksamhetsutövare i transaktionskedjan.
- Det är sannolikt att neobanker är en växande verksamhet där kriminellas användning i penningtvättsupplägg kommer att öka framgent och följa den allmänna tekniska utvecklingen.
- Det kan troligen föreligga en sårbarhet hos utländska neobanker eftersom de inte känner till den svenska kontexten, bland annat riskbedömningar av svenska kunder kan således bli begränsade. Detsamma kan även gälla för svenska neobanker som är verksamma internationellt.

6 Tänkbara åtgärder

6.1 Neobanker riktade mot företagskunder

Neobanker som enbart riktar sig mot företagskunder har inte analyserats inom ramarna för denna rapport. En ny analys kan vara behövlig för att undersöka dessa typer av neobanker utförligare och analysera riskerna för penningtvätt och finansiering av terrorism.

6.2 Internationellt samarbete

Denna rapport visar på att penningtvätt genom neobanker används vid delvis snabba skiktningar, oftast transaktioner mellan landsgränser och flera jurisdiktioner som är involverade. För att mitigera risker som kan uppkomma vid landsöverskridande transaktioner, behövs ett stärkt internationellt samarbete mellan Finanspolisen samt aktuella utländska FIU:er och utländska bolag. Det kan även finnas behov av ett ökat internationellt samarbete mellan Finansinspektionen och utländska tillsynsmyndigheter i frågor rörandes tillsyn av neobanker.

6.3 Mekanismen

Lagen (2020:272) om konto- och värdefackssystem möjliggör för myndigheter att snabbt kunna hämta information om var en person har konton och värdefack. Med hjälp av den tekniska plattformen, den s.k. Mekanismen, blir uppgifterna direkt och omedelbart tillgängliga för sökning, och manuella förfrågningar riktade mot de enskilda finansiella instituten kan undvikas. Av lagen om konto- och värdefackssystem framgår att den omfattar kreditinstitut, utländska kreditinstitut med filial i Sverige, värdepappersbolag samt utländska värdepappersbolag med filial i Sverige. Med kreditinstitut avses bank och kreditmarknadsföretag, således omfattas de flesta svenska neobanker inte av den nya lagen och kommer inte inkluderas i Mekanismen. Förslaget är att utöka vilka finansiella institutstyper som ska omfattas av Mekanismen.

För närvarande omfattas inte heller utländska gränsöverskridande finansiella institut som saknar filial i Sverige. Det innebär att majoriteten av neobanker hamnar utanför lagens tillämpningsområde. Detta till trots att det finns möjlighet att omsätta, förvara och dölja tillgångar via konton utfärdade av neobanker. Utländska finansiella institut ska rapportera in kunders konton till Skattemyndigheten i det egna landet i enlighet med CRS, Common Reporting Standard, och som även är OECD:s rapporteringsnorm för utbyte av

uppgifter om finansiella konton mellan olika stater och jurisdiktioner.²³ För närvarande råder det dock inte konsensus mellan länders myndigheter om huruvida e-pengainstitut ska lämna uppgifter till myndigheterna i enlighet med CRS. Det innebär alltså att det idag beror på institut till institut och land till land om ett e-pengainstitut, liksom andra finansiella aktörer, är skyldiga att rapportera enligt CRS. Förslaget är att utreda möjligheten att information som skickas in till Skatteverket gällande konton för svenska medborgare hos utländska finansiella företag ska göras enkelt tillgängligt för övriga myndigheter, exempelvis till de myndigheter som har tillgång till Mekanismen.

6.4 eID

Identifiering och verifiering av kunder vid registrering samt vid fortsatt användande av neobankernas tjänster skiljer sig åt vad gäller kvalitet och säkerhet. EU's eIDAS-förordning (910/2014)²⁴ gör det möjligt för den privata sektorn att frivilligt använda medel för elektronisk identifiering, detta är dock inget krav.²⁵ Det ställs däremot krav på den offentliga sektorn att stödja nationella eID (elektronisk legitimation) från andra medlemsländer.²⁶ Som det fungerar nu att användare lämnar ifrån sig personuppgifter och viss dokumentation till flera olika finansiella institut kan medföra risker så som identitetsstöld och falska identiteter.

För neobanker finns som nämnts möjlighet att använda sig av inloggning via eID, antingen genom integrering mot respektive EU land²⁷ eller via tredjepartleverantörer som tillhandahåller lösningen, detta är dock inte tvingande. Förslaget är således att se över om förordningen även bör ställa högre krav på den privata sektorn.

²³ <https://www.oecd.org/tax/automatic-exchange/common-reporting-standard/>

²⁴ Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden

²⁵ Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden, p. 17.

²⁶ <https://www.digg.se/4a3a85/globalassets/dokument/publicerat/publikationer/stodjande-atgarder-vid-nationellt-inforande-av-eidas-forordningen.pdf>

²⁷ <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eID+-+Public+Service+Providers>