SIMPT
Svenska institutet mot penningtvätt
Swedish Anti-Money Laundering Institute

Bank

Vägledning om allmän riskbedömning

Andra upplagan

Beslutad av Simpts styrgrupp i november 2024

Innehållsförteckning

Simpts vägledning har tagits fram av sju organisationer i finansbranschen och deras medlemmar. Den utgår från medlemmarnas behov av vägledning och är inte avsedd att vara heltäckande.

Vägledningen beskriver hur branschen tolkar och tillämpar penningtvättsregelverket i aktuella delar.

Vägledningen ersätter inte lagar, föreskrifter och andra rättskällor. Dessa måste alltid beaktas och tillämpas i förekommande fall.

Det finns inte någon skyldighet att använda vägledningen. Den som använder vägledningen måste alltid göra bedömningen om vägledningen är tillämplig i det enskilda fallet.

Denna del av vägledningen har tagits fram av medlemmar hos Svenska Bankföreningen. Den ska läsas tillsammans med och kompletterar den grundläggande vägledningen om allmän riskbedömning.

I denna del av vägledningen hänvisas bl.a. till lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism (penningtvättslagen). Alla laghänvisningar avser penningtvättslagen, om inte annat anges. Hänvisningar görs även till Europeiska bankmyndighetens (Eba) riktlinjer enligt artiklarna 17 och 18.4 i direktiv (EU) 2015/849 för kundkännedom och de faktorer som kreditinstitut och finansiella institut bör beakta vid bedömning av den risk för penningtvätt och finansiering av terrorism som förknippas med enskilda affärsförbindelser och enstaka transaktioner (riktlinjer för riskfaktorer avseende penningtvätt och finansiering av terrorism) som upphäver och ersätter riktlinjerna JC/2017/37, EBA/GL/2021/02 (Eba:s riktlinjer för riskfaktorer).

I denna andra upplaga har vägledningen omarbetats och utvecklats. Ett avsnitt om klientmedelskonton har lagts till.

1. Inledning

Syftet med denna vägledning är att den ska vara ett stöd för banker i arbetet med den allmänna riskbedömningen i praktiken. Vägledningen är inte avsedd att användas som en mall. Den allmänna riskbedömningen och metoden för att göra denna måste alltid anpassas efter den egna verksamheten.

Vägledningen ska läsas tillsammans med den grundläggande vägledningen om allmän riskbedömning. I den grundläggande vägledningen finns en redogörelse för de regelverkskrav som ställs vad gäller den allmänna riskbedömningen. I den grundläggande vägledningen finns också en metodbeskrivning och begreppskatalog, som kan användas som stöd i arbetet. Några processfrågor tas också upp där. Även andra delar av vägledningen, t.ex. vägledningen om allmän riskbedömning för finansbolag respektive på värdepappersområdet, kan vara relevanta för banker.

Penningtvätts- och terrorismfinansieringsrisker i banksektorn kan variera mycket. I denna vägledning finns några exempel på hot och sårbarheter som kan påverka risken med produkter och tjänster som kan användas för sparande, belåning och betalning. Vägledningen är något kategoriskt uppdelad mellan dessa områden, trots att det i praktiken ofta är så att en produkt eller tjänst kan ha flera användningsområden. Produkter och tjänster kan dessutom ha ett nära samband eller beroenden till varandra samt vara utformade på olika sätt.

Vägledningen omfattar också några exempel på produkter och tjänster. Syftet med exemplen är att illustrera riskfaktorer som kan beaktas i riskbedömningen. Exemplen omfattar bl.a. en beskrivning av avvikande kundbeteenden. Det är dock viktigt att banken själv avgör vad som anses vara ett avvikande kundbeteende och vilken misstankegrad detta innebär. Exemplen är inte uttömmande och kan inte användas som en mall. Varje bank måste alltid utgå från hur de egna produkterna och tjänsterna är utformade och de riskfaktorer som är relevanta för verksamheten.

Med produkter avses i denna vägledning både produkter och tjänster, om inget annat anges.

1.1 Några allmänna utgångspunkter

För att bedöma den inneboende risken måste banken analysera hur de egna produkterna skulle kunna utnyttjas för penningtvätt eller finansiering av terrorism. Detta kan beskrivas som hotet. Bedömningen kan göras utifrån olika aktiviteter som kan vara del av penningtvätts- och terrorismfinansieringsupplägg. Det handlar om värdeomvandlande aktiviteter, värdeöverförande och värdeförflyttanden aktiviteter, värdebevarande aktiviteter samt värdegenererande aktiviteter.

Som en del av riskanalysen bör banken även bedöma varför produkten är mer eller mindre attraktiv för penningtvätt och finansiering av terrorism och vad som kan påverka bankens förmåga att upptäcka misstänkt penningtvätt och finansiering av terrorism i förhållande till de olika aktiviteterna. Detta kan beskrivas som sårbarheten. Banken behöver också identifiera vilka åtgärder eller kontroller som motverkar att ett utnyttjade sker.

Om en produkt inte möjliggör någon eller några av de beskrivna aktiviteterna behöver banken naturligtvis inte analysera vilka faktorer som kan påverka bankens möjlighet att upptäcka penningtvätt eller finansiering av terrorism i förhållande till den aktuella aktiviteten.

1.2 Faktorer som kan påverka risken

I tabellen nedan beskrivs några riskfaktorer som kan vara relevanta för flera av bankens produkter och tjänster och som generellt sett kan öka respektive minska risken för penningtvätt och finansiering av terrorism.

När risken är förhöjd ska åtgärder vidtas för att mitigera risken. Banken kan behöva vidta skärpta åtgärder för kundkännedom, vilket bl.a. omfattar att inhämta ytterligare uppgifter, såsom uppgifter om varifrån medlen kommer (medlens ursprung). Möjligheten att bedöma uppgifter om medlens ursprung är ett exempel på något som bör beaktas i riskbedömningen. Banken kan också behöva skärpa övervakningen (monitoreringen) av kundens transaktioner.

Faktorer som kan öka risken
Kunden kan göra transaktioner på egen hand på distans.[1] Detta kan medföra att bankens medarbetare inte har möjlighet att ställa kompletterande kundkännedomsfrågor och frågor om transaktionen innan transaktionen sker.
Det saknas ett tydligt och rimligt syfte med kundens användning av produkten.
Bristande information om medlens ursprung. Det förekommer t.ex. att gärningspersoner använder falska underlag för att dölja brottsvinster och i vissa fall också för att öppna målvaktskonton. Det förekommer även att äkta skuldebrev återanvänds för att legitimera överföringar.[2]
Gränsöverskridande aktiviteter. Detta är något som kan minska spårbarheten. Även möjligheten att utreda kundens ägarstruktur och verklig huvudman kan försvåras.
Kontanthantering, både insättningar och uttag, särskilt kontantuttag i konfliktområden eller angränsande länder. Kontanter har en hög grad av anonymitet och en mycket begränsad spårbarhet.
Betalningar eller insättningar från tredje part, t.ex. amorteringar från konto som tillhör tredje part. Betalningar från tredje part kan innebära en begränsad spårbarhet.
Begränsningar i interna system för att t.ex. följa kundens aktiviteter. Banken bör bl.a. analysera sina interna system och bedöma om det finns brister i bankens möjlighet att tydligt följa t.ex. kundens värdeomvandlande aktiviteter såsom köp och försäljningar av fonder och värdepapper.

Faktorer som kan minska risken
Syftet med kundens användning av produkten är tydligt och rimligt.
Medlens ursprung är tydligt och rimligt.
Olika begränsningar, t.ex. beloppsbegränsningar samt begränsningar gällande uttag och insättning. Detta är faktorer som kan göra produkten mindre attraktiv för penningtvätt och finansiering av terrorism. Det gäller även när det ställs särskilda krav för att få tillgång till och kunna nyttja produkten.

[1] Här kan också risken för id-stölder eller s.k. utnyttjade identiteter uppmärksammas. Risken för att kunden agerar med en stulen identitet kan öka när banken möter kunden på distans (och minska när banken träffar kunden i fysiskt möte). Id-stölder handlar om att någons identitet används av en annan person för olika brottsliga upplägg, vanligtvis genom e-legitimation. Se Finanspolisen informerar: Varning för penningtvätt genom utnyttjade identiteter, september 2018.

[2] Finanspolisen informerar: Lån och Falska skuldebrev, november 2022.

2. Exempel på hot och sårbarheter i förhållande till produkter och tjänster som kan användas för sparande

2.1 Värdeomvandlande aktiviteter

Produkter och tjänster för sparande (sparprodukter) kan användas i värdeomvandlande syfte, exempelvis för köp och försäljning av fonder och värdepapper eller valutaväxling.

Gärningspersonerna kan använda sektorns legitima produkter. Exempel på detta är köp och försäljning av fondandelar med syftet att skikta eller integrera medel som har ursprung i brottslig verksamhet. På så sätt kan mottagaren ge sken av att pengarna kommer från upparbetade kapitalvinster.[3]

Värdepapper kan t.ex. användas för att integrera och placera brottsvinster.[4] Vid en försäljning skapar det bakomliggande värdepappret en legitimitet till innehavet av pengarna. Handel med värdepapper kan även utnyttjas för vissa förbrott, såsom insiderhandel och marknadsmissbruk, där de vidare transaktionerna med brottsvinsten är att betrakta som penningtvätt.

Banken bör utreda om det genom sparprodukten är möjligt att handla med icke marknadsnoterade värdepapper. Det kan finnas särskilda sårbarheter kopplade till denna typ av handel, främst på grund av bristen på genomlysning avseende de bolag vars aktier handeln avser. Icke marknadsnoterade värdepapper förekommer exempelvis vid investeringsbedrägerier.

2.2 Värdeöverförande och värdeförlyttande aktiviteter

Sparprodukter kan användas i värdeöverförande och värdeförflyttande syfte. Banköverföringar, betalningsförmedling över mobilapp och bankomatuttag är vanligt förekommande aktiviteter i penningtvättsupplägg.[5] Banken bör analysera vilka möjligheter till överföring, insättning, och uttag som är kopplade till sparprodukten. Begränsningar i dessa avseenden är exempel på sådant som kan minska risken. Exempelvis kan bindningstider och beloppslimiter göra produkten mindre attraktiv för penningtvätt och finansiering av terrorism.

Vad gäller kontoöverföringar påverkas risken även av vilka typer av överföringar som är möjliga för kunden att göra. Överföringstjänster där kunden själv kan göra överföringar utan begränsningar innebär typiskt sett en ökad möjlighet till stora eller frekventa överföringar, vilket är något som kan ses som attraktivt ur ett penningtvätts- eller terrorismfinansieringsperspektiv. Risken kan också öka om det är möjligt för kunden att göra överföringar till andra personers konton, eftersom skiktningsåtgärder ofta syftar till att ändra uppgift om innehavaren av medlen.

Banken bör även bedöma möjligheten till värdepappersflyttar till någon annan genom t.ex. gåva eller arv, om sparprodukten medger detta, och om det finns begränsningar gällande denna typ av överföring.

[3] Den nationella riskbedömningen av penningtvätt och finansiering av terrorism i Sverige 2020/2021 avsnitt 7.7.
[4] Se Eba:s: riktlinjer för riskfaktorer (EBA/GL/2021/02) riktlinje 15, som är sektorsspecifik för värdepappersföretag. Se också avsnitt 7.3 i den nationella riskbedömningen av penningtvätt och finansiering av terrorism i Sverige 2020/21, som handlar om värdepappersrörelse. Se även Simpts vägledning om allmän riskbedömning på värdepappersområdet.
[5] Jfr den nationella riskbedömningen av penningtvätt och finansiering av terrorism i Sverige 2020/2021 s. 18.

2.3 Värdebevarande aktiviteter

Sparprodukter kan vanligtvis användas i värdebevarande syfte för exempelvis lagring av brottsvinster. Sparande kan också vara en finansieringskälla för terrorism.

En av de främsta riskfaktorerna kopplade till värdebevarande aktiviteter är bristande information om medlens ursprung. Särskilda svårigheter att utreda detta kan uppstå vid gränsöverskridande förbindelser. Medlens ursprung kan också vara svårt att utreda när det gäller förmögenheter, särskilt sådana som har byggts upp över tid och där det kan finnas flera källor till medlens ursprung, vilket kan göra ursprunget mer komplext och oöverskådligt.

Värdebevarande aktiviteter kan genomföras i placeringsstadiet, t.ex. när pengarna investeras. Det kan vara lättare att investera brottsvinster i finansiella produkter när pengarna redan finns i det finansiella systemet. Här bör det även beaktas att vissa kunder kan ha hög kompetens och använda sig av komplicerade upplägg.[6] Förekomsten av professionella penningtvättare är en annan faktor att beakta.[7]

2.4 Värdegenererande aktiviteter

Sparprodukter skulle kunna medge värdegenererande aktiviteter, något som kan vara möjligt om sparprodukten medger exempelvis värdepappersbelåning.

2.5 Tabell med exempel

Tabellen innehåller exempel på hotaktiviteter, sårbarheter och åtgärder för att mitigera riskerna.

Möjlig hotaktivitet	Exempel på sårbarhet	Exempel på åtgärd
Kontoöverföring med syftet att skikta eller integrera medel som har ursprung i brottslig verksamhet	Möjligheten för kunden att själv göra överföringar till andra personers konton utan begränsningar, särskilt om de kan genomföras snabbt.	Införa begränsningar, t.ex. av belopp och möjligheten att göra överföringar till andra personers konton.
Investeringar, t.ex. köp av fondandelar med syftet att skikta eller integrera medel som har ursprung i brottslig verksamhet.	Möjlighet att köpa fondandel (göra en investering) direkt, utan att transaktionen går via ett konto i banken som tillhör kunden.	Åtgärder för skärpt kundkännedom för att utreda medlens ursprung.

[6] Jfr den nationella riskbedömningen av penningtvätt och finansiering av terrorism i Sverige 2020/2021 s. 63.
[7] Se Polismyndighetens, finanspolissektionen, rapport Professionella penningtvättare Branscher, modus och kopplingar till kriminella nätverk, mars 2024.

2.6 Exempel på produkter och tjänster för sparande

2.6.1 Sparkonto

2.6.1.1 Allmän beskrivning av sparkonto

Sparkonto är en av de mest grundläggande produkterna som banker erbjuder. Produkten riktar sig ofta till privatkunder med en lägre riskaptit där investeringar i t.ex. värdepapper av olika skäl inte har bedömts vara en lämplig sparform. Beroende på ränteläget kan ett sparkonto också vara intressant för andra kundkategorier.

Ett sparkonto kan normalt sett tecknas på distans och beroende på hur banken tar in nya kunder kan det vara enkelt för en privatperson att öppna ett sparkonto.

I Sverige finns i dag varken förmögenhetsskatt, arvsskatt eller gåvoskatt, vilket skulle kunna öka produktens attraktivitet internationellt sett. Samtidigt kan sådant som begränsningar vad gäller uttag och andra produktvillkor göra produkten mindre attraktiv för penningtvätt och finansiering av terrorism. Det bör dock samtidigt beaktas att den som vill tvätta pengar kan förmodas vara mindre känslig för sådant som produktvillkor och skatter, eftersom huvudsyftet inte är att göra bra placeringar.

När det finns möjlighet att koppla andra produkter och tjänster till ett sparkonto, t.ex. möjligheten att göra olika typer av transaktioner, bör det beaktas i riskbedömningen.

2.6.1.2 Särskilt relevanta hotaktiviteter

Värdeomvandlade aktiviteter, penningtvätt: Sparkontot är sannolikt en något mindre attraktiv produkt för penningtvätt, eftersom det inte erbjuder några större möjligheter att omvandla värden eller har några specifika fördelar jämfört med t.ex. ett transaktionskonto, som möjliggör värdeöverförande aktiviteter.

Värdebevarande aktiviteter, penningtvätt och finansiering av terrorism: Insättningar på ett sparkonto, både i form av kontanter och överföringar, är exempel på värdebevarande aktiviteter.

Sparkonto kan fungera som uppsamlingskonto vid terrorismfinansiering. Medlens ursprung är ofta legitimt och sparkontot som värdebevarare kan därför utgöra ett större hot gällande terrorismfinansiering än penningtvätt.

2.6.1.3 Särskilt relevanta sårbarheter

Det faktum att ett sparkonto ofta kan öppnas utan kontakt med bankens personal, kan ge en känsla av anonymitet och därmed öka produktens attraktivitet både vad avser penningtvätt och finansiering av terrorism. Även möjligheten för tredje part att göra insättningar kan öka attraktiviteten.

Terrorismfinansiering kan utföras genom insamling av medel, som skickas vidare utomlands. Insamlingen kan ske under en begränsad tid för att uppnå ett visst belopp. Ett sparkontos funktion är typiskt sett att löpande ta emot insättningar. Normalt sett bör relativt få uttag ske. Eftersom dessa funktioner och sätt att använda kontot på, stämmer väl överens med hur terrorismfinansiering kan gå till, kan det bidra till begränsade möjligheter att upptäcka ett utnyttjande i det syftet.

2.6.1.4 Särskilt relevanta avvikande kundbeteenden

Det kan vara svårt att upptäcka finansiering av terrorism eftersom det ofta rör sig om mindre belopp med legitimt ursprung. I allmänhet kan en ovilja att förklara eller försök att dölja medlens ursprung vid insättningar på sparkontot vara en riskfaktor.

En annan riskfaktor kan vara om det sker många insättningar på kontot från andra personer eller betalningsavsändare än kontohavaren.

3. Exempel på hot och sårbarheter i förhållande till produkter och tjänster som kan användas för belåning

Faktorer som kan påverka riskbedömningen av produkter och tjänster som kan användas för belåning (låneprodukter) är exempelvis olika typer av limiter och beloppsbegränsningar eller om kunden måste ha en annan produkt för att kunna ansöka om låneprodukten. Vilka möjligheter till utbetalning som låneprodukten medger är en annan faktor som kan påverka risken. Exempelvis bör risken normalt sett vara mindre om utbetalning endast kan ske till ett av kundens konton i banken än om lånet kan utbetalas till ett externt konto i utlandet.

Även den distributionskanal genom vilken produkten förmedlas kan påverka risken, exempelvis om ansökan, kreditprövning och utbetalning av ett lån sker på distans utan interaktion med en fysisk person på banken.

3.1 Värdeomvandlande aktiviteter

Många låneprodukter går inte att använda i värdeomvandlande syfte, men ett lån kan i sin tur användas för värdeomvandlande aktiviteter. Lånet kan exempelvis användas till köp av tillgångar och därmed omvandlas värdet. Lånet kan sedan betalas av med medel som har genererats på brottslig väg. På detta sätt kan en aktör tillgodogöra sig pengar med ursprung från en illegal aktivitet. Ett scenario kan vara att en person på kort tid får flera blancolån utbetalda till sitt konto varefter pengarna används till inköp av större kapitalvaror. Genom att amortera på lånen med pengar från brottslig verksamhet (integrering) tvättas pengarna.[8]

3.2 Värdeöverförande och värdeförflyttande aktiviteter

Låneprodukter kan användas i värdeöverförande syfte, exempelvis i syfte att föra beloppet till ett högriskland. En annan aktivitet kan bestå i att någon annan än låntagaren återbetalar lånet.

3.3 Värdebevarande aktiviteter

Låneprodukter används vanligtvis inte i värdebevarande syfte, men det kan ändå finnas metoder att utnyttja låneprodukter som ett led i penningtvätt eller finansiering av terrorism där värdet av de illegala medlen bevaras. Banken bör därför analysera om det är möjligt att utnyttja dess låneprodukter som ett led i exempelvis penningtvätt utan att det är fråga om ett värdeomvandlande, värdeöverförande eller värdegenererande syfte.

[8] Jfr den nationella riskbedömningen av penningtvätt och finansiering av terrorism i Sverige 2020/2021 avsnitt 7.10.

3.4 Värdegenererande aktiviteter

Låneprodukter kan användas i värdegenererande syfte. Det har förekommit att konsumentkrediter tas i eget namn eller annans (närstående) för att finansiera resor till länder i eller i närheten av konfliktområde. Då det är möjligt att låna från olika kreditgivare kan beloppen bli stora. Krediterna har sedan använts för att aktören ska kunna lämna landet utan avsikt att komma tillbaka.[9]

Bankens åtgärder och kontroller för att mitigera riskerna kan omfatta uppgifter och dokument som förekommer under kreditgivningen. Om uppgifter som hämtas in inom ramen för kreditbedömningen också används som uppgifter för kundkännedom, måste de dock hanteras enligt penningtvättslagen, vilket bl.a. innebär att de ska bevaras enligt bestämmelserna i 5 kap. penningtvättslagen (se också vägledningen om kundkännedom för finansbolag).

Under 2021 rapporterade Finanspolisen att de sett att kluster av individer på kort tid upptagit bolån med falska underlag hos samma bank.[10] Det kan vara förfalskade löneintyg och manipulerade kontoutdrag. Falska underlag kan användas i syfte att ge sken av en viss kreditvärdighet. I rapporten beskrivs också olika upplägg, bl.a. lånebedrägerier via målvakt där det saknas avsikt att betala skulden och upplägg där fastigheten övervärderas.

Konsumentkrediter är ett annat exempel där falska handlingar förekommer. Denna typ av krediter kan dessutom vara lättillgängliga för hotaktörer, eftersom ansökan ofta kan göras digitalt och utbetalning går snabbt. Kända tillvägagångssätt är falska handlingar för att uppnå kreditvärdighet, såsom förfalskade kontrolluppgifter. Ur ett penningtvättsperspektiv anses dock inte volymerna vara av betydande omfattning. Ur ett terrorismfinansieringsperspektiv anses det däremot vara förhållandevis stora belopp som kan frigöras av enskilda kredittagare.[11]

3.5 Tabell med exempel

Tabellen innehåller exempel på hotaktiviteter, sårbarheter och åtgärder för att mitigera riskerna.

Möjlig hotaktivitet	Exempel på sårbarhet	Exempel på åtgärd
Kunden upptar ett lån i syfte att finansiera terrorism.	Möjligheten att göra utlandstransaktioner till land som angränsar till aktivt konfliktområde. Möjligheten att göra kontantuttag i konfliktområde eller land som angränsar till konfliktområde.	Skärpta åtgärder för kundkännedom om kunden tar flera lån på kort tid eller om det har skett flera låneliknande transaktioner på kundens konto(n) under kort tid.
Illegala medel används för återbetalning eller extraamortering av ett bolån.	Möjligheten att amortera ett lån från ett konto som tillhör någon annan än kunden.	Skärpta åtgärder för kundkännedom och skärpt övervakning om amortering sker

[9] Den nationella riskbedömningen av penningtvätt och finansiering av terrorism i Sverige 2020/2021 s. 42 och 76.
[10] Finanspolisen informerar: Penningtvätt via fastigheter, februari 2021.
[11] Jfr den nationella riskbedömningen av penningtvätt och finansiering av terrorism i Sverige 2020/2021 avsnitt 7.10.

		från konto som tillhör någon annan än kunden. Det gäller även om kunden har högre amorteringstakt än vad som är rimligt i förhållande till kundens inkomst eller om kunden gör extraamortering utan rimligt förklaring.

3.6 Exempel på produkter och tjänster för belåning

3.6.1 Blancolån

3.6.1.1 Allmän beskrivning av blancolån

Långivning genom blancolån sker i regel till privatpersoner som är bosatta i det land där produkten erbjuds. Produktens utformning är vanligtvis ett konsumtionslån utan någon säkerhet knuten till lånet.[12]

Affärsförbindelser inleds ofta på distans, där den sökande ansöker om lån via internet (webb eller app) direkt hos banken eller hos någon av de etablerade kreditförmedlare som finns på marknaden. Det är vanligt att beslut meddelas relativt omgående efter ansökan och att utbetalning av lånet sker i nära anslutning till att kunden har signerat skuldebrevet.

Produkten får anses vara allmänt tillgänglig, d.v.s. det ställs inte höga, särskilda krav på kunden. De grundläggande kraven brukar generellt sett vara att sökanden inte har obetalda skulder hos Kronofogden, är folkbokförd i landet där produkten erbjuds och har en stadigvarande inkomst.

Produktens utformning och konkurrensen mellan aktörer bidrar till att förtidslösen generellt sett är vanligt förekommande.

3.6.1.2 Särskilt relevanta hotaktiviteter

Produkten blancolån kan av följande skäl vara attraktiv för personer som vill tvätta pengar genom att dölja pengarnas egentliga ursprung.

- Produkten anses vara allmänt tillgänglig.
- Det krävs ingen särskild förmåga hos hotaktören.
- Ansökningsprocessen är ofta digital och det går ofta fort både att inleda affärsförbindelsen och att få lånet utbetalt.
- Banken behöver inte känna kunden sedan tidigare eller på ett ekonomiskt övergripande sätt.

[12] Se också vägledningen om allmän riskbedömning för finansbolag.

Mot bakgrund av de skäl som anges ovan finns det en risk för att kunden tar flera mindre lån hos olika aktörer under en begränsad tidsperiod för att sedan genom återbetalning använda tillgångar kopplade till olika former av brottslig verksamhet, se också nedan under sårbarheter.

I likhet med vad som kan fallet vid exempelvis bolån, kan falska intyg förekomma i samband med att blancolån tas.[13] Intyget, t.ex. ett falskt arbetsgivarintyg, kan användas i syfte att styrka medlens ursprung eller uppvisa kreditvärdighet.

Värdeomvandlande aktiviteter, penningtvätt: De pengar som kunden lånar kan användas för att tillföra en brottslig verksamhet tillgångar, exempelvis via uppstart av företag, betalning av ”svarta” löner eller transaktioner kopplade till falska fakturor. De utbetalda pengarna kan också användas till inköp av större kapitalvaror eller andra typer av investeringar.[14]

Lånet kan betalas tillbaka med tillgångar som kommer från intäkter som inte har deklarerats eller beskattats eller andra tillgångar med illegalt ursprung. Genom att amortera på lånet med pengar från brottslig verksamhet (integrering) kan pengarna tvättas.[15]

Värdeöverförande aktiviteter, penningtvätt och finansiering av terrorism: Ett lån kan tas i syfte att föra beloppet till ett högriskland.

Värdegenererande aktiviteter, finansiering av terrorism: Lån kan tas i eget namn eller annans (närstående) för att finansiera resor till länder i eller i närheten av konfliktområden. Eftersom det är möjligt att ta lån hos olika långivare kan beloppen bli stora i jämförelse med de låga belopp som annars förekommer vid finansiering av terrorism.[16]

3.6.1.3 Särskilt relevanta sårbarheter

Banker har inte alltid en helhetsrelation till kunden och kan då inte följa alla de aktiviteter som kunden gör. En begränsad insyn är något som kan göra blancolån attraktiv för penningtvätt eller finansiering av terrorism.

Blancolån kan, under en begränsad tidsperiod, utnyttjas hos fler långivare samtidigt utan att de har kännedom om detta. Detta kan medföra att banken missar uppgifter som är relevanta för kundkännedomen. Amorteringar kan också i vissa fall göras av andra personer än låntagaren. Syftet kan vara att dels öka volymen av pengar som integreras, dels minska upptäcktsrisken då inga stora flöden av pengar sker hos samma långivare eller via den bank där låntagaren har sina huvudsakliga konton. Låneutbetalningsunderlag kan också användas med syftet att lämna en förklaring till att ursprunget till större överförda belopp är legalt.[17]

Ovan beskrivs att falska intyg kan användas för att ansöka om blancolån. För att minska sårbarheten för detta kan personalen i banken behöva ha utbildning för att kunna göra en bedömning av intyg och andra underlag.

En person som avser att tvätta pengar vill ofta ha möjlighet att snabbt kunna inleda och avsluta affärsförbindelser. En sådan person är därför i regel mer känslig för begränsningar i fråga om löptider och

[13] Jfr den nationella riskbedömningen av penningtvätt och finansiering av terrorism i Sverige 2020/2021 s. 79.
[14] Den nationella riskbedömningen av penningtvätt och finansiering av terrorism i Sverige 2020/2021 s. 75.
[15] Den nationella riskbedömningen av penningtvätt och finansiering av terrorism i Sverige 2020/2021 s. 75.
[16] Jfr den nationella riskbedömningen av penningtvätt och finansiering av terrorism i Sverige 2020/2021 s. 76.
[17] Den nationella riskbedömningen av penningtvätt och finansiering av terrorism i Sverige 2020/2021 s. 75.

lånebelopp samt för den tid det tar att inleda affärsförbindelsen, än för faktiska kostnader för lånet. Även kundens möjlighet att kunna förtidslösa lånet kan innebära en betydande sårbarhet.

3.6.1.4 Särskilt relevanta avvikande kundbeteenden

Personer som avser att tvätta pengar eller finansiera terrorism är i regel mindre känsliga för ränta och andra kostnader än för andra faktorer som påverkar den rörelsefrihet som en produkt kan innebära. Detta innebär att extra uppmärksamhet bör riktas mot de kunder som har korta affärsförbindelser med banken och de som nyttjar produkttypen flera gånger under en kortare period.

Om en kund tar ett lån och återbetalar detta kort därefter för att sedan ansöka om ett nytt lån nära inpå den tidigare återbetalningen, kan det vara ett tecken på att kunden önskar skapa flera större transaktioner i syfte att dölja medlens ursprung.

Om en kund gör större inbetalningar som endast delvis löser lånet, för att kort därefter ansöka om en utökning av lånet, kan det vara ett tecken på ett försök att dölja tillgångar med illegalt ursprung.

Kundens återbetalningsbeteende bör bedömas utifrån det syfte som kunden har angett med lånet. Exempelvis kan banken ha en lägre misstankegrad mot återbetalningar som görs närmare inpå utbetalning av ett nytt lån, när syftet har uppgetts vara del av ett överbryggningslån, än mot återbetalningar av lån där syftet förväntas innebära en längre återbetalningstid.

Kundbeteenden som bör uppmärksammas är när kunden önskar få utbetalning av ett lån till en annan persons konto, att utbetalningen ska delas upp i flertalet mindre transaktioner och/eller att kunden önskar utbetalning till ett konto i utlandet. Banken bör också vara uppmärksam på om det framkommer uppgifter som tyder på att kunden kan ha upptagit flera lån hos andra kreditinstitut kort innan ansökningstillfället.

3.6.2 Kreditkort

3.6.2.1 Allmän beskrivning av kreditkort

Kreditkort är en form av betalningsmedel. Kortet kan användas i fysiska butiker eller vid köp på internet. De flesta kort som erbjuds är VISA eller MasterCard och korten kan ofta användas i de flesta delar av världen.

Eftersom kortet är förenat med en kredit görs normalt sett en kreditprövning. Produkten erbjuds oftast till kunden via ett bankkontor, distansansökan eller tredje part.

3.6.2.2 Särskilt relevanta hotaktiviteter

Värdeomvandlande aktiviteter, penningtvätt och finansiering av terrorism: Det huvudsakliga hotet i relation till kreditkort är aktiviteter som möjliggör omvandling av ett värde genom att krediten återbetalas med brottsligt förvärvade medel (penningtvätt). Kreditkortet kan även användas för att få tillgång till kontanter och därmed minska spårbarheten i en transaktion (både penningtvätt och finansiering av terrorism).

Värdeöverförande och värdeförflyttande aktiviteter, penningtvätt och finansiering av terrorism: Ett kreditkort kan användas till aktiviteter som syftar till att överföra eller förflytta ett värde. Kortet kan användas av någon annan än kortinnehavaren. Ett värde kan också överföras mellan personer eller

företag genom att någon annan än kortinnehavaren betalar fakturan/återbetalar krediten. Kreditkort är dessutom lätta att transportera och använda över nationsgränser, vilket ökar dess attraktivitet, eftersom detta kan försvåra brottsutredningar.

Värdebevarande aktiviteter, penningtvätt och finansiering av terrorism: Ett kreditkort kan användas på ett värdebevarande sätt genom att kortinnehavaren gör inbetalningar som leder till ett positivt saldo.

Värdegenererande aktiviteter, finansiering av terrorism: Kreditkort kan användas för att generera ett värde genom att krediten frigör pengar som kan användas för illegala ändamål, i likhet med exempelvis blancolån.

3.6.2.3 Särskilt relevanta sårbarheter

Enligt bl.a. Finanspolisen[18] och Wolfsberg Group[19] kan följande sårbarheter vara relevanta för kreditkort:

• Möjligheten att få kontanter, särskilt i andra länder och i flera valutor.

• Möjlighet att ha extrakortsinnehavare.

• Möjlighet att använda kreditkortet för att skicka pengar till andra kortinnehavare.

• Möjlighet att betala krediten med kontanter eller motsvarande värden.

• Möjlighet för en tredje part att betala krediten.

• Möjlighet att få ett kreditkort omedelbart genom exempelvis en butik (denna riskfaktor är relevant även vad gäller distributionskanaler).

3.6.2.4 Särskilt relevanta avvikande kundbeteenden

Enligt bl.a. Finanspolisen och Wolfsberg Group (se avsnitt 3.6.2.3) kan bl.a. följande faktorer, som är av mer generell karaktär, vara relevanta vid inledandet av en affärsförbindelse:

• Informationen i ansökan är inkonsekvent.

• Informationen i ansökan stämmer inte med offentliga uppgifter.

• Osäkerhet avseende sökandens identitet.

Vissa faktorer i relation till kundbeteende är relevanta under en pågående affärsförbindelse. Dessa faktorer är mer specifikt relaterade till produktens karaktär och omfattar bl.a. följande.

• Återkommande uttag av kontanter genom kreditkortet. Omvandlingen av värdet, från kredit till kontanter, kan bidra till minskad spårbarhet. Uttag kan även användas för att skaffa tillgångar som kan användas inom ramen för ekonomisk brottslighet eller terrorismfinansiering.

• Uttag av höga summor kontanter i utlandet. Kreditkort är lätta att transportera över nationsgränser samtidigt som det är svårare för brottsutredande myndigheter att utreda brott över nationsgränser.

[18] Finanspolisen informerar: Penningtvätt genom betalkort, juni 2020.
[19] Wolfsberg AML Guidance on Credit/Charge Card Issuing and Merchant Acquiring Activities, 2009.

• Inbetalningar som överskrider krediten. Detta tillvägagångssätt kan användas för att gömma tillgångar. Det kan också användas som en form av överföring om inbetalningen görs av tredje part och sedan återbetalas till kortinnehavaren.

• Ovanliga köp av produkter eller tjänster i länder med högre risk för penningtvätt eller terrorismfinansiering.

• Privata köp på företagskort.

• Innehav av kort som kan användas för att omvandla kryptovaluta till annan valuta, s.k. crypto-to-plastic.

• Flera eller återkommande betalningar från utlandet, utan rimlig förklaring eller utan att kunden har en naturlig koppling till detta land.

• Fakturor betalas av tredje part utan naturlig koppling till kunden (naturlig koppling kan exempelvis vara make, maka, partner och sambo).

Ett scenario beträffande kort och penningtvätt är att en kund köper en vara kontant för en större summa pengar, exempelvis 80 000 kr. Dagen efter återkommer kunden vid öppningstid och har ångrat sig. Butiken har inte 80 000 kr i kontanter utan ombeds att sätta in pengarna på kortet.

3.6.3 Bolån

3.6.3.1 Allmän beskrivning av bolån

En fastighet eller en bostadsrätt kan utgöra säkerhet både för ett banklån och för hypotekslån. Som samlingsnamn används begreppet bolån.

Ett banklån har ingen räntebindningstid och kan extraamorteras eller lösas vid vilken tidpunkt som helst.

Ett hypotekslån har en räntebindningstid som normalt sett varierar mellan 3 månader och 10 år. Beroende på kvarvarande löptid varierar kostnaden för att göra en extraamortering eller att lösa lånet i sin helhet.

Bolån beviljas i regel enbart till privatpersoner som är bosatta i det land där produkten erbjuds. Vanligtvis tar en person ett bolån för att finansiera ett köp av en fastighet eller en bostadsrätt, men det kan också vara för att bekosta en utbyggnad eller renovering av bostaden eller avse inköp av kapitalvaror.

I huvudsak ges lån till fysiska personer som vill belåna en fastighet eller en bostadsrätt i Sverige, men det förekommer att säkerheten utgörs av utländska objekt.

Både traditionella banker, banker utan kontor och bolåneinstitut erbjuder fysiska personer bolån. Ibland krävs det att låntagaren kommer in på ett bankkontor och undertecknar handlingarna och ibland kan personen göra det på annan plats för att sedan skicka in reversen.

3.6.3.2 Särskilt relevanta hotaktiviteter

Det förekommer falska intyg i samband med bolån. Upplägget kan vara att personerna har lågt taxerade inkomster som inte gjort dem kreditvärdiga för ett bolån. I låneansökningarna uppger de att de har påbörjat en fast anställning och inkommer med arbetsgivarintyg för att styrka detta. De inblandade företagen kan användas för att erbjuda kreditvärdighet till personer som t.ex. arbetar svart eller lever av kriminell verksamhet. Lånet kan sedan komma att amorteras med brottsvinster.[20]

Värdeomvandlande aktiviteter, penningtvätt: Genom att uppta ett lån med en fastighet/bostadsrätt som säkerhet kan medel frigöras för olika inköp och därmed omvandlas värdet. Lånet kan sedan återbetalas med pengar från brottslig verksamhet.

Värdeöverförande aktiviteter, finansiering av terrorism: Genom att köpa fastighet/bostadsrätt kan pengar överföras till säljaren. En person som avser att finansiera terrorism kan vara intresserad av att överföra pengar till den som ska utföra ett terrorbrott. Det är dock mindre troligt att den transaktionen kommer att göras i form av ett fastighetsförvärv. Belåning i samband med fastighetsförvärv innebär ofta en långsiktighet som gör produkten mindre attraktiv för att finansiera terrorism, eftersom avyttrandet av egendomen kan ta tid. Utökning av lån på befintlig fastighet eller bostadsrätt (när det finns sådant utrymme) kan dock vara mer attraktivt för detta syfte.

Värdebevarande aktiviteter, penningtvätt: Investering av brottsvinster i en fastighet/bostadsrätt kan innebära värdebevaring och sannolikt även värdeökning. Brottsvinsterna kan exempelvis användas för att köpa material eller betala arbetskraft.

Värdegenererande aktiviteter, finansiering av terrorism: Genom att belåna en fastighet/bostadsrätt kan en person frigöra medel för finansiering av terrorism.

3.6.3.3 Särskilt relevanta sårbarheter

Ett lån som kan betalas av eller amorteras vid valfri tidpunkt kan vara attraktivt för den som avser att tvätta pengar. Om personen dessutom kan göra avbetalningar eller amorteringar via internetbanken och inte behöver vara i personlig kontakt med banken, ökar även det sårbarheten då bankens medarbetare inte har möjlighet att ställa kompletterande kundkännedomsfrågor eller frågor om den specifika transaktionen innan den genomförs.

Bankens förmåga att upptäcka avvikelser vid betalning är avgörande för bankens risk. Exempelvis bör banken bedöma sin förmåga att i övervakningen upptäcka sådant som en, i förhållande till kundens betalningsförmåga, onormalt ökad amortering eller lösen relativt kort efter att lånet har tagits.

3.6.3.4 Särskilt relevanta avvikande kundbeteenden

Personer som avser att tvätta pengar eller finansiera terrorism är i regel mindre känsliga för ränta och andra kostnader, än för andra faktorer som påverkar rörelsefriheten som en produkt kan ha. Detta gör att ett bolån i form av ett banklån kan vara mer attraktivt än ett hypotekslån. Det finns hypotekslån med olika räntebindningstid. Generellt kan en längre räntebindningstid göra ett lån mindre intressant för den som avser att tvätta pengar.

[20] Den nationella riskbedömningen av penningtvätt och finansiering av terrorism i Sverige 2020/2021 s. 79. Se också Finanspolisen informerar: Falska kontrakt vid fastighetsaffärer, maj 2022, samt Finanspolisen informerar: Penningtvätt via fastigheter, maj 2022.

Exempel på riskförhöjande faktorer:

• Om en kund inte verkar visa något intresse för avgifter eller kostnader för affären.

• Om en kund önskar köpa en osedd fastighet/bostadsrätt utan att visa intresse för priset eller ytterligare detaljer om affären.

• Om en kund tar ett bolån kan det vara misstänkt om oväntade personer eller betalningsavsändare gör amorteringar, särskilt om det utan rimlig förklaring sker från utlandet.

• Om ett bolån återbetalas i sin helhet efter en mycket kort tid och utan rimlig förklaring.

• Om en kund vill öka sitt bolån (när det finns sådant utrymme) utan rimlig förklaring eller om utbetalningen följs av ett stort kontantuttag.

3.6.4 Trade Finance

3.6.4.1 Allmän beskrivning av Trade Finance

Trade finance är framför allt en tjänst för internationell handel. Genom att använda sig av tjänsten underlättas kundens finansiering och finansiella riskhantering av varor, både genom att banken tillhandahåller finansiella produkter och tjänster som möjliggör säkra och effektiva transaktioner mellan köpare och säljare och genom att affären blir säkrare då betalning sker mot uppvisande av relevanta dokument. Sättet för betalning kan skilja sig åt både nationellt och regionalt, varför det alltid är viktigt att avtala om hur och när betalning ska ske.

Banken kan tillhandahålla finansieringslösningar för både köpare och säljare. Banken kan också erbjuda en garanti till säljaren att betalning kommer att ske, så länge som säljaren uppfyller villkoren i avtalet. Banken kan även erbjuda en garanti att göra en betalning till tredje part om en kund inte uppfyller sina åtaganden enligt avtalet.

Det är inte ovanligt att en stor del av affären sker i högriskregioner eftersom trade finance till sin natur är skapad för internationell handel. Att affären till sin natur är komplex, icke-transparent och involverar hantering av uppgifter och dokumentation som kan vara omfattande, är också sådant som kan bidra till en förhöjd risk.

Vid kundförhållanden som involverar trade finance är det viktigt att utreda faktiska kundbeteenden. Det kan göras genom exempelvis stickprov. Det är också viktigt att löpande följa upp affärer och att bedriva omvärldsbevakning med hjälp av externa källor.[21] Specialistkunskaper kring historiskt misstänkta beteende och produktegenskaper är ofta av stor betydelse för riskbedömningen.

Produktens komplexa natur och svårigheten att övervaka transaktioner kan försvåra för insyn i hela flödet, vilket kan medföra att produkten blir attraktiv för penningtvätt och terrorismfinansiering.

[21] Se den rapport som Fatf och Egmont Group har tagit fram: *Trade-Based Money Laundering*, mars 2021. Rapporten handlar framför allt om hur handelstransaktioner kan utnyttjas för att flytta pengar i stället för varor. Rapporten tar upp flera riskindikatorer. Trade-Based Money Laundering Risk Indicators (fatf-gafi.org). I rapporten hänvisas också till en rapport om *Trade-Based Money Laundering* från 2006. Den rapporten tar upp såväl tillvägagångssätt som riskindikatorer och är i vissa avseenden mer detaljerad än rapporten från 2021 Trade-Based Money Laundering (fatf-gafi.org).

3.6.4.2 Särskilt relevanta hotaktiviteter

Transaktioner inom trade finance kan vara komplexa och involvera flera parter, företag och länder. Komplexa betalstrukturer är något som kan utnyttjas i syfte att dölja penningtvättsupplägg.

Trade finance kan medföra att banken behöver öppna nya förbindelser med andra banker (korrespondentbanker) för att kunna genomföra transaktionerna. Kundens motparter väljer normalt sett sin lokala bank, som kan ligga i ett högriskland. Det innebär att motpartsbanken kan vara placerad i en stat som saknar effektiva system för bekämpning av penningtvätt eller finansiering av terrorism och att banken har en kundkrets som omfattar högriskkunder.

Värdeomvandlande aktiviteter: Försäljningar av varor till överpris alternativt underpris för tillgång till medel i exempelvis högriskområden.

Värdeöverförande aktiviteter: Smuggling av pengar till högriskområden.

Värdebevarande aktiviteter: Undandragande av finansiella tillgångar.

Värdegenererande aktiviteter: Förfalskade dokument för att kringgå skatter, tullar eller för att dölja vilken vara som affären faktiskt avser.

3.6.4.3 Särskilt relevanta sårbarheter

Komplexa affärer med olagliga motiv kan medföra att bankens medarbetare som ska granska affären har svårt att se helheten och upptäcka när misstänkta transaktioner/affärer genomförs. Bankens medarbetare kan också ha svårt att se om den vara som framgår av dokumenten faktiskt har skickats.

Den omständigheten att produkten är internationell och normalt sett används i högriskländer kan locka kunder som vill kringgå regler rörande penningtvätt och finansiering av terrorism.

Eftersom det normalt sett är banken som erbjuder den produkt som finansierar affären, går inte transaktionerna rörande affären på traditionellt sätt genom transaktionssystemet. Detta medför minskade möjligheter att upptäcka inblandning av misstänkta tredje parter. Här behöver banken ha kontroller för att kunna säkerställa vem den tredje parten är.

3.6.4.4 Särskilt relevanta avvikande kundbeteenden

Det är viktigt att övervaka kunder som genomför komplexa affärer och som handlar med motparter i högriskländer. Detta gäller både från ett penningtvätts- och terrorismfinansieringsperspektiv.

Det är viktigt att kunna upptäcka transaktioner där pris, komplexitet eller kvantitet på affären inte verkar rimliga. Över- eller underprissättning är sådant som kan tyda på avvikande beteende.

Transaktioner och beteenden som avviker från historiska mönster bör utredas.[22]

[22] Se föregående fotnot om rapporter från Fatf och Egmont Group om Trade-Based Money Laundering.

4. Exempel på hot och sårbarheter i förhållande till produkter och tjänster som kan användas för betalning

4.1 Värdeomvandlande aktiviteter

Många produkter och tjänster för betalning kan användas i värdeomvandlande syfte, exempelvis för köp av tillgångar av olika slag eller för valutaväxling.

Banken bör analysera vilka olika metoder som kunden kan använda för att undgå misstankar, exempelvis genom att kunden i referenstexten på kontoöverföringen uppger att betalningen avser köp av en vara eller en skattefri ersättning som spelvinst eller gåva. Det förekommer även att företag har affärsupplägg som helt eller delvis går ut på att utföra bedrägerier genom att ställa ut eller betala falska fakturor. För att dölja pengarnas ursprung och skapa en legitim bild av företagen kan brottsvinster även delas upp och föras över mellan flera olika konton, även över flera jurisdiktioner.[23]

Utöver att försvåra spårning kan produkterna och tjänsterna för betalning också vara del av skiktningsupplägg genom andra applikationer eller tjänster. Ett exempel är att hotaktören med hjälp av betaltjänsten flyttar pengar till och från nätkasinon där pengar vinns eller förloras mellan samarbetande parter.[24]

Om det finns möjlighet att genomföra valutaväxling genom produkten eller tjänsten för betalning kan detta också uppfattas som attraktivt ur ett penningtvätts- eller terrorismfinansieringsperspektiv.[25]

Kryptovalutor möjliggör metoder för att tvätta brottsvinster och även sådan växling kan ske med hjälp av betaltjänster.[26]

Banken bör även beakta om produkten eller tjänsten för betalning möjliggör kontant betalning av en vara eller tjänst. Kontanthantering innebär generellt sett en mycket begränsad spårbarhet.

Fastighetsmarknaden anses vara attraktiv för penningtvätt. Exempelvis kan hyresintäkter användas som förklaring till medel med illegalt ursprung. Vidare kan bolån amorteras med brottsvinster, genom produkter och tjänster för betalning.[27]

4.2 Värdeöverförande och värdeförflyttande aktiviteter

Banköverföringar, betalningsförmedling över mobilapp och bankomatuttag är vanligt förekommande värdeöverförande och värdeförflyttande aktiviteter i penningtvättsupplägg.[28] Faktorer som kan påverka bedömningen av risken är exempelvis om det finns begränsningar gällande belopp och antal betalningar. Risken påverkas även av vilka typer av betalningar som tillåts. Generellt sett bör betalningar till eller från ett konto som innehas av kunden hos ett annat svenskt kreditinstitut anses som

[23] Jfr den nationella riskbedömningen av penningtvätt och finansiering av terrorism i Sverige 2020/2021 s. 109.
[24] Den nationella riskbedömningen av penningtvätt och finansiering av terrorism i Sverige 2020/2021 s. 66.
[25] Jfr den nationella riskbedömningen av penningtvätt och finansiering av terrorism i Sverige 2020/2021, bl.a. avsnitt 7.4.
[26] Staten och betalningarna, SOU 2023:16, s. 739 och Finanspolisens årsrapport 2022 s. 15.
[27] Penningtvätt via fastigheter, Fastighetsmäklare som möjliggörare, Polismyndigheten, Finanspolisinspektionen februari 2021.
[28] Jfr den nationella riskbedömningen av penningtvätt och finansiering av terrorism i Sverige 2020/2021 s. 18.

mindre riskfyllda än exempelvis betalningar till eller från utlandet, där riskerna inom EES kan vara lägre än vad de är för betalningar till eller från länder utanför EES.

Betalningsförmedlingstjänster där kunden själv har möjlighet att göra betalningar till andra personers konton utan begränsningar innebär typiskt sett en ökad möjlighet till stora eller frekventa betalningar, något som också kan ses som attraktivt ur ett penningtvätts- eller terrorismfinansieringsperspektiv.

Medlens ursprung är också en riskfaktor. Gärningspersonerna kan använda falska underlag för att dölja brottsvinster.

Banken bör också beakta om produkten eller tjänsten för betalning är knuten till en annan produkt och hur detta kan påverka risken.

4.3 Värdebevarande aktiviteter

Produkter och tjänster för betalning kan vanligtvis inte användas i värdebevarande syfte.

4.4 Värdegenererande aktiviteter

Produkter och tjänster för betalning kan användas i värdegenererande syfte, exempelvis för att samla in pengar i syfte att finansiera terrorism.

Frivilliga donationer kan ske genom att personer eller organisationer genomför insamlingskampanjer där de offentligt eller i dold regi uppmanar människor att donera pengar. I vissa fall görs det tydligt för donatorerna att pengarna är avsedda att finansiera en terroristorganisation, medan det i andra fall framställs som att donationerna är stöd i kris- och konfliktområden. Inte heller insamlaren är alltid medveten om att medlen går till att stödja terrorism, då mottagaren i utlandet kan ha misslett insamlingsorganisationen i Sverige genom en falsk beskrivning av verksamheten. Det kan även förekomma att personer och organisationer på mottagarsidan blandar någon form av legitimt arbete, t.ex. humanitärt stöd, med terrorism.[29]

Insamling kan bedrivas av stiftelser och ideella föreningar. Insamling kan även bedrivas av enskilda. En särskild sårbarhet är möjligheten att få tillräcklig information om den som samlar in medlen. Här bör särskilt beaktas vilket syfte och vilken typ av verksamhet som stiftelsen eller föreningen bedriver, vilket är information som banken bör hämta in.

4.5 Tabell med exempel

Tabellen innehåller exempel på hotaktiviteter, sårbarheter och åtgärder för att mitigera riskerna.

Möjlig hotaktivitet	Exempel på sårbarhet	Exempel på åtgärd
Kontanthantering som ett sätt att föra in eller överföra brottsvinster i det finansiella systemet.	Möjligheten att använda tjänsten för kontant betalning av en vara eller tjänst.	Skärpta åtgärder för kundkännedom. Transaktionsövervakning

[29] Se vidare den nationella riskbedömningen av penningtvätt och finansiering av terrorism i Sverige 2020/2021 avsnitt 3. Se också Eba:s riktlinjer för riskfaktorer (EBA/GL/2021/02) och bilagan till riktlinjerna som handlar om kunder som är icke-vinstdrivande organisationer (EBA/GL/2023/03).

Handel med kryptovalutor i syfte att skikta och integrera brottsvinster.	Möjligheten att göra transaktioner kopplade till kryptovaluta	Om kunden gör transaktioner kopplade till kryptovaluta: Skärpt transaktionsövervakning samt begränsning av korttransaktioner och överföringar till och från vissa plattformar

4.6 Exempel på produkter och tjänster för betalning

4.6.1 Kontanthantering

4.6.1.1 Allmän beskrivning av kontanthantering

Svenska myndigheter anser att kontanter generellt sett är starkt förknippade med höga risker för penningtvätt och finansiering av terrorism. Stora kontanta transaktioner anses ofta som misstänkta.[30]

Den organiserade brottligheten bedöms ha ett fortsatt behov av kontanta medel för att kunna omsätta brottsvinster från olika förbrott samt för illegala inköp och betalning av varor.[31]

Manuell kontanthantering möjliggör insättningar och uttag av kontanter över disk. Manuell hantering sker på bankens kontor och automatisk hantering sker där anslutna automater finns.

Eftersom kontanters ursprung är mycket svårt att verifiera och för att kontanter kan användas förhållandevis anonymt, bör extra försiktighet iakttas vid erbjudandet av denna tjänst.

4.6.1.2 Särskilt relevanta hotaktiviteter

Värdeomvandlande aktiviteter, penningtvätt: Vid insättningar omvandlas kontanter till kontomedel som kan föras vidare inom det finansiella systemet.

Värdeförflyttande aktiviteter, penningtvätt och finansiering av terrorism: Både brottsligt och legitimt intjänade pengar kan förflyttas och byta ägare utan upptäckt av kontrollåtgärder såsom transaktionsövervakning. Kontantöverföringar kan användas i kombination med andra tjänster i syfte att finansiera terrorism.

Värdebevarande aktiviteter, penningtvätt: Kontanter kan användas för att bevara vinning från brott.

4.6.1.3 Särskilt relevanta sårbarheter

Anonymiteten utgör en sårbarhet vid kontanthantering. Det är svårt att härleda och följa kontanter som förs in och ut ur det finansiella systemet, till skillnad mot transaktioner som görs mellan konton.

En konstruerad affär med förfalskade handlingar kan räcka för att brottsligt intjänade kontanter ska kunna byta ägare på ett till synes legitimt sätt. Verkar affären och de tillhörande handlingarna riktiga kan det räcka för att en insättning ska godkännas. Dessutom kan kontanter förflyttas geografiskt och

[30] Den nationella riskbedömningen av penningtvätt och finansiering av terrorism i Sverige 2020/2021 s. 14. Se också Polismyndighetens rapport Penningtvätt genom utförsel av kontanter, oktober 2023. Även norska Økokrim har publicerat en rapport om kontanter i den kriminella ekonomin: Nå er det NOK, november 2023.
[31] Den nationella riskbedömningen av penningtvätt och finansiering av terrorism i Sverige 2020/2021 s. 15.

över landgränser på ett sätt som hade kunnat upptäckas om det hade gjorts i den finansiella systemet. Det kan röra sig om brottsliga medel eller helt legitimt intjänade medel som är avsedda att finansiera terrorism. Kontanters ursprung är alltså svårt att säkerställa och förhållandevis enkelt att förfalska.

4.6.1.4 Särskilt relevanta avvikande kundbeteenden

Kunder som regelbundet hanterar större belopp i kontanter bör uppmärksammas. Om hanteringen och beloppen inte är rimliga i förhållande till kundens övriga ekonomi, finns det ytterligare skäl att agera.

Kurirer kan användas för att förmedla pengar till terroristorganisationer, vilket innebär att kontanter fysiskt transporteras över landsgränser.

4.6.2 Uttags- och insättningsautomater (kontanthantering)

4.6.2.1 Allmän beskrivning av uttags- och insättningsautomat

Uttags- och insättningsautomater fyller en viktig funktion vad gäller hantering och tillgång till kontanter. Uttags- och insättningsautomater utgör för många i samhället den mest tillgängliga formen för hantering av och tillgång till kontanter. Målgruppen är därför generellt sett bred.

Eftersom uttags- och insättningsautomater inte innebär något personligt möte medger tjänstetypen en hög grad av anonymitet. Därtill innebär kontanthantering generellt sett en mycket begränsad spårbarhet.

4.6.2.2 Särskilt relevanta hotaktiviteter

Svenska myndigheter anser att kontanter generellt sett är starkt förknippade med höga risker för penningtvätt och finansiering av terrorism. Stora kontanta transaktioner anses ofta som misstänkta.[32]

Den organiserade brottsligheten bedöms ha ett fortsatt behov av kontanta medel för att kunna omsätta brottsvinster från olika förbrott samt för illegala inköp och betalning av varor och restriktionsvaror.[33]

Värdeöverförande och värdeförflyttande aktiviteter, penningtvätt: Det huvudsakliga penningtvättshotet i förhållande till uttags- och insättningsautomater är kopplat till olika typer av aktiviteter som syftar till att överföra eller förflytta ett värde. ”Svarta” pengar kan föras in i det finansiella systemet för att påbörja penningtvätt genom kontantinsättningar i insättningsautomat.

Kontantuttag kan göras för att sedan användas för att betala svarta löner eller göra vinstuttag (skatte- och avgiftsundandragande), vilket är ett vanligt modus inom såväl högriskbranscher som inom den organiserade brottsligheten.

Insättningar kan följas av en mängd snabba överföringar, vilket gör att tillgångarna fort kan flyttas till andra konton i andra institut och länder, vilket försvårar utredningarna. Uttag kan föregås av överföringar mellan olika konton.

[32] Den nationella riskbedömningen av penningtvätt och finansiering av terrorism i Sverige 2020/2021 s. 14.
[33] Den nationella riskbedömningen av penningtvätt och finansiering av terrorism i Sverige 2020/2021 s. 15.

Värdeöverförande och värdeförflyttande aktiviteter, finansiering av terrorism: Det huvudsakliga hotet relaterat till finansiering av terrorism i förhållande till uttags- och insättningsautomater består i att personer tar ut kontanter genom kontantuttag i uttagsautomat utomlands innan de tar sig över gränsen till konfliktområden alternativt tillfälligt åker tillbaka till en lugnare gränsstad för uttag för att använda dem i terroristverksamhet. Det förekommer också att kontanter smugglas med kurirer från Sverige till konfliktområden.

4.6.2.3 Särskilt relevanta sårbarheter

Uttags- och insättningsautomater försvårar möjligheten att vidta ytterligare kontroller eftersom det inte sker något personligt möte där kompletterande frågor kan ställas.

Hanteringen av kontanter innebär en begränsad grad av spårbarhet, vilket kan utnyttjas för olika syften.

Uttag kan ofta göras globalt genom uttagsautomater som är märkta med Visa/MasterCard. Ett kort som ger möjligheter till kontantuttag kan då användas i olika länder och ge tillgång till kontanter i olika valutor.

Det finns en hög grad av rörlighet och flexibilitet relaterat till användandet. Uttagskort och tillhörande koder är lätta att flytta och kan lämnas till en annan person som därmed kan göra både insättningar och uttag, vilket medger anonymitet.

4.6.2.4 Särskilt relevanta avvikande kundbeteenden

När det gäller uttags- och insättningsautomater finns det många relevanta avvikande kundbeteenden som typiskt sett kan vara intressanta att reagera på och eventuellt utreda ytterligare:

• Många uttag/insättningar som genomförs vid flera olika automater.

• Ovanligt stora uttag/insättningar.

• Tidigare inaktivt konto som plötsligt blir aktivt, t.ex. genom ett stort kontouttag eller insättning.

• Internationella kontantuttag och – när det gäller finansiering av terrorism – särskilt uttag som görs i gränsområden till konfliktområden.

• Insättning i inhemsk valuta och uttag i utländsk valuta.

4.6.3 Swish

4.6.3.1 Allmän beskrivning av Swish

Swish är en bankgemensam tjänst för att i realtid skicka pengar via kundens mobilnummer.

Privatpersoner kan både skicka och ta emot betalningar mellan varandra, förutsatt att deras bank deltar i Swishsamarbetet.

Privatpersoner kan betala till företag, föreningar eller organisationer som har anslutit sig till Swish Företag.

Kunden måste ha ett konto i en svensk bank och måste anmäla till banken vilket mobilnummer som denne vill ansluta till Swish. Detta kan kunden göra själv på internetbanken och sedan ladda ned Swish-appen.

Vid en överföring kommer pengarna in på mottagarens konto inom några sekunder. Betalning kan göras dygnet runt, alla dagar i veckan. Det finns beloppsgränser som beslutas av respektive bank.

Det är inget krav att kunden har ett svenskt abonnemang. Även ett kontantkort eller ett utländskt abonnemang fungerar. Kunden kan byta mobilnummer hur många gånger som helst.

4.6.3.2 Särskilt relevanta hotaktiviteter

Värdeöverförande aktiviteter, penningtvätt och finansiering av terrorism: Det huvudsakliga penningtvätts- och terrorismfinansieringshotet är den värdeöverföring som Swish möjliggör. Pengar som kommer in på ett konto kan snabbt föras vidare till andra konton i syfte att försvåra spårbarheten.

Pengar kan flyttas mellan kundens egna konton i olika banker. Pengar kan även flyttas till andra personer i samma bank, men också mellan banker.

Pengarna kan skickas till en mottagare som befinner sig i ett annat land. Det enda kravet är att mottagaren har ett konto i Sverige. Eftersom mottagaren inte behöver befinna sig i Sverige kan Swish användas för att ge personer utomlands tillgång till likvida medel där. Mottagaren kan disponera pengarna med hjälp av ett bank- eller kreditkort, antingen genom att ta ut kontanter i en uttagsautomat eller för betalning av varor och tjänster.

4.6.3.3 Särskilt relevanta sårbarheter

En person som har Swish kan själv på internetbank eller i mobilapp höja de av banken satta beloppsgränserna, upp till en viss gräns. Detta ökar risken då bankens medarbetare inte har möjlighet att ställa kompletterande kundkännedomsfrågor eller frågor om den specifika transaktionen innan överföringen görs.

En juridisk person kan använda sig av Swish avsett för fysiska personer och kan på så sätt både skicka och ta emot betalningar, trots att produkten inte är avsedd för detta. Detta i kombination med att en kund själv kan höja beloppsgränserna ökar den inneboende risken med produkten.

Ytterligare en riskhöjande faktor kan vara hur tjänsten erbjuds, dvs. i vilka kanaler som en person kan teckna tjänsten. Om det kan ske utan personlig kontakt är det något som kan öka risken. En person som vill ansluta sig till Swish kan själv göra det på sin internetbank eller via mobilapp. Bankens medarbetare har då inte möjlighet att ställa kompletterande kundkännedomsfrågor innan tjänsten aktiveras.

Avgörande för bankens sårbarhet och exponering för att utnyttjas för penningtvätt och finansiering av terrorism är bankens förmåga att följa upp transaktioner. Det är viktigt att banken kan identifiera transaktioner som avviker både från det som anses vara ett normalt beteende och det som avviker från den kännedom banken har om kunden och kundens förväntade beteende, men även transaktioner där en juridisk person använder Swish avsett för fysiska personer.

4.6.3.4 Särskilt relevanta avvikande kundbeteenden

Följande är exempel på riskförhöjande faktorer:[34]

• En kund som upprepade gånger byter mobilnummer.

• En kund som upprepade gånger byter anslutet konto.

• En kund som upprepade gånger höjer de av banken satta beloppsgränserna.

• En kund som gör eller tar emot många transaktioner.

• En kund som driver företag tar emot medel på ett privat konto.

• Pengar kommer in på ett konto och flyttas skyndsamt vidare till någon annans konto eller till eget konto i en annan bank. Detta är ett avvikande beteende även vid andra typer av överföringar, men Swish kan, på grund av sin utformning, vara mer attraktiv för detta ändamål. Banken måste utgå från vad som kan anses vara ett normalt beteende och sedan utifrån sina egna erfarenheter och vad som framkommer i olika rapporter bestämma var gränsen för ett avvikande beteende går. En kund som t.ex. byter mobilnummer varje månad eller en kund som varje vecka själv höjer beloppsbegränsningarna som är satta av banken kan vara avvikande. I sammanhanget är det relativt vanligt att målvakter/målvaktskonton används. Det är ofta unga personer som används som penningmålvakter.[35]

4.6.4 Utlandsbetalningar

4.6.4.1 Allmän beskrivning av utlandsbetalningar

Banker, men även andra aktörer, tillhandahåller tjänsten utlandsbetalningar. En kund kan välja olika typer av utlandsbetalningar beroende på hur snabbt pengarna ska nå mottagaren och till vilket land som de ska skickas. Betalningar kan göras till och från de allra flesta länder och banker. Det belopp som skickas sätts in på ett konto i den mottagande banken. Bankernas kunder kan även ta emot betalningar på sina konton i banken.

Både fysiska och juridiska personer kan skicka och ta emot utlandsbetalningar.

Normalt sett kan kunden själv utföra utlandsbetalningar via internetbanken, via bankens app eller genom att besöka ett av bankens/betalningsförmedlarens kontor.

4.6.4.2 Särskilt relevanta hotaktiviteter

Personer som vill tvätta pengar eller finansiera terrorism är i regel intresserade av produkter och tjänster som möjliggör snabba förflyttningar av pengar. Utlandsbetalningar uppfyller det kriteriet. Utlandsbetalningar kan användas för att sända och ta emot pengar till och från länder som saknar effektiva system för bekämpning av penningtvätt eller finansiering av terrorism och som därmed en högre risk för penningtvätt och finansiering av terrorism.

Värdeöverförande aktiviteter, penningtvätt: Det huvudsakliga penningtvättshotet i relation till utlandsbetalningar är att det är en aktivitet som möjliggör värdeöverföring. Pengar som kommer in på ett

[34] Se också Finanspolisen informerar: Betaltjänsten Swish, maj 2018.
[35] Jfr den nationella riskbedömningen av penningtvätt och finansiering av terrorism i Sverige 2020/2021 s. 41.

konto kan fördelas på flera andra konton, även utomlands, i syfte att försvåra spårbarheten. En annan värdeöverförande aktivitet är när pengar snabbt flyttas mellan konton i olika länder.

Värdeöverförande aktiviteter, finansiering av terrorism: Det huvudsakliga terrorismfinansieringshotet i relation till utlandsbetalningar är aktiviteter som möjliggör värdeöverföring. Till skillnad från penningtvätt finansieras ofta terrorism med ”vita” pengar. Det kan avse lön, sparande eller krediter som tagits i flera finansiella institut. Pengarna kan sedan skickas till en mottagare i ett annat land som kan ta ut beloppet i kontanter eller skicka det vidare till en slutmottagare. Terrorism kan finansieras med små belopp, men göra stor skada.

Värdeomvandlande aktiviteter, penningtvätt och finansiering av terrorism: En betalning kan göras i exempelvis SEK och utbetalningen göras i USD. De hot som tjänsten utgör för banker och andra är desamma oavsett om det rör sig om finansiering av terrorism eller penningtvätt.

4.6.4.3 Särskilt relevanta sårbarheter

Utlandsbetalningar kan användas i syfte att bryta kopplingen till pengarnas illegala ursprung, för att försvåra spårbarheten eller för att föra över medel i syfte att finansiera terrorism.

Kunden kan använda flera kanaler och göra transaktionerna på distans, vilket medför att bankens medarbetare inte har möjlighet att ställa kompletterande kundkännedomsfrågor och frågor om transaktionen innan transaktionen sker. Avgörande för sårbarheten är bankens möjlighet att upptäcka transaktioner som avviker från det normala och som avviker från den kunskap banken har om kundens förväntade beteende.

Utlandsbetalningar kan användas för att sända och ta emot pengar till och från länder som saknar effektiva system för bekämpning av penningtvätt eller finansiering av terrorism och som därmed har en högre risk för penningtvätt och finansiering av terrorism. Avgörande för bankens riskhantering är att banken har identifierat vilka dessa länder är och vad det finns för möjlighet att bygga in kontroller i systemen, t.ex. spärrar i form av beloppsbegränsningar. Identifieringen av länder som har förhöjd risk för penningtvätt respektive finansiering av terrorism bör göras separat, eftersom riskerna kan skilja sig åt.

4.6.4.4 Särskilt relevanta avvikande kundbeteenden

Banken måste utgå från vad som kan anses normalt och utifrån sina egna erfarenheter och vad som framkommer i olika rapporter bestämma var gränsen för vad som är avvikande går. En fysisk person som till exempel gör flera utlandsbetalningar varje vecka till olika länder eller en kund som trots låg inkomst skickar och/eller tar emot stora belopp regelbundet kan vara avvikande.

Exempel på riskförhöjande faktorer:

• En kund som inte synes vara intresserad av kostnaderna för tjänsten.

• En kund som betalar till länder som banken anser utgör högre risk för penningtvätt och/eller finansiering av terrorism.

• En kund som utför och/eller tar emot många transaktioner och där det inte stämmer med den kunskap som finns om kunden, t.ex. om kundens verksamhet och familjesituation.

4.6.5 Klientmedelskonton

4.6.5.1 Allmän beskrivning av klientmedelskonton

Klientmedelskonto är en benämning som förekommer i fråga om konto som innehas av kunden i syfte att hålla annans medel avskilda från egna medel. Det som ur ett penningtvättsperspektiv särskiljer ett klientmedelskonto från andra konton är att medlen på kontot innehas av kontohavaren för någon annans räkning. Medlen tillhör alltså någon annan än kontohavaren.

Formerna för nyttjandet av klientmedelskonton kan skilja sig åt, t.ex. i fråga om hur lång tid som medel finns på kontot och storleken på beloppen på kontot. Dessutom finns det stora variationer när det gäller kontohavarens avtalsrelationer med sina kunder.

I andra länder förekommer begreppet *pooled account*. Begreppet används t.ex. i Eba:s riktlinjer för riskfaktorer (EBA/GL/2021/02). I den svenska språkversionen har *pooled account* översatts till klient-medelskonto (avsnitt 2.12 g), men även till ”gemensamt konto” (riktlinje 9.16).

I Eba:s riktlinjer definieras *pooled account* som *ett bankkonto för klientmedel som öppnas av en kund, till exempel en jurist eller notarius publicus. Klienternas pengar sammanblandas, men klienterna kan inte direkt instruera banken att utföra transaktioner* (avsnitt 2.12 g). Definitionen motsvarar det som normalt sett avses med klientmedelskonto.

Begreppet ”gemensamt konto” i riktlinje 9.16 ska inte sammanblandas med vad som i Sverige normalt sett anses vara ett gemensamt konto. I Sverige används gemensamt konto inte sällan som benämning på konton där medel förvaras för flera kontohavare gemensamt, men utan att kontot är att jämställa med ett klientmedelskonto. I dessa fall saknas krav på att hålla medlen avskilda från egna medel. Exempel på denna typ av konto är ett gemensamt konto som innehas av makar med uttagsrätt var för sig eller ett konto som öppnas för att nyttjas gemensamt för ett hushålls löpande utgifter.

Begreppet *pooled account* förekommer också för att beskriva ett gemensamt konto som investerare använder när de går samman i syfte att göra t.ex. en aktieaffär. Genom att gå samman kan de investera ett större belopp och därigenom ofta göra en bättre affär. Det är inte heller i dessa fall fråga om ett klientmedelskonto. I sammanhanget kan det nämnas att begreppet pooled account inte omfattar koncernkonton. Cash pool är en vanligt förekommande term för koncernkonto, men detta ska alltså inte förväxlas med pooled account. Ett koncernkonto är inte heller att jämställa med ett klientmedels-konto.

4.6.5.2 Särskilt relevanta hotaktiviteter

Ett klientmedelskonto kan användas för upplägg där tillgångar köps via en bulvan för att dölja medlens ursprung eller det verkliga ägarskapet.

När pengar skickas via klientmedelskonton kan det ge sken av att syfte och ursprung är kontrollerat och legitimt, trots att det är fråga om brottsvinster.[36] Anonymiteten och möjligheten att dölja medlens ursprung anses var det största hotet med klientmedelskonton. Det kan vara fråga om avsevärda belopp.[37]

[36] Jfr Finanspolisen informerar: Klientmedelskonton nyttjas för penningtvätt, december 2023.
[37] Jfr den nationella riskbedömningen av penningtvätt och finansiering av terrorism i Sverige 2020/2021 avsnitt 7.12.

4.6.5.3 Särskilt relevanta sårbarheter

Det är bankens kund (kontohavaren) som har information om vem eller vilka som är ägare till medlen. Banken kan därför i vissa fall med svårighet och i andra fall inte alls informera sig om medlens ursprung.

Skiktningsscenarion kan likna det förväntade användandet av ett klientmedelskonto, där pengar tas emot och snabbt skickas vidare. Vid exempelvis fastighetsaffärer är det inte ovanligt att det förväntade belopp som passerar klientmedelskontot är stort, vilket gör att större summor kan skiktas utan att bedömas som avvikande.

4.6.5.4 Särskilt relevanta avvikande kundbeteenden

I den nationella riskbedömningen av penningtvätt och finansiering av terrorism 2020/2021 och i Finanspolisen informerar[38] tas bl.a. följande exempel upp:

• Återbetalning av handpenning till samma konto eller annat konto än det som inbetalningen gjordes ifrån.

• Stora transaktioner till eller från utlandet (internationella betalningar).

[38] Finanspolisen informerar: Klientmedelskonton nyttjas för penningtvätt, december 2023.