

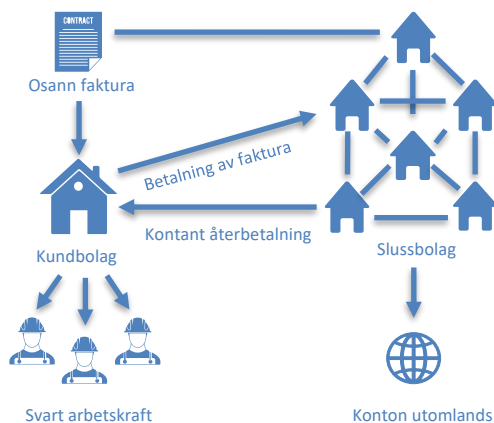
Den ryska organiserade brottslighetens systematiska penningtvätt fortgår

Finanspolisen tillsammans med det finansiella underrättelsecentret¹ kan bekräfta att storskalig penningtvätt och skatteundandragande i Sverige, med bas i den ryska organiserade brottsligheten, fortgår. Tillvägagångssätten är inte unika men det är däremot omfattningen och sambandet med annan samhällshotande brottslighet. Brottsligheten bedöms vara fortgående och de aktuella brottsnätverkens förmåga är hög. Brottbekämpande myndigheter har under lång tid arbetat mot problematiken utan att uppnå en varaktig effekt. I syfte att reducera miljöns förmåga till penningtvätt och skatteundandragande har finanspolisen i samverkan med det finansiella underrättelsecentret ingått i en sekretessbrytande samverkansoperation med flera banker. Analys av material från operationen påvisar att brottsligheten pågår i industriell skala trots att fenomenet är känt sedan tidigare.

Finanspolisen vill härmed informera verksamhetsutövare, primärt inom svenska banksektorn, och andra samhällsaktörer om problematiken samt lyfta utvalda och för analysen relevanta slutsatser. Detta bör ses som ett uppdaterat och bredare komplement till den fenomenrapport finanspolisen gav ut hösten 2024².

Penningtvätt i industriell skala

Penningtvätten möjliggörs genom sammankopplade kluster av tusentals bolag och identiteter, sammanflätade genom banktransaktioner, gemensamma styrelseuppdrag, släktskap eller adresser.



Upphovet till penningtvätten grundar sig i ett företags behov att tvätta pengar och/eller få tillgång till kontanter för att avlöna svart arbetskraft. Företaget, här kallat *kundbolaget* köper tjänsten av penningtvättsnätverket som har tillgång till ett stort antal *slussbolag*. Upplägget sker primärt genom osanna fakturor som ställs ut i fabriksmässig omfattning från slussbolaget till kundbolaget för en tjänst som inte utförs. Den skräddarsydda fakturan ger legitimitet till transaktionen när kundbolaget betalar för den fabricerade tjänsten till ett av slussbolagens bankkonton.

Figur 1: Illustrationen är en förenkling, variation förekommer.

¹ Finansiella underrättelsecentret, Finuc inrättades den 1 april 2025. Centret är en samverkan mellan Polismyndigheten, Skatteverket, Ekobrottsmyndigheten och privata aktörer.

² Fördjupad modusrapport, systematisk penningtvätt inom den rysktalande organiserade brottsligheten, Finanspolisen, A629.012/2024.

I syfte att sedan försvåra spårbarheten ytterligare sker transaktioner mellan olika slussbolag, även transaktioner till utländska konton förekommer. Pengar betalas sedan tillbaka till kundbolaget genom exempelvis kontanter, bilköp eller kontoinsättningar. En procentandel går till penningtvättsnätverket som en kostnad kundbolaget betalar för tjänsten. Upplägget har bekräftats i flera domar.

Miljardbelopp flyttas mellan svenska bankkonton

Penningtvättsens omfattning bedöms vara unik både i antal involverade företag, personer och bankkonton likväl som i kronor. Misstänkta transaktioner motsvarande 2,9 miljarder svenska kronor har analyserats inom den tidsbegränsade operationen och över 3 000 misstänkta unika personobjekt och företag har ingått i materialet. Den totala omfattningen präglas av ett stort mörkertal, dels på grund av miljöns användning av kontanter och kryptovaluta genom underground banking-strukturer, dels på grund av att transaktioner och involverade objekt inte identifieras av bankernas kontroll- och monitoreringssystem i tillräcklig utsträckning.

Personer och företag i uppläggen

Nätverken är styrda på ett företagsliknande sätt, hierarkiskt uppbyggda med ett ledarskikt och möjliggörare med olika grad av befogenhet. Utnyttjade identiteter är en avgörande beståndsdel i nätverkens verksamhet. Analys av cirka 1 700 personer visar en dominans av individer med kopplingar till rysktalande och postsovetiska länder, där hälften är födda utomlands. Georgien, Uzbekistan, Ukraina, Ryssland och Lettland är vanligast och endast en tredjedel har enbart svenskt medborgarskap.

Av samtliga bedöms cirka en femtedel vara utnyttjade identiteter och en av tjugo bedöms vara en central aktör. Miljön har en relativt hög andel kvinnor, en dryg tredjedel, där fyra av tio har identifierats som möjliggörare. Andelen utnyttjade identiteter är sannolikt underskattad i analysen då dessa är svåra att upptäcka, vilket innebär att den verkliga siffran i miljön sannolikt är högre. Identiteterna används ofta för att agera målvakter i styrelser. Deras Bank-ID utnyttjas även för transaktioner, vilket sker antingen mot betalning, under tvång eller ovetandes. Många har tidigare domar för ekonomisk brottslighet.

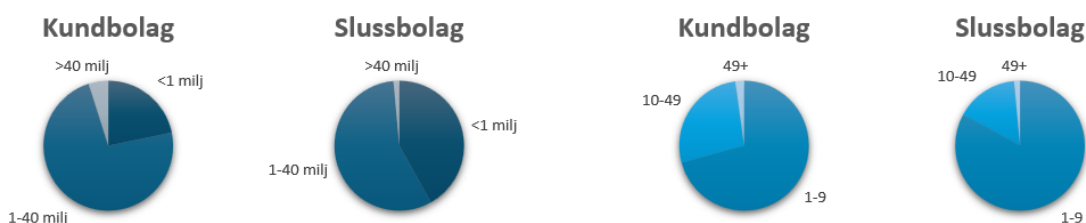


Figur 2: Fördelningen i kategorier av de 1 700 personobjekten som delades inom samverkan.

Bland de drygt 3 000 objekten som analyserats utgjorde unika företagsentiteter cirka 40 procent. Ungefär en fjärdedel av företagen klassificerades som ett kundbolag och ungefär en femtedel som slussbolag. Resterande företag kunde inte tillskrivas en tydlig kategori. Antalet identifierade

slussbolag i det här materialet kan sättas i relation till de 22 bekräftade slussbolag som ingick i penningtvättsdomen B 13688-25, vilka tvättade nära 400 miljoner kronor.

Företag inom byggbranschen är kraftigt överrepresenterade i materialet, oaktat företagets specifika roll i brottsupplägget. Beträffande verksamhetsinriktning är företag inom bygg- och fastighetssektorn, följt av fordonshandel och bemanning vanligt förekommande. Trettio procent av bolagen hade fler än tre SNI-koder, vissa upp emot tio. Populationen domineras av aktiebolag men innefattar även enskilda firmor och föreningar. Kundbolagen är större än slussbolagen beträffande både omsättning och antal anställda.



Figur 3: Fördelning av omsättning i intervall för kundbolag respektive slussbolag.

Figur 4: Fördelning av antalet anställda i intervall för kundbolag respektive slussbolag.

Konkurser, likvidation eller avregistrering är vanligare bland slussbolagen än bland kundbolagen. Detta bedöms inte som avvikande eftersom en del av upplägget är att maximera transaktioner genom slussbolaget för att sedan försätta bolaget i konkurs eller avregistrera det. Gemensamt för de båda bolagskategorierna är att de har haft internationella transaktionsflöden och bankkonton i flera länder.

Kontanternas roll i brottsupplägget

Kontantransaktioner utgör endast två procent av de misstänkta flödena inom operationen. 90 procent är genomförda i svenska kronor. Efter euro (EUR) är uzbekistanska som (UZS), polska zloty (PLN), amerikanska dollar (USD) och georgiska lari (GEL) de vanligaste utländska valutorna bland kontanttransaktionerna. Även om beloppen i dessa valutor är i sammanhanget små, kan de indikera hur tillgång och efterfrågan kan se ut. De skulle även kunna indikera till vilka länder den svarta arbetskraften som avlönas med kontanter har nära anknytning. Den låga synligheten i banksystemet beror på att merparten av kontantflödet inom miljön kringgår svensk monitorering genom uttag utomlands, kontant bilförsäljning, kryptoväxling eller användning av parallella banksystem (t.ex. underground banking). Dessa metoder möjliggör hantering av stora kontantvolymerna utan att passera svenska banker eller synas i bolagens bokföring, vilket är avgörande för att avlöna svart arbetskraft och slutföra penningtvätten.

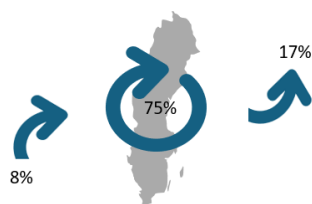
Fordonsaffärer

Cirka 200 miljoner kronor har kunnat identifieras och härledas till misstänkta fordonsrelaterade upplägg, som en del av penningtvätten. Majoriteten av transaktionerna går till svenska motparter, men flöden till Norge, Litauen och USA förekommer. Ett återkommande modus är att ett

slussbolag, finansierat av ett kundbolag eller privatpersoner, köper bilar av, ibland medvetna, återförsäljare. Fordonen registreras på målvakter, avregistreras eller förs utomlands för kontantförsäljning, varvid pengarna återförs till Sverige via banköverföring, kontanter eller kryptovaluta. Analysen visar även mångmiljonbelopp i Swish- och banköverföringar märkta med registreringsnummer eller bilmodeller. Sådana markeringar kan användas för att maskera penningtvätt under förevändning av bilhandel, även när inget faktiskt ägarbyte sker, ett upplägg som bekräftats i rättspraxis.

Internationella förgreningar

Transaktioner inom Sverige utgör 75 procent av de totala beloppen, medan utgående internationella flöden utgör cirka en femtedel och resterande del avser inkommande transaktioner till Sverige. Kontoöverföringar stod för nästan 90 procent av beloppen som gick utomlands, resterande var i stort sett uteslutande korttransaktioner. De största mottagarländerna var Litauen, Polen, Irland och Storbritannien.



Företagstransaktioner till Paysera och Revolut dominerar i de fall Litauen är mottagare, men även ett väsentligt antal privatkonton finns med i materialet. Till Polen och Storbritannien gick mestadels transaktioner från företag till företag men även ett antal större transaktioner till privatpersoner. Irland sticker ut gällande korttransaktioner till Revolut och Paysend.

Figur 5: Fördelningen av de 2,9 miljarder kronor i misstänkta transaktioner.

Den gränsöverskridande delen av upplägget gynnas eftersom transaktioner ofta går via utländska neobankers och betalningsinstitut, något som begränsar spårbarhet och minskar transparensen. Även om endast en femtedel av volymen utgörs av gränsöverskridande transaktioner bedöms den faktiska omfattningen vara större, då förflyttning ofta sker i senare skeden eller via andra kanaler. Kryptotransaktioner direkt från svenska banker är marginella; istället flyttas medel sannolikt utomlands (exempelvis till Revolut) innan växling till kryptovaluta sker, vilket försvårar spårbarheten ytterligare.

Administrativa möjliggörare viktiga för brottsupplägget

Bland de delade objekten inom samverkan har ett tjugotal redovisningsfirmor och över 20 administrativa möjliggörare identifierats. Dessa aktörer verkar enskilt, eller via en redovisningsfirma, och hanterar t.ex. löneadministration, bokföring och utfärdar falska fakturor för slussbolagen. De hanterar rekrytering av målvakter och nyttjar deras BankID, inklusive signering av transaktioner. Även kluster av myndighetsrelaterade transaktioner har kunnat härledas till dessa aktörer. Det är vanligt att de innehar fullmakter för hundratals bolag samt står registrerade som deklara-sionsombud.

Andra typer av möjliggörare som via sin profession eller särskild kompetens förekommer inom miljön och har observerats i analyserat material. Det innefattar bland annat auktoriserade revisorer, fastighetsmäklare, tolkar och individer med särskild juridisk kompetens.

Penningtvättens samband med annan brottslighet

Den rysktalande organiserade brottsligheten är multikriminell på ett system- och samhällshotande sätt där annan brottslighet berikas. Välfärdssystemet utnyttjas genom bidrag, lönegarantier, a-kassa och obetalda skulder. Konkurer och tillgången till billig arbetskraft snedvrider konkurrensen och offentliga upphandlingar blir urholkade. Den bidrar till människoexploatering och människohandel både i och utanför Sverige. En systematisk kartläggning sker av banker och myndigheter för att komma runt regelverken och utnyttja sårbarheterna. Detta resulterar i hot mot näringsliv och skadat förtroende för banker och myndigheter.

Kontakter mellan aktörer i materialet och högt uppsatt brottsaktörer inom andra kriminella miljöer har identifierats. Det handlar bland annat om länkar genom kontanthantering till *våldsnätverk* i Sverige och deras narkotikahandel. Efterfrågan på kontanter i den ena miljön och tillgången till kontanter i den andra skapar utrymme för affärsförbindelser. Det förekommer även transaktionskopplingar mellan individer verksamma i penningtvättsupplägget och den *ryska ambassaden* i Sverige.

Svenska bankers motåtgärder är inte tillräckligt effektiva

Även om bankernas arbete mot penningtvätt utvecklas kontinuerligt, bedöms det inte vara tillräckligt effektivt. Under operationen identifierades misstänkta transaktioner på 2,9 miljarder kronor, varav 75 procent inom Sverige. Detta understryker behovet av stärkt sårbarhetsreducerande arbete hos bankerna.

Samverkansoperationen resulterade i att över 1 000 konton stängdes, närmare 200 kunder nekades och drygt 50 miljoner kronor belades med dispositionsförbud. Den låga nivån på frysta medel i relation till de totala transaktionssummorna illustrerar hur snabbt pengar förflyttas och betonar vikten av snabba och förebyggande åtgärder. Åtgärderna som genomfördes i samband med samverkan bedöms ha en störande och temporärt reducerande effekt på brottsligheten, men givet det kontinuerliga utbytet av företag och identiteter som används, är det sannolikhet att brottsligheten kommer att fortsätta. Följande delar bedömdes under samverkan som försvårande omständigheter och bidrar sannolikt till att brottsligheten kan fortgå:

- Nuvarande monitorering av riskindikatorer och transaktionsanalys är reaktivt och sker ofta i för sent skede. Övervakning och granskning av enskilda kunder är inte hållbart, istället krävs övergång till mer skalbara analysmetoder. Det är inte alla banker som har integrerat kundkännedomsinformationen i övervakningen av transaktioner, vilket gör det svårare att identifiera ett avvikande transaktionsbeteende.
- Brister i datakvaliteten i inrapporteringen till finanspolisen försvårar arbetet att kartlägga penningtvättsupplägg avsevärt och kopplingar mellan personer och företag upptäcks inte. Det påverkar följaktligen bedömningar och slutsatser. Inom genomförd analys kan saknad motpartsinformation för utländska konton och bankgirotransaktioner som rapporterats av banker nämnas som specifikt bristfälliga.
- Digitala banktjänster för onboarding och kontoöppning underlättar avsevärt för aktuell brottslighet. Nuvarande kontroll- och säkerhetsmekanismer är inte tillräckliga, vilket blir tydlig i relation till mängden konton, företag och individer som kan användas i ett och samma brottsupplägg.
- Bristande kundkännedomskontroller vid nya förhållanden, t.ex. när nya styrelsemedlemmar eller kontofullmakter läggs till, möjliggör att bolag med befintliga konton,

etablerade styrelser och god kredithistorik övertas och missbrukas i stor skala, utan att det uppmärksammas av banken i tid. Att konsultera flera källor för att få en heltäckande bild av en styrelsesammansättning och att uppgifterna trots det är föråldrade hämmar möjligheten till en ändamålsenlig bedömning av risken.

- Digitala identitetshandlingar, primärt BankID, som samägs av sex svenska storbanker, saknar tillräckliga kontrollmekanismer för att t.ex. hindra en obehörig individ att förfoga över en mängd utnyttjade identiteters BankID:n.

För att förebygga och förhindra denna fenomenliknande penningtvätt behöver metoderna anpassas för mängden illegala transaktioner och kunder som används. Följande åtgärdsförslag identifierades under samverkan och bedöms ha en förebyggande effekt på brottsligheten som rapporten beskriver:

- Överväg att begränsa produktutbudet för kunder av högre risk och minimera grundfunktionaliteten för ett, enligt kontraheringsplikten berättigat konto.
- Att för nya kunder av hög risk införa obligatorisk fysisk inställelse hos banken kan begränsa användandet av utnyttjade identiteter. Även vid förändrat transaktionsbeteende eller förändringar i ledande positioner bör fysisk inställelse övervägas.
- För ett pågående kundengagemang bör riktlinjerna för när en ny kundkännedomsprocess ska utföras ses över. Överväg att se över typen av kundkännedomsfrågor och dess effektivitet, utöka frågeställningarna och uppföljningen vid indikationer om misstänkt beteende.
- Bankerna bör omhänderta den tillgängliga kundinformation som finns att tillgå från primärt Bolagsverket, Skatteverket och Migrationsverket samt privata aktörer. Prenumerationstjänster bör användas för snabbare tillgång till förändringar och uppdaterad kundkännedom.
- Egen analys och bearbetning av informationen bör appliceras på bankens egna kunddatabas för att skapa triggers och egna riskindikatorer. Här är informationsdelning och riskbaserat arbetssätt inom banken avgörande, rätt avdelning bör ha tillgång till information för att effektivt kunna upptäcka och förebygga penningtvätten.
- Nära samarbete, delning av information och kunskap mellan avdelningar inom banken, exempelvis mellan sälj, risk och onboarding samt anti-penningtvätt är nödvändig. Både för att stoppa enskilda kunder men även för att uppmärksamma prioriteringsbehov och resursfördelning inom banken.
- Även mediabevakning och domar har lyfts av bankerna själva som bra källa för att identifiera kriminella kunder. Det senare är numera begränsat på grund av sekretessbestämmelser.

Bankerna är enligt penningtvättslagstiftningen skyldiga att rapportera misstänkta transaktioner till finanspolisen. Att rapportera är en skyldighet men ersätter på intet sätt ett aktivt arbete mot penningtvätt. Bankerna är de som kan stoppa transaktioner, stänga konton eller neka och/eller avsluta kundengagemang. En bred tillämpning skulle ha en starkt brottsförebyggande effekt.

Andra aktörers möjlighet att påverka brottsligheten

I syfte att uppnå varaktig effekt och reducera brottsligheten krävs förebyggande insatser och tidig upptäckt, där flera samhällsfunktioner kan bidra, inte minst den svenska banksektorn. För att aktörer, särskilt banker, effektivt ska kunna motverka penningtvätt är tillgången till korrekt och aktuell information avgörande. En förändring av bankernas arbetsmetoder kräver därför att både tillgängligheten och kvaliteten på denna nödvändiga information förbättras.

Bolagsverket

Samverkansoperationen identifierar Bolagsverket som en av de myndigheterna med störst potential att påverka den aktuella brottsligheten. Bolagsverket har inte bara ett registrerande uppdrag, de har även ett brottsförebyggande uppdrag³. Att utföra åtgärder inom det uppdraget skulle kunna ge en betydande genomslagskraft i arbetet mot företag som brottsverktyg.

Styrelsebyten, byte av verklig huvudman eller andra företrädare är en riskindikator som ofta förekommer i upplägg där företag används som brottsverktyg. Informationsluckor gällande målvakter med egna eller utnyttjade identiteter som innehar en mängd styrelseuppdrag och/eller andra styrande positioner är även det en sårbarhet. Avsaknad av ett verkligt huvudmannaregister och centralt aktieägarregister begränsar möjligheten att förstå hur bolag kan sammankopplas och potentiella kriminella kopplingar kan undgå upptäckt. Nedan följer förslag som uppmärksammas inom samverkansoperationen för Bolagsverket att överväga:

- Möjligheten till att digitalisera dokument, såsom årsredovisningar.
- Möjligheten digitalisera kontrollen av inlästa dokument (enligt föregående punkt) för att detektera osanna eller falska dokument samt hitta identiska massproducerade årsredovisningar eller andra dokument.
- Möjligheten att utveckla Bolagsverkets kontrollfunktioner för att säkerställa att både befintliga och nya registeruppgifter är korrekta.
- Möjlighet till utökade kontroller vid bolagsstart vid flertalet historiska konkurser, näringsförbud eller dylikt.
- Möjligheten att införa begränsningar, sanktioner eller likvidation för bolag vid återkommande uppenbara felaktigheter eller förseningar av exempelvis årsredovisningar.
- Möjligheten att införa högre krav på fysisk inställelse för styrelse och verklig huvudman.
- Möjligheten att kräva id-handlingar på nya styrelseledamöter och/eller företrädare.
- Möjligheten till ökad kontroll vid styrelseförändringar och bakgrundskontroll av styrelsemedlemmar.
- Möjligheten till utökade kontroller vid bolagsöverlåtelser.
- Möjligheten att blockera falska identiteter från att tillträda bolagsstyrelser.
- Möjligheten att blockera bekräftade målvakter, falska, osanna, försvunna etc. identiteter från till exempel bolagsstyrelser.
- Möjligheten att inrätta ett centralt aktieägarregister för onoterade bolag för att försvåra dolt ägande.
- Möjligheten till begränsningar vid utlandsbaserad styrelse och särskild delgivningsperson.

Skatteverket

Skatteverket är den myndighet som har i uppdrag att upprätthålla korrekta register inom folkbokföring, vilket inkluderar uppgifter om bland annat bosättning och identitet. Bristande adresskontroller utnyttjas av kriminella genom till exempel skenskrivningar i bostadsområden. Det finns fall om uppemot hundra identiteter som varit skrivna på närliggande adresser under nästan fyra års tid. Gällande inkomstuppgifter har det uppmärksamats att kriminella skickar in osanna korrigeringar av inkomstuppgifter till Skatteverket. Bristande kontroller, som leder till missbruk av identiteter, är en av de större sårbarheterna i arbetet mot den rysktalande organiserade brottsligheten

³ <https://www.regeringen.se/pressmeddelanden/2024/03/tydligare-kontrollerande-roll-ska-starka-bolagsverkets-brottsförebyggande-arbete/> 2026-06-25.

och den åtkomst till välfärdssamhället och banksystemet som en identitet medför. Nedan följer förslag som uppmärksammats inom samverkansoperationen för Skatteverket att överväga:

- Möjligheten att dela information om deklarationsombud med verksamhetsutövare och/eller andra väsentliga aktörer
- Möjligheten till ett delat register för bekräftade företagsmålvakter med verksamhetsutövare och/eller andra väsentliga aktörer

Finansinspektionen

Finansinspektionen (FI) har tillsynsansvar gällande bankernas arbete mot penningtvätt. Det är särskilt viktigt med samsyn kring kontraheringsplikt och möjligheten att stänga ned konton och avsluta kundrelationer. I samverkansoperationen var fördelningen bland nekade kunder 78 procent företag, vilket delvis kunde förklaras av bankerna med att kontraheringsplikten inte gäller företag. Även bedömningen av vad som är en ny kund vid exempelvis styrelseförändringar och de efterföljande kraven på kundkännedom är viktigt att tydliggöra. Nedan följer förslag som uppmärksammats inom samverkansoperationen för Finansinspektionen att överväga:

- Se över sitt arbetssätt och anpassa sin tillsyn för att främja bankernas nödvändiga förändring i sitt arbetssätt mot penningtvätt. Enligt senaste nationella riskbedömningen⁴ bedöms bankerna tillhöra högsta riskkategorin, vilket även medför en omställning av finansinspektionens tillsynsarbete. Att se över att tillsynen riktas för att främja ett effektivt arbete för bankerna mot penningtvätt är en del i Finansinspektionens roll att tillsammans motverka att svenska banker används som brottsverktyg.

Övriga möjliga motåtgärder

Länsstyrelserna utövar tillsyn och kan utfärda sanktioner till de redovisningsbyråer som lyfts om möjliggörare inom miljön. För ökad kontroll är licensiering eller auktorisering för bolagsförmedlare något som bör övervägas, något som även Brå⁵ uppmärksammat.

Eftersom byggbranschen är överrepresenterad inom ROB-miljön kan flera aktörer inom byggsektorn lyftas här. Ett exempel är misstänkta bidragsbedrägeri mot *Byggarbetarnas arbetslöshetskassa* genom utnyttjade identiteter. En trolig hypotes är att a-kassan utnyttjas i perioder, "mellan jobb" och genom utnyttjade identiteter där en vit lön, högre än snittlönen, ger möjlighet till en högre nivå på a-kassa. Givet tillgången till utnyttjade identiteter kan stora belopp tillskannas bedrägligt.

Kronofogden utövar tillsyn av konkursförvaltare och möjligheten att föreslå sin egen konkursförvaltare för tingsrätten att förordna, är något som missbrukas i kriminella syften och är en del i den illegala omsättningen av bolag kopplat till aktuell brottslighet.

Revisorsinspektionen och *Fastighetsmäklarinspektionen* har alla tillsynsobjekt som förekommer inom ROB-miljön och deras ansvar i arbetet mot penningtvätt har uppmärksammats i flera tidigare rapporter⁶.

⁴ Nationell riskbedömning av penningtvätt och finansiering av terrorism i Sverige 2024/2025, Samordningsfunktionen, Polismyndigheten, A360.891/2024.

⁵ Brottsförebyggandet, Brå, Företag som brottsverktyg (2025:20).

⁶ Professionella penningtvättare Branscher, modus och kopplingar till kriminella nätverk, Finanspolisen, mars 2024.

Framåtblick

Den digitala plånboken EU Digital Wall

Möjligheten att utnyttja andra personers identitet genom att använda digitala identitetshandlingar såsom *BankID*, är en av sårbarheterna som möjliggör den här typen av brottslighet. På europeisk nivå sker införandet av den *digitala plånboken EU Digital Wallet*.⁷ I SOU 2024:45 beskrivs att risk föreligger för att identiteter missbrukas. Det konstateras även i utredningen att brott som begås med användning av identitetsplånböcker kommer att behöva förebyggas och utredas på andra sätt än via brukar- och transaktionsdata. Ingen närmare bedömning av möjligt missbruk har ingått i analysen, men givet miljöns anpassningsförmåga och internationella täckningsområde är det sannolikt att digitala plånböcker kommer utnyttjas för aktuell brottslighet.

Virtuala IBAN (vIBAN)

vIBAN är en global standard för identifikation av bankkonton för främst internationella betalningar. Till skillnad från vanliga IBAN kan ett bankkonto ha flera *vIBAN* kopplat till sig, och kontohavare, ursprungsland och utgivare maskeras för mottagare. *vIBAN* möjliggör snabba internationella betalningar och teoretiskt finns inga begränsningar i hur många led eller mellanhänder som kan finnas mellan avsändare och slutgiltig mottagare. Detta försvårar spårbarheten avsevärt i arbetet mot penningtvätt. I en rapport⁸ från Danmarks Financial Intelligence Unit, från 2026 uppmärksammas att så kallade fakturafabriker⁹, massproducenter av osanna fakturor har börjat använda sig av *vIBAN* i allt större utsträckning. Ingen analys har gjorts inom operationen av hur utbrett användandet är i den aktuella kriminella miljön i Sverige, men baserat på de danska observationerna bedöms sannolikheten för illegalt användande som stor.

A602.520/2026

⁷ "Digital identitetsplånbok, även kallad EU Digital Identity Wallet (EUDIW), är ett viktigt steg i EU:s arbete för att göra digitala tjänster enklare, säkrare och mer tillgängliga över landsgränserna. Målet är att varje medlemsland senast 2026 ska erbjuda minst en digital identitetsplånbok – en tjänst där invånare och företag enkelt och säkert kan identifiera sig, dela information och signera digitalt." <https://www.digg.se/digitala-tjanster/digital-identitetsplanbok> 2026-05-27.

⁸ Fictitious invoices and virtual IBANs Danish FIU, 2026

⁹ Mer kring begreppet 'fakturafabrik' finns att läsa i Fördjupad modusrapport, systematisk penningtvätt inom den rysktalande organiserade brottsligheten, Finanspolisen, A629.012/2024.