Bedrägerier och penningtvätt

Analys av bedrägerier ur ett brottsvinstperspektiv

Polisen

Polismyndigheten, Finanspolissektionen, januari 2022

Utgivare: Polismyndigheten, Nationella operativa avdelningen, Box 12256, 102 26 Stockholm
Dnr: A697.130/2021, Saknr: 423
Omslagsfoto: Polisen
Upplaga: Internet
Datum: 2022-01-26

Innehåll

Inledning

Antalet anmälda bedrägerier per år ökade stadigt fram till 2018. Därefter har trenden vänt något men bedrägerier är fortfarande en av de vanligaste brottstyperna. Såväl privatpersoner och företag som svenska staten utsätts för bedrägerier som summerar till miljardbelopp årligen. Den omfattande bedrägeribrottsligheten återspeglas i rapporteringen till Finanspolisen och nästan var femte penningtvättsrapport rör misstankar om att pengarna kommer från bedrägeri. Bedrägerier är också den i särklass vanligaste typen av brottslig verksamhet som förekommer i fällande domar vid penningtvättsbrott.[1] Det beror delvis på att det i enklare bedrägeriupplägg ofta är relativt okomplicerat att styrka att pengarna kommer från brott då det går att se mellan vilka konton och kontoinnehavare en överföring har skett.

Syftet med denna rapport är att ge en bild av penningtvätt kopplat till olika typer av bedrägerier och bedöma hotet från bedrägerierna ur ett brottsvinstperspektiv. Inledningsvis ges en beskrivning av olika bedrägerityper och vad rapporteringen till Finanspolisen säger om hanteringen av brottsvinsterna.[2] Därefter görs en jämförande analys av bedrägeriernas omfattning och de kriminella aktörerna bakom upplägen. Sist i rapporten presenteras några förslag på tänkbara åtgärder för att minska sårbarheter kopplat till de bedrägerier som bedöms utgöra de största hoten ur ett brottsvinstperspektiv.

[1] BRÅ (2019), *Penningtvättsbrott – En uppföljning av lagens tillämpning*

[2] Ett stort antal verksamhetsutövare är skyldiga att anmäla sådant som misstänks utgöra ett led i penningtvätt eller finansiering av terrorism till Finanspolisen. Skyldigheten gäller inte bara finansiella aktörer utan även annan typ av verksamhet, bland annat revisorer, advokater och fastighetsmäklare.

Sammanfattning

Finanspolisens analys av penningtvätt i samband med bedrägerier bekräftar bilden att det ofta handlar om multikriminella aktörer och att det är stor risk att bedrägerivinsterna återinvesteras i annan allvarlig brottslighet.

Genomgången visar att det finns strukturella skillnader mellan aktörerna bakom olika typer av bedrägerier vad gäller ekonomisk kapacitet, organisationsförmåga och tillgång till våldskapital. Brottsvinsternas omfattning skiljer sig också åt, liksom i vilken utsträckning penningtvätten upptäcks och rapporteras till Finanspolisen. Både mörkertalet och den faktiska omfattningen bedöms vara särskilt stor för moms- och välfärdsbedrägerierna. Trots ett fåtal misstankerapporter om momsbedrägerier summerade de rapporterade beloppen till flera hundra miljoner kronor under 2020.

Baserat på resultatet av analysen har Finanspolisen gjort en bedömning av hotnivån för de olika bedrägerityperna ur ett brottsvinstperspektiv. I bedömningen görs ingen värdering av bedrägeriernas konsekvenser eller vilka som drabbas. Jämförelsen bygger enbart på en skattning av brottsvinsternas omfattning, de kriminella aktörernas förmåga och risken att pengarna återinvesteras i organiserad brottlighet.

Ur det perspektivet utgör moms- och välfärdsbedrägerierna det största hotet. Dessa bedrägerier genererar miljardbelopp årligen som kan återinvesteras i annan allvarlig brottslighet. Aktörerna har hög ekonomisk och organisatorisk förmåga och tydliga kopplingar till organiserad brottslighet.

Så kallade BEC-bedrägerier (Business E-mail Compromise) utgör också ett betydande hot mot bakgrund av den stora omfattningen och organisatörernas koppling till kriminella nätverk. BEC-bedrägerierna ligger bakom en väsentlig del av rapporteringen till Finanspolisen.

Även för låne- och vishingbedrägerier bedöms hotnivån vara betydande, men av olika skäl. Lånebedrägerierna summerar till relativt stora belopp och möjliggör för grovt kriminella att tillgodogöra sig brottsvinster genom ägande av bland annat fastigheter. Vishingbedrägerierna genererar relativt sett mindre belopp men är den bedrägerityp där störst andel misstankerapporterade personer har samband med annan brottslighet och till kriminella nätverk. Vishingbedrägerierna bedöms vara en viktig inkomstkälla för den organiserade brottsligheten i Sverige och det finns tecken på att unga i utsatta områden utnyttjas som målvakter.

För att minska det hot som brottsvinsterna från bedrägerier utgör behöver ett antal sårbarheter täppas till. Det handlar om att stärka bankers och andra verksamhetsutövares förmåga att upptäcka och förhindra bedrägerierna innan de sker, men också om ökad kontroll hos utbetalande myndigheter i samband med moms- och välfärdsbedrägerier.

Exempel på sådana sårbarhetsreducerande åtgärder är:

- Systematisk övervakning av transaktioner på skattekonton med avseende på penningtvättsrisker - från både Skatteverkets och bankernas sida.
- Högre grad av kundanpassning i övervakningen av transaktioner på företagskonton.
- Teknisk lösning hos bankerna för att upptäcka och förhindra BEC-bedrägerier innan transaktionerna genomförs.
- Stärkt kontroll av identitet och löneunderlag i samband med kreditgivning för att minska risken för lånebedrägerier.

1 Bedrägerier och penningtvätt

Olika typer av bedrägerier genererar brottvinster på olika sätt, varför hanteringen av pengarna skiljer sig åt. I bedrägerier mot privatpersoner eller företag handlar penningtvätten om att dölja pengarnas ursprung för att kunna konsumera eller investera dem i den legala ekonomin. I bedrägerier mot staten, till exempel i syfte att få bidrag utbetalade, ger medlen redan från början intryck av att vara legitima. Här vill aktörerna i stället dölja pengarnas slutmål. Processen att tvätta pengar brukar generellt sett beskrivas i tre steg; placering, skiktning och integrering.

Placering

Placering handlar om att få in brottsvinsterna i det finansiella systemet, till exempel via kontantinsättningar eller köp och försäljning av varor.

Skiktning

Skiktning är transaktioner som görs för att dölja spåren mellan pengarnas ursprung och slutmål. Pengarna flyttas ofta i flera steg för att minska risken för upptäckt.

Integrering

I det sista steget ska pengarna integreras i den vita ekonomin. Det kan göras genom allt från löpande konsumtion till investering i fastigheter och företag.

I samband med bedrägerier behövs sällan det första steget ovan eftersom den som utsätts förmås göra en överföring till bedragarna, vilket innebär att brottspengarna redan är inne i det finansiella systemet.[3] I princip alla bedrägeribrott följs däremot av någon form av skiktning som syftar till att minska spårbarheten. Brottsvinsterna hamnar typiskt sett på ett målvaktskonto hos en person eller ett företag för att sedan slussas vidare i olika transaktioner.

Det finns ingen entydig koppling mellan ett visst bedrägerimodus och det efterföljande penningtvättsförfarandet men det går ändå att se några övergripande skillnader mellan bedrägerikategorierna. Generellt kan sägas att ju enklare form av bedrägeri desto mindre sofistikerad är också penningtvätten. Uppläggen spänner från uttag av kontanter till komplexa kedjor av överföringar mellan företag i olika länder. När det handlar om större belopp är det vanligare att pengarna tvättas via företagskonton och också vanligare att pengarna förs utomlands direkt, utan att skiktas i Sverige först. Vid bedrägerier i mindre skala används privatkonton och eventuella utlandsöverföringar görs först i senare led, troligen för att de tar längre tid att genomföra och innebär en större risk för upptäckt i bankernas monitorering.

Relativt få penningtvättsrapporter visar på användning av kryptovaluta utom i de fall där det är en del av själva bedrägeriupplägget. Det kan dock vara så att bedrägerivinster växlas till kryptovaluta senare i penningtvättskedjan utan att det framkommer i rapporteringen. Rapporterna till Finanspolisen fokuserar oftast på den initiala transaktionen i bedrägeriet eller den första delen av skiktningsfasen. Ibland fryser också banken pengarna på målvaktskontot direkt när bedrägeriet upptäcks och då går det inte att se hur skiktningen annars hade sett ut.

[3] Inget av de tillvägagångssätt som diskuteras i denna rapport involverar kontanter som en del av bedrägeriet. Kontanter kan däremot förekomma i den efterföljande penningtvätten.

Nedan beskrivs olika bedrägerityper som nämns i rapporter om misstänkt penningtvätt till Finanspolisen. Bedrägerierna är indelade i tre kategorier utifrån tillvägagångssätt; moms- och välfärdsbedrägerier, bedrägerier med social manipulation samt övriga bedrägerier. Det är stor skillnad mellan kategorierna vad gäller antalet rapporter. För vissa bedrägerityper är underlaget mer begränsat men säger ändå något om hanteringen av brottsvinsterna.

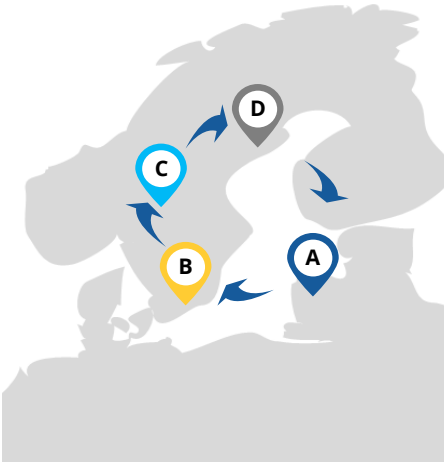
1.1 Moms- och välfärdsbedrägerier

Moms- och välfärdsbedrägerier syftar till att komma över offentliga medel på felaktiga grunder. I så kallade momskaruseller handlar det om utbetalning av skattemedel. Det finns också olika typer av välfärdsbedrägerier som riktas mot bland andra Försäkringskassan, Arbetsförmedlingen, CSN och Migrationsverket. Ett annat aktuellt exempel är bedrägerier gällande korttidsstöd från Tillväxtverket under coronapandemin.

Eftersom brottsvinsterna betalas ut från myndigheter ifrågasätts transaktionerna sällan av bankerna och det finns ingen målsägande i form av privatperson eller företag som upptäcker och anmäler förlusten. Därför kan det dröja innan bedrägerierna uppdagas men när det väl sker vill gärningsmännen ha säkrat pengarna. Med penningtvätt avses alltså här de åtgärder som de kriminella aktörerna vidtar för att minska spårbarheten mellan bidrags- eller moms utbetalningarna och den slutliga användningen av pengarna.

1.1.1 Momsbedrägerier (MTIC)

Momskaruseller eller MTIC-bedrägerier (Missing Trader Intra Community) går ut på att lura till sig momspengar från staten. I affärer mellan bolag i olika EU-länder råder så kallad omvänd skattskyldighet, vilket innebär att köparen, inte säljaren, är skattskyldig. Detta utnyttjas i momskaruseller på så sätt att aktörerna inkasserar ingående moms utan att betala den utgående momsen.[4] Genom att upprepa en kedja av gränsöverskridande transaktioner mellan företag kan bedrägerierna skalas upp till omfattande belopp. Illustrationen nedan visar i ett förenklat exempel hur det går till.



1. **Företag A** i ett annat EU-land säljer varor till **Företag B** i Sverige för €1000 (0% moms).
2. **Företag B** säljer varorna vidare inom Sverige till **företag C** för €900 + moms. Med falska fakturor skapas osann ingående moms som balanserar bort utgående moms. **Företag B** betalar därmed ingen moms till staten och gör en vinst på €900 + moms - €1000.
3. **Företag C** säljer vidare till **företag D** för €910 + moms och gör en vinst på €10. Moms på köp respektive försäljning tar i princip ut varandra.
4. **Företag D** säljer tillbaka varorna till **företag A** för €950 (0% moms). Efter att **företag D** fått tillbaka moms på inköpet blir vinsten €40.
5. **Företag A** kan åter exportera varorna till **företag B** för €1000 och tjäna mellanskillnaden €50.

[4] Ingående moms är momsen på inköp av en vara och som företaget har rätt att få tillbaka. Utgående moms är momsen som läggs på försäljningen och som företaget sedan ska betala in till staten.

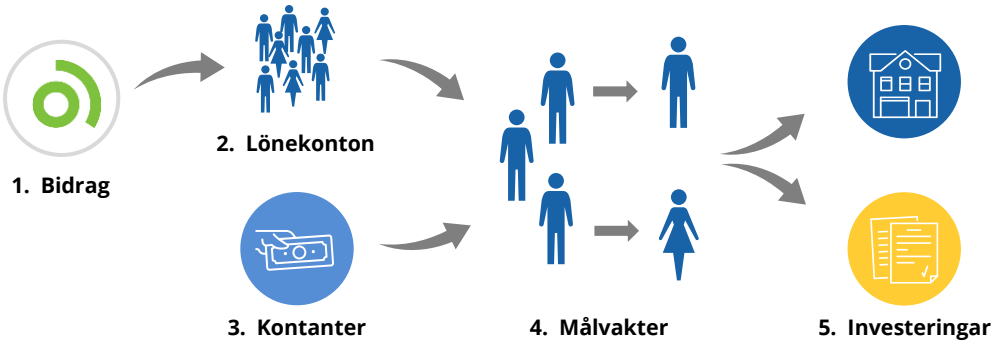
För att minska risken för upptäckt kan bolagen använda sig av utländska betalningsplattformar, vilket leder till att man inte fångar upp transaktionerna i Sverige. Rapporteringen till Finanspolisen om misstänkta momskaruseller är så begränsad att det är svårt att dra generella slutsatser om hur brottsvinsterna tvättas men den gemensamma nämnaren är att det görs via företagskonton. Det finns exempel med små företag vars verksamhet inte har något naturligt samband med de varor som bedrägerierna bygger på. Det kan vara en liten lokal näringsidkare inom detaljhandel eller service som på pappret också ska driva partihandel inom elektronik och som skickar stora summor till utlandet.

1.1.2 Välfärdsbedrägerier

Rapporteringen om välfärdsbedrägerier är ännu mer sparsam. Finanspolisen får en del rapporter om misstänkt bidragsfusk hos enskilda individer. I de fallen vidtas sällan några penningtvättsåtgärder utan pengarna används direkt till konsumtion.

När det gäller mer systematiska välfärdsbedrägerier, via verksamhet inom till exempel skola eller omsorg, är underlaget i penningtvättsregistret i princip obefintligt. Annat underrättelsematerial tyder dock på att vinster från den typen av bedrägerier tvättas med något enklare tillvägagångssätt jämfört med momssnurrorna. Pengarna skiktas med transaktioner på både privat- och företagskonton. Uttag och insättningar av kontanter kan också förekomma.

Exemplet nedan visar schematiskt hur brottsvinsterna hanterades i ett fall där en företrädare för restaurangbolag dömts för grovt penningtvättsbrott. Pengarna som tvättades kom både från skattebrott och från bedrägeri mot Arbetsförmedlingen. Bidragsbedrägeriet bestod i att de anställda inte fick behålla löner som finansierats med olika typer av anställningsstöd.



1. Restaurangbolaget rekryterade personal från ett land i Asien. Lönerna betalades med stöd från Arbetsförmedlingen; instegsstöd, nystartsjobb och särskilt anställningsstöd.
2. Med bankdosor och koder kunde bolagsföreträdaren kontrollera de anställdas lönekonton och skicka pengarna vidare till andra privatpersoner som utnyttjades som målvakter.
3. Även oredovisade kontanter från restaurangverksamheten sattes in på olika privatkonton.
4. Brottspengarna skiktades via målvaktskonton i flera led.
5. Pengarna investerades slutligen i flera bostadsrätter i Stockholmsområdet och i kapitalförsäkringar.

1.2 Social manipulation

Bedrägerier med hjälp av social manipulation handlar om att vilseleda en person att begå en handling som ger ekonomisk vinning till gärningspersonen. Hit hör BEC-bedrägerier, romans- och investeringsbedrägerier samt vishing, smishing med mera.

1.2.1 BEC

BEC-bedrägerierna (Business E-mail Compromise), även kallade VD-bedrägerier, skiljer sig från övriga bedrägerier med social manipulation i så måtto att de riktas mot företag. Upplägget bygger på att bedragaren i e-post utger sig för att vara någon annan, som en högt uppsatt chef eller en leverantör, för att förmå en anställd i ett bolag att genomföra transaktioner, ofta fakturabetalningar till ett annat land.

Rapporterna till Finanspolisen rör nästan enbart penningtvätt via målvaktskonton i Sverige där pengarna kommer från bedrägerier som begåtts mot företag i andra länder. I de flesta fall är målvakterna privatpersoner men företagskonton används också. Efter den initiala bedrägeritransaktionen sker penningtvätten ofta via skiktning med kontoöverföringar inom Sverige. Överföringarna kan i ett senare skede följas av att pengar skickas till utlandet, ibland i kombination med kontantuttag. Kontantuttag och utlandsöverföringar görs då ofta hos ombud för utländska betalningsinstitut.

1.2.2 Investeringsbedrägerier

Investeringsbedrägerier går ut på att vilseleda någon att föra över pengar i tron att det avser en placering i finansiella instrument, företag eller liknande. Kryptovaluta förekommer i många av rapporterna, vanligen för att den som utsätts har haft för avsikt att placera pengar i kryptovaluta men luras att betala till en plånbok som kontrolleras av någon annan.

Liksom i BEC-bedrägerierna är det vanligt att pengar skiktas med gränsöverskridande transaktioner. Större delen av rapporterna till Finanspolisen gäller svenska bankkunder som utsatts för bedrägeri och där pengarna skickats utomlands, vilket innebär att penningtvätten sker i en annan jurisdiktion. På motsvarande sätt rör rapporter om misstänkta mottagare i Sverige bedrägerier där målsägande finns i ett annat land och där det svenska målvaktskontot utgör ett led i penningtvätten. Företagsmålvakter är relativt vanligt, inte sällan med utländska ägarbolag. Från målvaktskonton i Sverige skickas pengarna ofta vidare till företag utomlands, exempelvis med falska fakturor som underlag för transaktionen. Ibland skiktas pengarna även med kreditkortsbetalningar eller med överföringar till privatpersoner.

1.2.3 Romansbedrägerier

I romansbedrägerier försöker bedragarna bygga en personlig relation för att förmå den som drabbas att låna ut eller skänka pengar. Upplägget kan också användas i syfte att rekrytera personer som målvakter.

Även i romansbedrägerier rapporteras fler drabbade än målvakter. Pengarna skickas ofta direkt utomlands men det händer att de går till målvaktskonton i Sverige och att den första delen av skiktningen görs inom landet. Det kan vara en kombination av kontoöverföringar till andra banker, Swish-betalningar och kontantuttag. Till skillnad från investeringsbedrägerier är målvakterna i romansbedrägerier nästan uteslutande privatpersoner

1.2.4 Vishingbedrägerier

Vishingbedrägerier innebär att gärningsmännen kontaktar någon per telefon och utger sig för att ha befogenheter, exempelvis i egenskap av banktjänsteman på den utsattes bank. På så sätt förmås den som kontaktats att utföra en handling som ger ekonomisk vinning till bedragarna. Motsvarande tillvägagångssätt via SMS (smishing) har också räknats in i vishingbedrägerierna i analysen.

I vishingbedrägerier förekommer det att pengarna skiktas med hjälp av kryptovaluta genom att den som utsätts förmås att föra över pengar till en kryptoplånbok som kontrolleras av gärningsmännen. Generellt sett tycks dock hanteringen av brottsvinster vara mindre sofistikerad jämfört med övriga modus i kategorin social manipulation. Det är ovanligt med gränsöverskridande transaktioner och penningtvättsåtgärderna är i allmänhet enklare. En förklaring till det kan vara att bedrägerierna snabbt upptäcks och bedragarna har kort tid på sig att säkra brottsutbytet. Pengarna går till privatkonton och tas ofta ut i kontanter, antingen direkt eller efter Swish-överföring till andra privatpersoner som i sin tur tar ut kontanterna.

1.3 Övriga bedrägerier

Utöver tillvägagångssätten i kategorierna ovan kan nämnas två andra typer av bedrägerier i rapporteringen till Finanspolisen; lånebedrägerier och annonsbedrägerier.

1.3.1 Lånebedrägerier

Det förekommer två varianter av lånebedrägerier i rapporteringen. Den som Finanspolisen får flest rapporter om gäller personer som söker lån med falska underlag för att på så sätt uppfylla kreditvillkoren, oftast för att finansiera ett bostadsköp. Detta upplägg är vanligt bland kriminella som har ekonomisk möjlighet att betala för lånen men gör det med illegalt intjänade medel. I de fallen blir bostaden och lånet verktyg för penningtvätt.

Den andra varianten innebär att gärningsmännen tar lån, själva eller med hjälp av bulvan, utan att ha för avsikt att betala tillbaka pengarna. Flera blancolån söks ofta samtidigt från olika kreditgivare för att komma över större belopp. Skiktningen sker typiskt sett via privatkonton och inom Sverige, åtminstone initialt. I senare led kan pengarna skickas utomlands via ombud för penningöverföring.

1.3.2 Annonsbedrägerier

I annonsbedrägerier vilseleds en person att betala för en utannonserad vara eller tjänst som antingen inte levereras eller visar sig vara falsk eller felaktig. Det kan också vara så att säljaren inte får betalt av köparen.

Det finns exempel på skiktning med hjälp av kryptovaluta där den som utsätts för över pengar till en kryptoväxlare i tron att det handlar om betalning för en vara. Rapporteringen tyder dock på att brottsvinster från annonsbedrägerier oftast tvättas i enklare upplägg och att pengarna i huvudsak stannar i Sverige. Det tycks vara relativt vanligt att pengarna tvättas eller konsumeras av samma personer som låg bakom bedrägeriet. I den mån målvakter används görs Swish-överföringar till ett målvaktskonto som direkt följs av kontantuttag.

2 Omfattning

Misstanke om att pengar härrör från bedrägerier är en vanlig anledning till att rapportera till Finanspolisen. Under 2020 hade nära en femtedel av misstankerapporterna bedrägerikoppling. Rapporterna kom i huvudsak från banker och rörde både kunder som blivit utsatta för bedrägerier och kunder som misstänks hantera bedrägerivinster. I ungefär hälften av fallen framgick det vilken typ av bedrägeri som misstanken gäller. Diagrammen nedan visar antal rapporter respektive summan av rapporterade transaktioner i de fall det gått att kategorisera rapporten efter bedrägerityp.

Observera att både antal och belopp ska tolkas med stor försiktighet eftersom mörkertalen skiljer sig väsentligt åt mellan bedrägerityperna och klassificeringen bygger på rapportörernas egen bedömning. Det finns även andra osäkerhetsfaktorer som kan göra att summan både över- och underskattas. Å ena sidan kan rapporterna innehålla transaktioner som inte är relevanta för det misstänkta bedrägeriet eller penningtvätten. Det kan också finnas dubbletter när en bank rapporterar utifrån att en kund blivit utsatt och en annan bank rapporterar samma transaktion för att en kund misstänks vara målvakt. Å andra sidan finns det också misstankerapporter där transaktionerna inte har rapporterats i strukturerat format och därför inte kommit med i statistiken alls.

Felkällorna ovan, och det faktum att endast omkring hälften av rapporterna kunnat kategoriseras, gör att det inte går att dra några slutsatser om omfattningen i absoluta tal. Statistiken kan dock ändå ge en bild av hur de olika kategorierna förhåller sig till varandra. Förhållandet mellan bedrägerityperna vad gäller antal respektive belopp ligger också i linje med sammanställningar som gjorts internationellt.[5]

Diagram 1 Antal rapporter 2020

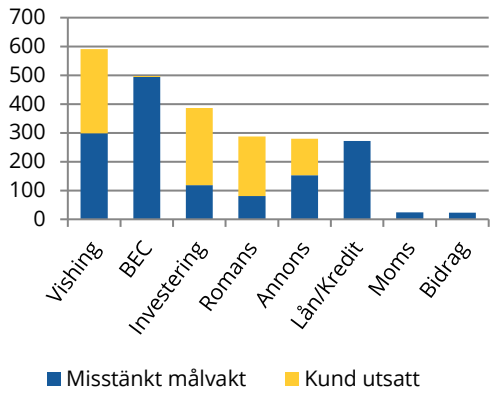
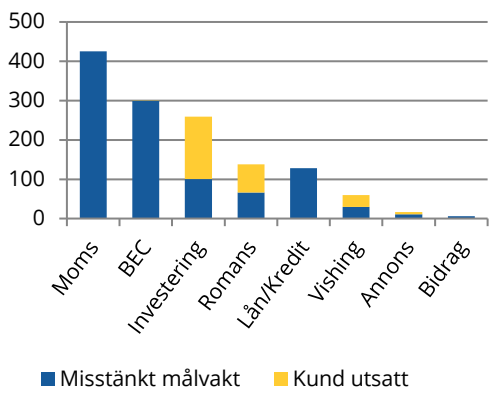


Diagram 2 Rapporterade belopp (mkr)



Både den faktiska omfattningen och mörkertalet bedöms vara särskilt stort för moms- och välfärdsbedrägerierna. Trots ett fåtal rapporter om momsbedrägerier summerar dessa transaktioner till mycket stora belopp, drygt 400 miljoner kronor på ett år. Vad gäller välfärdsbedrägerier är rapporteringen närmast obefintlig och omfattningen bedöms vara många

[5] Se till exempel Federal Bureau of Investigation, *2020 Internet Crime report.*

gånger större än vad statistiken visar. I den statliga utredningen om utbetalningar från välfärdssystemen bedömdes de avsiktligt felaktiga utbetalningarna uppgå till i storleksordningen 10 miljarder kronor årligen.[6]

I kategorin social manipulation märks BEC-bedrägerierna som genererar flest rapporter om misstänkta målvakter och summerar till stora belopp. Här är det värt att notera att BEC-rapporteringen nästan uteslutande rör bedrägerier mot företag i andra länder men där penningtvätten sker i Sverige. Vinster från BEC-bedrägerier som drabbar svenska företag tvättas i stället utomlands och eventuella rapporter skickas till Finanspolisens motsvarigheter internationellt. Staplarna avseende BEC i diagrammen ovan speglar därför omfattningen av den misstänkta penningtvätten, inte bedrägerierna, i Sverige.

Rapporterna om vishingbedrägerier är visserligen flest till antalet men här handlar det om betydligt mindre belopp som rapporteras, se diagram 2.

Mörkertalet i rapporteringen om bedrägerier med social manipulation bedöms vara litet jämfört med moms- och välfärdsbedrägerierna, särskilt för BEC- och vishingbedrägerier där en förhållandevis stor del sannolikt upptäcks och rapporteras. Vid romans- och investeringsbedrägerier finns däremot ett visst mörkertal eftersom det kan vara så att den som utsätts antingen inte är medveten om detta eller avstår från att anmäla. Romansbedrägerierna upptäcks oftast av banken som reagerar på avvikande transaktioner på kundens konton.

Rapporteringen om lånebedrägerier indikerar att omfattningen är mindre jämfört med kategorierna ovan men här finns troligen ett relativt stort mörkertal. Polisens underrättelser visar att lånebedrägerier används systematiskt inom organiserad brottslighet och att problematiken är mer utbredd än vad som framkommer i rapporteringen.

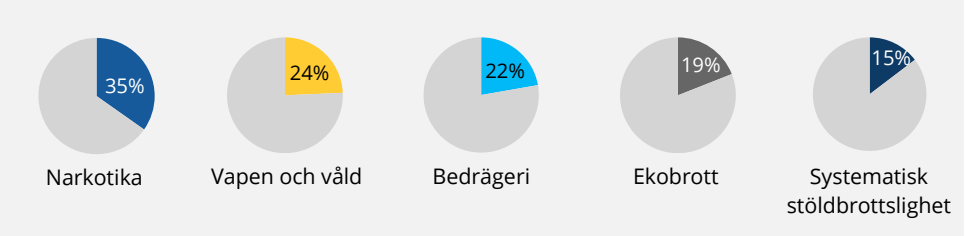
Annonsbedrägerierna är den bedrägerityp som omsätter lägst belopp. Antalet rapporter är visserligen högt men det handlar om små summor per rapport. Mörkertalet är sannolikt litet då den som drabbas upptäcker bedrägeriet relativt omgående och benägenheten att rapportera bedöms vara hög.

[6] Samlade åtgärder för korrekta utbetalningar frånvälfärdssystemen, SOU 2019:59.

3 Kriminella aktörer

Drygt hälften av de personer som misstankerapporteras till Finanspolisen i samband med bedrägerier förekommer i underrättelser om annan brottslighet än penningtvätt. Diagram 3 visar de brottsområden som flest personer i urvalet misstänks ha kopplingar till.[7] Som framgår av diagrammet är det vanligare med träffar på narkotikabrottslighet än på bedrägerier. Det bekräftar Finanspolisens bild att det handlar om multikriminella aktörer och att det är stor risk att bedrägerivinsterna återinvesteras i annan allvarlig brottslighet. Bedrägeribrottsligheten utgör med andra ord ytterligare en inkomstkälla för kriminella nätverk som står bakom organiserad narkotikahandel och skjutvapenvåld.

Diagram 3 Andel rapporterade personer med koppling till olika brottsområden

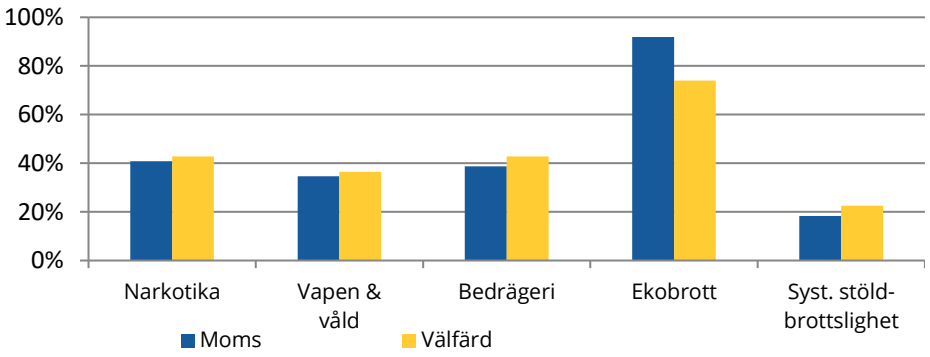


3.1 Moms- och välfärdsbedrägerier

Hela 85 procent av dem som rapporterats i samband med moms- och välfärdsbedrägerier finns i annat underrättelsematerial hos Polisen. Den höga andelen säger dock troligen mer om verksamhetsutövarna förmåga att upptäcka bedrägerierna och mörkertalet i rapporteringen än om aktörerna. De få rapporter som finns är nämligen ofta resultatet av en fråga från Polisen eller Ekobrottsmyndigheten som gjort verksamhetsutövaren uppmärksam på personer och företag som redan är kända av brottsbekämpande myndigheter.

Merparten av underrättelserna rör ekonomisk brottslighet som exempelvis skattebrott, se diagram 4. Momsbedrägerier och systematiska välfärdsbedrägerier förutsätter hög ekonomisk kapacitet och god organisationsförmåga. Aktörerna behöver tillgång till legala samhällsstrukturer för att starta eller överta bolag, ibland i flera länder.

Diagram 4 Andel med koppling till andra brottsområden – välfärdsbedrägerier



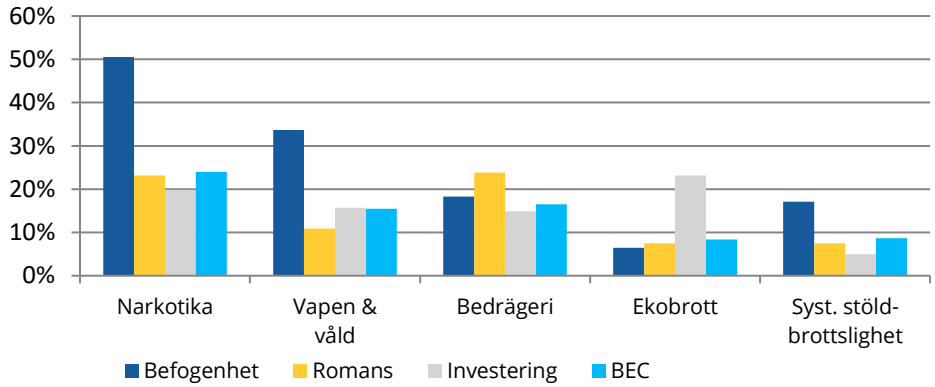
[7] Urvalet består av ca 2000 personer som under 2020 antingen själva misstankerapporterats i samband med bedrägerier eller företräder bolag som rapporterats för misstänkt moms- eller välfärdsbedrägeri.

Narkotika- och våldsbrottslighet är också relativt vanligt och framför allt aktörerna bakom välfärdsbedrägerierna bedöms ha tillgång till våldskapital. Det är den bedrägerityp med störst andel rapporterade i kriminella grupperingar, bland annat släktbaserade nätverk och kriminella MC-gäng. Här finns även enstaka kopplingar till brottsaktiv extremism och till korruption.

3.2 Social manipulation

Hälften av dem som rapporterats i samband med vishingbedrägerier förekommer i underrättelser om narkotika eller vapen- och våldsbrottslighet, se diagram 5. Bland aktörerna finns kopplingar till flera kriminella nätverk och var tionde person är skriven i ett utsatt område, vilket är en högre andel jämfört med andra bedrägerityper. De som misstankerapporterats i samband med vishingbedrägerier har den lägsta genomsnittsåldern, cirka 30 år, och mer än var sjunde person är 20 år eller yngre. Underlaget indikerar att unga i utsatta områden utnyttjas som målvakter i uppläggen.

Diagram 5 Andel med koppling till olika brottsområden – social manipulation



För övriga tillvägagångssätt med hjälp av social manipulation är det färre träffar i underrättelsematerialet. En förklaring till det kan vara att personer utanför kriminella kretsar utnyttjas som målvakter. I romansbedrägerierna är det till exempel inte ovanligt att den som utsätts luras till att fungera som målvakt i ett bedrägeri som riktas mot någon annan. Ett tecken på det är en högre andel kvinnor som misstankerapporteras för romansbedrägerierna. Andelen rapporterade kvinnor är nästan 50 procent att jämföra med omkring 30 procent för övriga bedrägerier. Romansbedrägerierna drabbar också kvinnor i betydligt större utsträckning än män.

I rapporterna om BEC-bedrägerier finns en tydlig överrepresentation av misstänkta personer bosatta i Sverige som har nigerianskt och annat västafrikanskt ursprung. Det ger anledning att misstänka att ett visst kriminellt nätverk med rötter i dessa länder utövar påtryckning mot sina landsmän för att agera målvakt. Nätverket, som är aktivt i ett stort antal länder, är relativt välorganiserat och besitter ett ansenligt våldskapital.

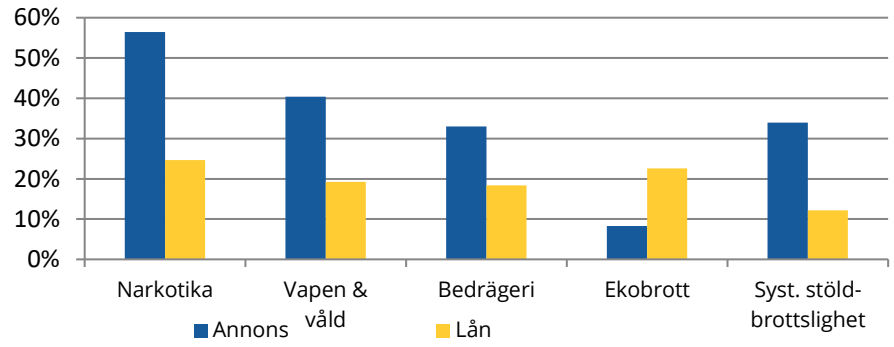
Även när det gäller romansbedrägerierna finns tecken på att samma nätverk i vissa fall ligger bakom men det bedöms inte finnas samma systematik i rekryteringen av målvakter som i BEC-bedrägerierna.

I investeringsbedrägerierna finns en övervikt mot annan ekonomisk brottslighet bland aktörerna, vilket också kan förväntas. Upplägen förutsätter hög ekonomisk kapacitet, även om de i allmänhet ställer lägre krav på organisation och infrastruktur än moms- och välfärdsbrotten. Investeringsbedrägerierna är den bedrägerityp där de misstankerapporterade har högst genomsnittsålder, drygt 50 år.

3.3 Övriga bedrägerier

En stor del av dem som rapporterats till Finanspolisen i samband med annonsbedrägerier misstänks ha kopplingar till narkotika, vapen och våld, se diagram 6. Relativt många förekommer också i underrättelser om systematisk stöldbrottslighet. Bland aktörerna finns kopplingar till ett antal kriminella grupperingar, bland annat kriminella MC-gäng. Underlaget tyder på en lägre organisationsnivå i förhållande till andra kategorier och penningtvätten tycks i högre grad hanteras av samma personer som utför bedrägerierna.

Diagram 6 Andel med koppling till olika brottsområden – övriga bedrägerier



Bland personerna i rapporter om misstänkta bolånebedrägerier är det färre som förekommer i annat underrättelsematerial och de träffar som finns är relativt jämnt fördelade mellan olika brottsområden.

En förklaring till få träffar kan vara att aktörerna använder bulvaner som rekryteras utanför den kriminella sfären. Underrättelser från bland annat Encro-materialet visar att lånebedrägerier förekommer frekvent inom organiserad brottslighet.[8] Bakom upplägen finns möjliggörare som erbjuder tjänster som att förmedla insiderkontakter på banker, rekrytera målvakter eller tillhandahålla falska anställningsintyg.

Några av rapporterna rör blancolån där förövaren inte har för avsikt att betala tillbaka pengarna. Här är det vanligare att personerna finns i annan underrättelseinformation och träffarna indikerar att lånen i vissa fall syftar till att finansiera brottsaktiv extremism.

[8] Encro-materialet syftar på innehållet i den krypterade kommunikationstjänsten Encrochat. Tjänsten användes i princip uteslutande av kriminella aktörer inom grov narkotikabrottslighet i Europa, bland annat i Sverige.

4 Hotet ur ett brottsvinstperspektiv

Ekonomisk vinning är en stark drivkraft för organiserad brottslighet och bedrägerier är en lukrativ inkomstkälla. Bedrägerierna omsätter stora summor som kan återinvesteras i brottsligt verksamhet och användas för att rekrytera till kriminella miljöer.

Genomgången visar att det finns strukturella skillnader mellan de kriminella aktörerna bakom olika typer av bedrägerier i fråga om ekonomisk kapacitet, organisationsförmåga och tillgång till våldskapital med mera. Bedrägeriernas omfattning och komplexitet skiljer sig också åt. Ju större omsättning och ju högre kapacitet hos aktörerna, desto allvarligare är hotet från bedrägerierna.

Tabell 1 jämför hotnivån ur ett brottsvinstperspektiv. Jämförelsen gör ingen värdering av skada eller vem som drabbas utan baseras enbart på en skattning av brottsvinsternas omfattning, de kriminella aktörernas förmåga och risken att pengarna återinvesteras i organiserad brottlighet. Med den utgångspunkten bedöms bedrägerierna mot offentlig verksamhet utgöra det största hotet, se tabell.

Tabell 1 Jämförelse av hotnivå utifrån omfattning och aktörer

Högst hotnivå	**Moms – och välfärdsbedrägerierna** bedöms utgöra det största hotet ur ett brottsvinstperspektiv. Brotten genererar mångmiljardbelopp årligen som kan återinvesteras i annan allvarlig brottslighet. Aktörerna har hög ekonomisk och organisatorisk förmåga och tydliga kopplingar till organiserad brottslighet. I samband med de bidragsrelaterade brotten förekommer även misstankar om korruption.
Lägre hotnivå	**BEC-bedrägerier** utgör ett lägre men fortfarande betydande hot mot bakgrund av omfattningen, den systematiska rekryteringen av målvakter och organisatörernas koppling till organiserad brottslighet. Även **lånebedrägerier** omsätter stora summor och möjliggör för grovt kriminella att tillgodogöra sig brottsvinster genom ägande av bland annat fastigheter. Upplaggen skapar också incitament för att rekrytera möjliggörare, som bankinsiders. **Vishingbedrägerierna** genererar lägre vinster men har störst andel rapporterade personer med koppling till annan brottslighet och till kriminella nätverk. Det finns också tecken på att unga i utsatta områden utnyttjas som målvakter.
Lägst hotnivå	**Romans- och investeringsbedrägerier** riktas i huvudsak mot enskilda individer och det bedöms inte finnas samma systematik i rekryteringen av målvakter som i exempelvis BEC-bedrägerierna. Hotet bedöms därför vara mer begränsat, trots att vinsterna kan uppgå till relativt stora belopp. **Annonsbedrägerierna** omsätter små belopp i sammanhanget och utgör därför också ett begränsat hot. Bland aktörerna finns kopplingar till kriminella nätverk men det tycks inte finnas någon högre grad av organisation bakom bedrägerierna och penningtvätten.

5 Sårbarhetsreducerande åtgärder

För att minska det hot som bedrägerierna utgör sett till brottsvinster och penningtvätt behöver ett antal sårbarheter täppas till. Det handlar om att stärka verksamhetsutövarnas förmåga att upptäcka och förhindra bedrägerierna innan de sker men också om ökad kontroll hos utbetalande myndigheter i samband med moms- och välfärdsbedrägerier.

5.1 Skärpt kontroll vid utbetalning av bidrag

För att upptäcka och förhindra välfärdsbedrägerierna krävs framför allt skärpt kontroll hos de utbetalande myndigheterna. Bankernas förmåga att upptäcka transaktioner kopplat till välfärdsbedrägerier är begränsad och mörkertalet i rapporteringen till Finanspolisen bedöms vara mycket stort. Den främsta anledningen till det är att utbetalningar från myndigheter som till exempel Försäkringskassan och Arbetsförmedlingen förutsätts vara legitima.

Regeringen har tillsatt en utredning om stärkta möjligheter att bekämpa bidragsbrott för myndigheter som omfattas av bidragsbrottslagen.[9] Utredningen ska titta på hur hanteringen hos de utbetalande myndigheterna kan förbättras och hur samverkan mellan myndigheter kan effektiviseras.

5.2 Övervakning av skattekonton med avseende på penningtvättsrisker

Skatteverket omfattas inte av utredningsuppdraget ovan och det finns för närvarande inga krav på systematisk övervakning från Skatteverkets sida för att upptäcka misstänkta transaktioner till och från skattekonton. Däremot är Skatteverket en av de myndigheter från vilka utbetalningar kan komma att samlas hos en ny myndighet. Utredningen om samordning av statliga utbetalningar från välfärdssystemen föreslog i sitt betänkande att inrätta en ny myndighet i syfte att förebygga, förhindra och upptäcka felaktiga utbetalningar.[10]

Övervakning av skattekonton vore en viktig åtgärd, inte bara för att komma tillrätta med momsbedrägerierna utan också för att minska risken att kontona utnyttjas för penningtvätt generellt sett. Som exempel kan nämnas underrättelser om att kriminella använder skattekonton som mellanstation vid försäljning av kryptovaluta. Genom att studsa pengarna från försäljningen via skattekontot kan aktörerna undgå upptäckt i bankernas monitorering.

En svårighet för bankerna när det gäller att upptäcka momsbedrägerier är att de inte kan se vad utbetalningar från Skatteverket avser. Alla flöden samlas på skattekontot och endast nettobeloppet betalas ut. Utan bakgrundsinformation om pengarna har bankerna små möjligheter att upptäcka oegentligheter. Det finns dock indikationer på att skattekonton utnyttjas för penningtvätt som även bankerna skulle kunna fånga upp, till exempel:

- Pengar sätts in på skattekonto för att kort därefter föras tillbaka eller tas ut kontant.
- Pengar sätts in på ett skattekonto från olika håll.
- Inkomster som inte rimmar med de belopp som överförs från skattekonton.

[9] Kommittédirektiv 2021:39.

[10] SOU 2020:35.

5.3 Mer kundanpassad monitorering av företagskonton

Huvudansvaret för att upptäcka moms- och välfärdsbedrägerierna vilar rimligen på de utbetalande myndigheterna men bankerna bör också kunna bli bättre på att upptäcka dessa, framför allt upplägg som involverar företag. Som tidigare nämnts får Finanspolisen exempelvis in misstankar om att pengar härrör från bidragsfusk hos enstaka individer men ytterst få rapporter om mer systematiska bedrägerier via exempelvis assistansbolag.

Transaktionsmönster på privatkonton är relativt enhetliga medan företagstransaktioner kan variera avsevärt, både över tid och mellan olika verksamheter. För att kunna upptäcka avvikelser behöver monitoreringen därför i högre grad anpassas utifrån kundkännedom om företagen och här bedömer Finanspolisen att det finns stor förbättringspotential. Bankernas begränsade förmåga att upptäcka misstänkta transaktioner på företagskonton utgör en sårbarhet i bekämpningen av penningtvätt och finansiering av terrorism, särskilt som de storskaliga upplägen bygger på nätverk av företag.

Det finns ett antal varningsflaggor som kan öka chansen till upptäckt av penningtvätt via företagskonton i allmänhet och momsbedrägerier i synnerhet, bland annat:

- ”Studskonton” där pengar sätts in bara för att snabbt betalas ut igen.
- Orimligt snabb omsättningsökning på företagskonton.
- Kontoomsättning som inte står i proportion till företagets lokal- eller personalkostnader.
- Inbetalningar på höga belopp från stora bolag till små nystartade bolag eller bolag med ny styrelse.
- Transaktioner i bolag med befattningshavare utan erfarenhet av branschen och med inslag av utländsk expertis.

5.4 Teknisk lösning för att förebygga BEC-bedrägerier

Trots att det borde vara tekniskt möjligt att identifiera och förebygga BEC-bedrägerierna så uppmärksammar flertalet av bankerna problemet först när pengarna redan finns på kontot eller i värsta fall har skickats vidare. Här skulle det behövas tekniska lösningar för att identifiera försök till BEC-bedrägerier och stoppa transaktionen innan betalningen går igenom.

5.5 Säkrare distansinloggning kan minska risken för vishingbedrägerier

Även när det gäller vishingbedrägerierna kan verksamhetsutövarna vidta förebyggande åtgärder. En del handlar om att säkerställa att kunderna förstår hur produkter för distansinloggning ska användas och vilka risker som finns. Vid inloggning på distans bör det också göras en kontroll av att de enheter som används befinner sig på samma geografiska plats.

Viss fördröjning innan nya digitala tjänster fungerar fullt ut kan också bidra till att minska risken för bedrägerier. Det kan till exempel vara en begränsning av hur stora belopp som kan överföras med en ny tjänst under en testperiod.

Ytterligare ett område som kan förbättras gäller kundkännedom och monitoreringen av transaktionerna utifrån denna.

5.6 Ökad kontroll vid kreditgivning

Att lån beviljas på felaktiga grunder kan bero på bristande kontroll men det förekommer även möjliggörare i form av insiders som beviljar krediterna.[11]

Tänkbara sårbarhetsreducerande åtgärder kopplat till lånebedrägerier är:

- Förbättrad digital identifiering eller utökad fysisk kundkontakt samt verifiering av arbetsgivarintyg och liknande underlag.
- Skärpt kontroll och säkerhetssamtal vid anställning för att undvika att banktjänstemän utsätts för intressekonflikter. Central handläggning, roterande kundrelationer och dualitet i handläggningen kan också minska risken att lån beviljas av insiders.

[11] Se även Fipo informerar om insiderproblematik på bankerna, juni 2021.