2024-05-07

Justitiedepartementet
Finansdepartementet

UPPTRAPPADE ÅTGÄRDER MOT AKTIVA BEDRÄGERINÄTVERK

Svenska Bankföreningen hemställer om att regeringen vidtar åtgärder för att skapa förbättrade förutsättningar för brottsbekämpande myndigheter att motverka den organiserade bedrägeribrottsligheten. Förslagen enligt denna hemställan är sammanfattningsvis följande.

1. Brottsbekämpande myndigheter ges ett uttryckligt uppdrag och tillräckliga resurser för att kunna ligga i framkant och besitta den senaste tekniken och IT-kompetensen.
2. Brottsbekämpande myndigheter ges ett uttryckligt uppdrag att införa adekvata rutiner för att sprida information som är nödvändig för att förebygga, upptäcka och rapportera brott.
3. Brottsbekämpande myndigheter ges ett uttryckligt uppdrag att samordna och centralisera handläggningen av den organiserade grova bedrägeribrottsligheten till den myndighet eller enhet som har bäst förutsättningar för en snabb och effektiv utredning samt lagföring.
4. Införande av ett lagstadgat skyndsamhetskrav i förhållande till Polismyndighetens eller Säkerhetspolisens beslut om dispositionsförbud.

Besök (Visit):
Blasieholmsgatan 4B
Stockholm
Sverige (Sweden)

Post:
Box 7603
SE-103 94 Stockholm
Sverige (Sweden)

t: +46 (0)8 453 44 00

e: info@swedishbankers.se
www.swedishbankers.se

Bakgrund
Kriminella nätverk som i allt större omfattning sysslar med organiserade telefonbedrägerier mot framförallt äldre personer har under senare tid hamnat i fokus. Ett par uppmärksammade reportage i media har belyst tillvägagångssättet för dessa bedrägerier.[1] Det har framgått att de kriminella nätverken är cyniska, hänsynslösa och överhuvudtaget förefaller ta till alltmer offensiva metoder. Nätverken nyttjar möjligheterna att identifiera och filtrera grupper av tilltänkta offer via offentliga källor, nyttja massutskick av SMS med falskt innehåll[2], vid personlig telefonkontakt stressar och manipulerar nätverken bankkunden att invaggas i tron att denne talar med till exempel bankens säkerhetsavdelning.

Det är fråga om kriminella nätverk som arbetar yrkesmässigt och inte sällan sysslar med olikartad grov brottslighet som kan innefatta även narkotikahandel och våld. Det är alltså ingen främmande tanke att nätverken kan finansiera inköp av narkotika och vapen eller ersätta utförare av våldsbrott med utbyte från telefonbedrägerier.[3]

Bankerna vidtar åtgärder
På regeringens uppdrag arbetar bankerna för närvarande intensivt för att ta fram ett omfattande åtgärdsprogram för att stärka bankkundernas skydd mot bedrägerier, i möjligaste mån utan att hindra den omfattande mängd legala överföringar eller betalningar som dagligen sker mellan privatpersoner.

Utan att i detalj gå in på de enskilda åtgärderna, är det i huvudsak fråga om anpassning av produktutbud i förhållande till betalningar, strävan efter en bankgemensam infrastruktur samt begränsningar av konton för kriminella till att avse endast basala funktioner.[4]

Bakgrunden till åtgärdsförslaget är att regeringen, VD:arna för de sex största bankerna i Sverige, Svenska Bankföreningens vd och Polisen sammanträdde i februari 2024 för att diskutera hur arbetet mot bedrägerier kan stärkas och hur samverkan mellan bankerna och Polisen kan förbättras.

Utöver ett anpassat produktutbud och övriga åtgärder har de enskilda bankerna en transaktionsövervakning som är under ständig utveckling för ökad precision i syfte att motverka bedrägerier.

---

[1] SVT:s Uppdrag Granskning i januari respektive mars 2024.
[2] Jfr. Svenska Bankföreningens framställning den 15 maj 2023 om att motverka spoofing.
[3] Jfr. Polismyndighetens rapport ”De dödliga bedrägerierna” (Dnr A554.314/2022).
[4] Åtgärdsförslaget utarbetas genom Svenska Bankföreningen av en arbetsgrupp med representanter från Danske Bank, Handelsbanken, ICA Banken, Länsförsäkringar Bank, Nordea, SEB och Swedbank.

Sammantaget genomför bankerna åtgärder som bedöms medföra starkt ökade förutsättningar att begränsa de kriminella nätverkens genomförande av storskaliga telefonbedrägerier. Bankerna är inte främmande för att vidta ytterligare åtgärder om de bedöms adekvata och behövliga för att motverka fortsatta bedrägerier av olika typ.

Brottsbekämpande myndigheter behöver ges förbättrade förutsättningar
Regeringens uppdrag till bankerna att presentera åtgärder innefattade även en möjlighet att inkomma med förslag med bäring på andra aktörer av betydelse för bedrägeripreventionen och bedrägeribekämpningen.

Även om bankernas arbete med bedrägeriprevention är betydelsefullt åligger det myndigheterna, i första hand polis och åklagare, att genom förebyggande åtgärder, utredning och åtal bekämpa denna brottslighet.

Att de kriminella nätverken redan verkat storskaligt under en viss tid står klart.[5] Kontakterna i brottsliga syften gentemot bland andra bankkunder har ökat. Det sammanlagda brottsutbytet har ökat och utgör idag en betydelsefull inkomstkälla för nätverken, som i många fall sysslar med även annan brottslighet än bedrägerier. Åtal och fällande domar avseende dessa nätverk har ännu inte kunnat iakttas i någon större omfattning, även om det är rimligt att utgå ifrån att polis och åklagare arbetar efter bästa förmåga utifrån dagens förutsättningar.

Polisen har offentligt meddelat att man känner till cirka 20 stycken olika ”grupperingar” eller kriminella nätverk som sysslar med storskaliga telefonbedrägerier av liknande slag som datahackaren avslöjat.[6] Det är av stor vikt att tillräckligt skyndsamma och offensiva åtgärder vidtas för att sätta stopp för brottsligheten[7] – att de kriminella nätverken inte tillåts att verka mer eller mindre ostört.

Uppgiftsinhämtning från ”datahackare”
I brottsbalken (1962:700) regleras straffansvaret för den som *olovligen* vidtar olika åtgärder i ett datasystem.[8]

---

[5] Jfr. Polismyndighetens rapport ”De organiserade bedrägerierna” (Dnr A354.340/2021).
[6] SVT:s Uppdrag Granskning i mars 2024. Programmet visade bland annat hur en anonym privatperson i skepnad av en ”datahackare”/”systemknäckare” på egen hand lyckats såväl avläsa som intervenera i den omfattande bedrägeribrottslighet som bedrivs av ett kriminellt nätverk.
[7] Detta särskilt mot bakgrund av bland annat att en enskild person, det vill säga datahackaren (se fotnot 6), på eget bevåg och med privat teknisk utrustning har kunnat vidta omfattande åtgärder för att identifiera och kartlägga ett specifikt kriminellt nätverk. Det kan härvid noteras att datahackaren även i realtid kunnat förhindra brott
[8] 4 kap. 9 c § brottsbalken

Hemlig dataavläsning (HDA)[9] innebär att en domstol ger åklagare och polis tillstånd att vidta vad som annars i allmänhet skulle anses vara ett dataintrång – åtgärden sker alltså per definition inte *olovligen*. En enskild person, som inte har formella möjligheter att erhålla domstols tillstånd till HDA, gör sig således skyldig till dataintrång om denne tar sig i någon annans dator eller mobiltelefon för att utföra såväl avläsning som intervention.

Den typ av åtgärder som datahackaren utfört är därmed i normalfallet straffbara enligt svensk lag. Trots detta samarbetar polis och åklagare med datahackare såtillvida att man i vart fall upprepat tagit emot material som kan användas inom ramen för en förundersökning och så småningom åberopas som bevisning i svensk domstol.

Mot bakgrund av problembilden med organiserade bedrägerier i samhället finns goda grunder för att polisen väljer att agera på detta vis.

Förfarandet belyser dock en brist i förhållande till brottsbekämpande myndigheters förutsättningar att såväl förhindra pågående brottslighet som att på egen hand inhämta bevisning av sådan typ som det här är fråga om. I det långa loppet är det knappast tillfredställande att från myndighetshåll förlita sig på information från en enskild, som trots allt begår relativt allvarlig brottslighet (möjligen *grovt* dataintrång) när denne inhämtar informationen.

IT-tekniska förutsättningar

Det är berättigat att ställa sig frågan om brottsbekämpande myndigheter i tillräcklig omfattning disponerar den tekniska utrustning och kunskap som krävs för att kunna genomföra den typ av offensiva åtgärder som är påkallade. I praktiken kan det alltså handla om till exempel att på ett tillräckligt rättssäkert sätt genom HDA[10] bereda sig full access till en bedragares dataenhet för såväl avläsning som intervention. Det kan avse inte enbart dataenheter som befinner sig i Sverige, utan även i övriga delar av världen.[11] Nätverkens bedrägeribrottslighet är i hög grad internationell och rörlig.

Förutom verktyg för övervakning och avläsning behöver brottsbekämpande myndigheter tillgång till avancerad IT-teknik för att kunna bearbeta, sammanställa och analysera stora mängder information på ett automatiserat vis med hjälp av till

[9] Åtgärden regleras genom lagen (2020:62) om hemlig dataavläsning.
[10] Det är av vikt att HDA, vars motiv utifrån användning av ny avancerad teknik och AI blir alltmer relevanta i jämförelse med andra hemliga tvångsmedel, når en tillräcklig mognad och används på det mest effektiva sättet.
[11] Att detta är tekniskt genomförbart visar inte minst datahackaren, som besitter obetydliga resurser i jämförelse med brottsbekämpande myndigheter. De legala förutsättningarna behandlas i det följande.

exempel AI.[12] Sådana analyser har potential att avslöja mönster och trender, vilka i sin tur kan användas för att prioritera och fatta ändamålsenliga operativa beslut.[13]

Vidare kräver ett anskaffande av den senaste tekniken att brottsbekämpande myndigheter ges förutsättningar för rekrytering av personal med stor kompetens inom ”digital brottsbekämpning” med hjälp av till exempel AI. Detta för att tekniken ska kunna utnyttjas fullt ut.

Sammantaget etableras på så vis en god beredskap för bekämpning av en alltmer avancerad och internationell brottslighet. Om de kriminella nätverken framöver i större omfattning övergår till användande av exempelvis AI behöver korresponderande proaktiva motåtgärder vidtas.

Regeringen bör härvid tillse att brottsbekämpande myndigheter ges ett tydligt uppdrag och tillräckliga resurser för att säkerställa att de ligger i framkant och besitter den senaste tekniken och IT-kompetensen som kan utnyttjas på ett snabbt och effektivt sätt – att genom ”digital brottsbekämpning” kunna nyttja HDA och andra liknande åtgärder.[14]

Hemlig dataavläsning och intervention mot rörliga internationella nätverk
En grundläggande regel för polisiär verksamhet följer av 2 § polislagen (1984:387), nämligen att det är polisens uppgift och ansvar att förebygga brottslig verksamhet. Om polisen får kännedom om ett förestående brott, till exempel ett grovt bedrägeri, genom vad som framkommer i en pågående HDA eller på annat vis, ska brottet om möjligt avvärjas genom polisens ingripande.[15]

En förklaring till att brottsbekämpande myndigheter inte alltid vidtar åtgärder och därmed förhåller sig passiva kan i vissa fall vara antaganden om att nätverken verkar från utlandet.[16]

---

[12] Under förutsättning att detta bedöms som tillräckligt säkert och tillförlitligt. Stadskontoret har under 2024 i rapporten ”Myndigheterna och AI” utvecklat frågorna om användningen av AI och därvid framhållit att det finns skäl för regeringen att förtydliga styrningen av myndigheternas roll inom området.
[13] För bankernas del kan AI användas för att till exempel skapa bättre precision i transaktionsövervakningen, dvs. minska andelen falska träffar.
[14] Enligt *Polismyndighetens* och *Åklagarmyndighetens* regleringsbrev 2024 ska återrapportering avse bland annat hur myndigheterna har säkerställt en ökad operativ förmåga att bekämpa grova brott med koppling till kriminella nätverk och för specifikt Polismyndighetens del hur man säkerställt att den tekniska förmågan kontinuerligt utvecklas och anpassas efter brottsutvecklingen.
[15] I vissa fall har polisen möjlighet förhålla sig passiv under en viss tid, och istället enligt ett visst förfarande dokumentera brottet i bevissyfte för lagföring vid ett senare tillfälle, s.k. *interimistisk passivitet*.
[16] Då i första hand utanför den krets av länder som tillämpar förenklade och standardiserade förfaranden för rättsligt samarbete i form av europeisk utredningsorder (EIO) respektive europeisk arresteringsorder (EAW).

I detta avseende kan det vara värt att påtala att det i många fall initialt är oklart varifrån brottslighetens bedrivs, och att antaganden om den saken inte bör förhindra brottsförebyggande eller brottsutredande åtgärder i Sverige. Det torde även i många fall förhålla sig på det viset att de kriminella nätverken verkar delvis från Sverige, såtillvida att det finns personer här som sköter praktiska detaljer eller agerar målvakter.[17] Om det framkommer att nätverken helt eller delvis verkar från utlandet, vilket i praktiken kan handla om att ett och samma nätverk verkar från flera olika länder, återstår att hantera denna situation utan att för den skull låta brottsligheten fortgå.

Det aktiva handlande som konstituerar genomförandet av brottet sker i Sverige – det är här som en bankkund mottar en bedräglig kontakt, legitimerar sig, loggar in och vidtar åtgärder för att överföra pengar. Det är i Sverige som bankkunden blir vilseledd av det kriminella nätverket. Det är även i Sverige som nätverket får utbyte av brottet och möjlighet att disponera över detta, för att därefter föra det till annat land. Effekten av brottet har inträtt i Sverige. Brottet är även helt och hållet riktat mot svenska intressen. En svensk domstol är därmed behörig att döma över brottsligheten. Med domsrätten följer att svenska tvångsmedel kan tillämpas.

Myndighetsutövning på annat lands territorium är i normalfallet inte tillåten med beaktande av den allmänna folkrättsliga *territorialprincipen*.

Ett rimligt antagande är att de kriminella nätverken använder såväl fasta som mobila internetuppkopplingar i kombination med internetbaserade molntjänster /applikationer, och att det därmed kan råda oklarhet om var exempelvis servrar är lokaliserade (s.k. ”loss of location”). Det kan vara fallet även om det finns uppgifter om var nätverket eller delar av det *vid en viss tidpunkt* befinner sig – det är av vikt att notera att dessa personer[18] ofta är rörliga och flyttar sin enhet/dator mellan olika länder.

Att under sådana omständigheter låta territorialprincipen förhindra utredningen av allvarlig brottslighet förefaller vara ett obsolet synsätt.[19]

---

[17] Jfr. Svenska Bankföreningens framställning 2023-09-25 om ett målvaktsregister.
[18] HDA kan användas för att utreda vem som skäligen kan misstänkas för brottet. Åtgärden ska alltid vara av synnerlig vikt för utredningen, vilket inte torde vålla några betänkligheter i de aktuella fallen.
[19] HD anger i Ö 5686-22 att territorialprincipen har utvecklats i tider då verkställighetsåtgärder vanligen förutsatte att myndighetsföreträdare var fysiskt närvarande på platsen för verkställigheten. HD uttalar vidare att det inte alltid är självklart hur principen ska förstås när en sådan företrädare genomför en åtgärd som berör en annan stat utan att beträda den statens territorium.

För övrigt är det i allmänhet svårt att se hur ett annat land skulle invända aktivt mot svenska försök att utreda eller intervenera mot denna typ av brottslighet, vilken drabbar enbart svenska intressen och som skulle innebära att en svensk myndighetsföreträdare inte ens beträder det andra landets territorium. Det kan även i allmänhet vara värt att fråga sig om intressen från länder som motverkar möjligheterna till effektiva svenska brottsutredningar ska tillåtas bli bestämmande.

I detta sammanhang kan påtalas att det är tillåtet att vidta ett annat ingripande tvångsmedel utan att territorialprincipen blir avgörande, närmare bestämt *genomsökning på distans*.[20] Vad som skiljer HDA från genomsökning på distans är i huvudsak att det förstnämnda antagligen förutsätter installation av mjukvara på en enhet i syfte att kringgå autentisering och att åtgärden används för fortlöpande övervakning. Genomsökning på distans är tillåtet när det såväl är känt att informationen är lagrad i ett visst land som när *loss of location* föreligger.

I likhet med bestämmelserna om genomsökning på distans saknar bestämmelserna om HDA begränsningar till avläsning av information inom Sverige. Vidare ställer lagen (2020:62) om hemlig dataavläsning inga krav på att domstolens beslut om åtgärden ska innehålla uppgift om till exempel IP-nummer, utan identifiering ska ske av ett visst ”avläsningsbart informationssystem” [21], vilket skapar flexibilitet i förhållande till bland annat var i världen ett sådant system befinner sig.

Till syvende och sist är det upp till varje enskild åklagare och slutligen domstol att bedöma om förutsättningar för till exempel HDA föreligger, men en alltmer internationell och avancerad brottslighet i kombination med tekniska framsteg kan medföra skäl att ompröva och revidera gamla principer.[22] Det allmänna intresset av att en gång för alla sätta stopp för dessa nätverk måste anses vara mycket stort.

Värt att påtala är vidare att det i vissa fall kan visa sig finnas begränsade möjligheter för svensk domstol att lagföra en misstänkt. Det kan röra sig om att personen kan antas befinna sig i ett land där överlämning eller utlämning till Sverige inte är ett gångbart alternativ.[23] Istället för att inhämta ytterligare uppgifter genom HDA kan intervention utgöra en framkomlig väg för att i vart fall få stopp på brottsligheten, markera att myndigheterna är det kriminella nätverket på spåren och att beteendet är

[20] Jfr. HD Ö 5686-22.
[21] En teknikneutral formulering som innefattar även framtida teknisk utrustning (SOU 2017:89, s 338)
[22] Regeringen har, utan att anse sig ha underlag för närmare övervägande av frågan om exekutiv jurisdiktion utanför Sverige, konstaterat att det för en effektiv brottsbekämpning är angeläget att reglerna om tillgång till elektronisk bevisning kan tillämpas i praktiken, även när informationen finns utanför Sverige eller när det är okänt var den finns (jfr. prop. 2021/22:119 s. 85 f.).
[23] I allmänhet är inte heller överförande av lagföring till annat land ett gångbart alternativ i dessa situationer.

oacceptabelt. Kan man systematiskt och med uthållighet intervenera eller obstruera på teknisk väg mot nätverkets verksamhet är mycket vunnet, även om lagföring alltså får stå tillbaka.

För det fall tillräckligt offensiva åtgärder för att sätta stopp för de kriminella nätverken inte kan vidtas under rådande legala förutsättningar, bör övervägas om lagstiftaren behöver modernisera lagstiftningen för att kunna angripa nuvarande och framtida brottslighet.[24] I ett sådant sammanhang torde frågan om exekutiv jurisdiktion utanför Sverige vara av särskilt intresse.

Kartläggning och informationsdelning

Det står klart att de kriminella nätverk som utför storskaliga telefonbedrägerier ofta är såväl omfattande som välorganiserade, med definierade roller inom uppläggen. För att få en sammanhållen och fullständig bild över de kriminella nätverken, deras medlemmar och eventuella anknytningar sinsemellan krävs en sammanhållen organisation som har förmåga att överblicka och kartlägga mer än en begränsad del.

Det är brottsbekämpande myndigheter som har verktygen och kunskapen att genomföra sådana kartläggningar, inte enskilda verksamhetsutövare såsom banker.

Kartläggningar och analyser av de kriminella nätverken och deras verksamhet – som brottsbekämpande myndigheter redan idag genomför på ett adekvat sätt – behöver omsättas och delas till inte bara de egna utredningsverksamheterna, utan även till verksamhetsutövare, det vill säga så snart legala förutsättningar finns. Utan aktuell information om de kriminella nätverken och deras modus har bankerna betydligt sämre förutsättningar att upptäcka oegentligheter och att implementera en transaktionsövervakning med god precision. I sin tur innebär detta risker för bankkunderna och i förlängningen banken.

Idag föreligger brister i förhållande till en snabb och effektiv delning av information och analyser. Det finns åtskilligt att vinna på förbättringar i detta hänseende i förhållande till verksamhetsutövarna, naturligtvis i den mån som förundersökningens intressen tillåter delning. Det kan handla om att såväl stoppa bedrägliga transaktioner som återföra pengar till brottsoffer.

Det bör därför från regeringens sida tydliggöras att brottsbekämpande myndigheter inte enbart ska samla in, analysera och sammanställa information enligt ovan, utan även ha adekvata rutiner för att sprida informationen till alla relevanta parter, såväl internt som externt. Till exempel underrättelseverksamhet tjänar knappast sitt syfte

[24] Detta även mot bakgrund av att det är svårt att se en framtida utveckling mot ett mer omfattande och effektivt rättligt samarbete i brottmål gentemot vissa regioner och länder som realistisk.

om den inte resulterar i något som är praktiskt användbart i arbetet med att förebygga, upptäcka och rapportera brott.

Resursfördelning
Mot bakgrund av att en del av regeringens nationella strategi mot organiserad brottslighet handlar om att slå sönder den kriminella ekonomin är det rimligt att i större utsträckning prioritera bedrägeribrotten.

Det ankommer på Polismyndigheten att ta emot anmälningar och utreda förmögenhetsbrott riktade mot personer, dit bedrägeri hör. Bedrägeribrott, i vart fall organiserade sådana, är i många fall relativt resurskrävande och ofta komplicerade att utreda, vilket kan ha att göra med att det ofta krävs bland annat olika former av ekonomiska analyser och IT-forensiska undersökningar. Vidare är de nätverk som sysslar med organiserade bedrägeribrott ofta svåröverskådliga såtillvida att många personer är involverade med skilda roller i upplägget, till exempel målvakter, ID-kapade personer och personer med i övrigt svag anknytning till det svenska samhället.

Det torde vara allmänt känt att polisens bedrägeriutredande verksamhet sedan länge är resursmässigt eftersatt med stora ärendebalanser och åklagardirektiv som inte kan utföras inom rimlig tid, vilket i sin tur har bidragit till en låg andel uppklarade bedrägerier. Det är inom ramen för denna utredningsverksamhet som de organiserade telefonbedrägerierna ska behandlas. Det finns dessutom anledning att befara att polisen inom sina bedrägerisektioner inte har tillräckligt enkel och snabb tillgång till de digitala verktyg som behövs för att effektivt utreda brotten.

Inom polisen konkurrerar bedrägeribrotten med övrig polisiär verksamhet avseende resurser för bland annat hemliga tvångsmedel. Av naturliga skäl har fokus hos brottsbekämpande myndigheter legat på att försöka komma till rätta med grova våldsbrott. Det kan därmed vara svårt för polis och åklagare att få snabb tillgång till adekvata tvångsmedel i utredningar om grova bedrägerier, trots att legala förutsättningar finns och att det är angeläget att komma till rätta med de organiserade telefonbedrägerierna.[25]

Det kan i detta sammanhang vara av intresse att konstatera att EBM generellt sett har enklare tillgång till mer omfattande resurser än polisen och Åklagarmyndigheten. Dessa resurser kan innefatta till exempel IT-forensisk analys, kvalificerade ekorevisorer och ekoutredare, spaning, underrättelseverksamhet, hemliga

[25] Regeringen annonserade i april 2024 en ”[k]raftsamling för att stoppa den kriminella ekonomin” och angav därvid att ”[d]en grova organiserade brottsligheten är systemhotande och måste krossas. För att lyckas med det behöver den kriminella ekonomin strypas.”

tvångsmedel samt erfarenhet och rutin avseende internationellt rättsligt samarbete inom ekobrottsområdet.[26]

Brottsbekämpande myndigheter bör ges i uppdrag att samordna och centralisera sin handläggning av organiserade grova bedrägerier till den myndighet eller enhet som har bäst förutsättningar att ta ett helhetsgrepp och genomföra en samlad utredningsverksamhet, inkluderande åtgärder på ett internationellt plan och hemliga tvångsmedel med den senaste tekniken. Resurserna till bedrägeriutredning innefattande hemliga tvångsmedel, i synnerhet HDA, bör därvid utökas till den myndighet som får uppdraget på sitt bord.

Dispositionsförbud

Dispositionsförbudet[27] utgör ett adekvat verktyg för att förhindra att brottsutbyte från till exempel telefonbedrägerier omsätts eller tvättas av de kriminella nätverken, och möjliggör ett snabbt återställande av pengar till brottsoffret.

En förutsättning för att så ska bli fallet är dock en ändamålsenlig och effektiv tillämpning av dispositionsförbudet, i enlighet med lagstiftarens avsikt. Det kräver i sin tur att såväl verksamhetsutövare som brottsbekämpande myndigheter agerar och kommunicerar med den enkelhet och snabbhet som är påkallad.

Det kan konstateras att det idag föreligger systematiska brister i tillämpningen av dispositionsförbudet. Bankerna rapporterar i allmänhet till Finanspolisen så snart förutsättningar finns. Orsaken till bankernas snabba agerande är, förutom lagstadgad rapporteringsskyldighet, vetskapen om att pengarna i regel mycket snabbt överförs och försvinner ur banksystemet, till förmån för de kriminella nätverken och till nackdel för brottsoffret.

Efter bankernas rapportering till Finanspolisen ligger åtgärdsmöjligheten utanför bankens kontroll. I detta skede kan banken inte göra annat än att invänta återkoppling i form av eventuellt beslut om dispositionsförbud för bankens omedelbara verkställighet.

Det kan dock konstateras att beslut om dispositionsförbud i många fall inte alls meddelas, och när så sker är det inte ovanligt att pengarna redan har hunnit föras vidare eller har tagits ut, vilket naturligtvis fått till följd att banken inte kunnat

[26] Omfattande bedrägerier kan i många fall ha anknytning till brott som faller direkt under EBM:s kompetensområde, vilket innebär att den samlade brottsligheten ofta handläggs där.
[27] Dispositionsförbudet regleras i 4 kap. 11 § lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism och utgör en tillfällig tvångsmedelsåtgärd, eller ett förstadium till ett annat tvångsmedel, som i brådskande fall ska förhindra en kontoinnehavare att kunna tillgodogöra sig eller vidarebefordra pengar från brott.

verkställa dispositionsförbudet och i förlängningen inte kunnat återföra pengarna till brottsoffret.[28]

Inom ramen för bankverksamhet går det i praktiken i många fall till så att banken av sin kund uppmärksammas på att denne utsatts för brott genom att en misstänkt transaktion har gjorts från kundens konto till ett annat konto. Ofta kan det vara fråga om ett misstänkt telefonbedrägeri där kunden alltså har lurats att genomföra transaktionen. Banken uppmanar då kunden att göra en polisanmälan och gör dessutom i många fall en egen sådan anmälan.[29] Vidare skickar banken omedelbart en penningtvättsrapport till Finanspolisen. I normalfallet sker detta genom goAML, vilket är Polisens portal för de verksamhetsutövare som ska rapportera bland annat misstänkt penningtvätt.

Om förutsättningar föreligger bör Finanspolisen därefter, efter vissa åtgärder, fatta ett beslut om dispositionsförbud.

Kriminella nätverk agerar ofta snabbt och har i allmänhet kontinuerlig kontroll över de bankkonton som används inom brottsligheten. På så vis minskar nätverken risken för upptäckt och därmed stoppade transaktioner. I sin tur innebär detta att beslut om dispositionsförbud skulle behöva fattas inom en kort tid efter bankens rapportering för att pengarna ska kunna säkras på det sätt som lagstiftaren avsett.

För att bekämpa de organiserade telefonbedrägerierna är det av vikt att dispositionsförbudet används på ett effektivare sätt än vad som hittills varit fallet, så att dess potential utnyttjas bättre.

För att uppnå detta bör det i PTL införas ett skyndsamhetskrav i förhållande till Polismyndighetens eller Säkerhetspolisens beslut om dispositionsförbud, efter rapportering skett från en verksamhetsutövare. En sådan reglering skulle ligga i linje med den befintliga regleringen om skyndsamhet i övrigt inom ifrågavarande handläggning.[30] Det kan alltså förefalla märkligt att en viss del av handläggningen

[28] Av 3 kap. 3 § penningtvättslagen följer en skyldighet för verksamhetsutövare att förhindra transaktioner som misstänks ha samband med specifikt penningtvätt eller finansiering av terrorism. Bestämmelsen ersätter dock inte en myndighets beslut om tvångsmedel, utan syftar till att om möjligt kvarhålla ett misstänkt brottsutbyte under verksamhetsutövarens kontroll under en ospecificerad tid.
[29] Polisen har uttryckt en avsikt att inrätta en särskild digital ”funktionsbrevlåda” för att underlätta för brottsanmälningar.
[30] Jämlikt 4 kap. 11 § lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism (PTL) ska ett beslut om dispositionsförbud ska *så snart som möjligt* anmälas till åklagare, som *skyndsamt* ska pröva om åtgärden ska bestå. Åtgärden upphör att gälla när *två arbetsdagar har gått* från Polismyndighetens eller Säkerhetspolisens beslut, om den inte hävts före det.

inte omfattas av skyndsamhetskrav, vilket måste anses vara en starkt bidragande orsak till dagens relativt ineffektiva tillämpning av dispositionsförbudet.

SVENSKA BANKFÖRENINGEN

Hans Lindberg Erik Wendeby

Det kan vara värt att notera att EU:s sjätte penningtvättsdirektiv innehåller förändrade bestämmelser avseende bland annat ledtiderna för dispositionsförbudet, vilka föreslås införas i en ny penningtvättslag. För det fall föreslagna ändringar genomförs genom den nya penningtvättslagen förefaller detta i praktiken innebära att någon form av skyndsamhetskrav införs i förhållande till Polismyndighetens eller Säkerhetspolisens beslutsfattande, detta i kombination med att verksamhetsutövarna först efter tre arbetsdagar efter rapporteringen får genomföra en transaktion om beslut om dispositionsförbud inte fattats då (jfr. art 20.1 och 52 i direktivet). Ett införande av en reglering med motsvarande innehåll torde innebära ett ökat behov av nya rutiner och resurstilldelning för i synnerhet Finanspolisen. Frågan är emellertid så pass angelägen att den inte kan anstå till ett eventuellt införande av en ny penningtvättslag.