Hotbildsbedömning för Sveriges banker

Publicerad maj 2025

Svenska Bankföreningen
Finance Sweden

Hotbildsbedömning för Sveriges banker

Publicerad maj 2025

Bankernas säkerhetsorganisationer beskriver och bedömer årligen den branschgemensamma hotbilden med utgångspunkt från bankernas verksamhet. Ett hot består av en förmåga, en vilja och ett tillfälle.

Bankernas specialister på fysisk säkerhet, identifiering, cybersäkerhet, informationssäkerhet, bedrägerier, kortsäkerhet, penningtvätt, outsourcing, sanktioner, kontanter och säkerhetsskydd bidrar till rapporten.

Hotbildsbedömningen är uppdelad i ett antal områden som avslutas med en bedömning av risk- och hotnivå. Åtgärder som bankerna inte kan vidta själva listas som behov av åtgärder från politik och myndigheter.

Sammanfattning 4

Kränkning, personhot och våld mot bankpersonal 6

Hotbilden från insiders och möjliggörare 9

Det säkerhetspolitiska läget, kontinuitet och civil beredskap 11

Informationssäkerhets- och cybersäkerhetshot 13

Bedrägerier och finansiell brottslighet 16

Penningtvätt 26

Nyttjande av företag i brottsliga syften 30

Finansiering av terrorism 33

Internationella sanktioner 34

Bank- och värdetransportrån och angrepp mot uttagsautomater 36

Utmaningarna med kontanter 37

Sammanfattning

Det säkerhetspolitiska läget och brottsutvecklingen i Sverige de senaste åren påverkar i dag bankerna och kunderna huvudsakligen inom områdena cybersäkerhet, bedrägerier och penningtvätt. Under hösten 2024 ökade antalet överbelastnings-attacker samtidigt som de blev mer avancerade och svårare att bekämpa. Bankernas åtgärder mot telefonbedrägerier har haft effekt och under 2024 minskade brottsvinsterna för det tillvägagångssättet markant jämfört med 2023. Inom penningtvättsområdet har samverkan stärkts nu 2025 genom inrättandet av ett finansiellt underrättelsecentrum där bankerna deltar. Bankernas samarbete har stärkts inom alla säkerhetsområden, både mellan bankerna och med myndigheterna.

Inom området **kränkning, personhot och våld mot bankpersonal** rapporterar bankerna om ökad spänning och tuffare bemötande från kunder de senaste åren. Många medarbetare vill inte representera banken i rättsliga sammanhang. Exponering av enskilda medarbetare kan öka hotbilden mot individen snarare än mot banken. En trygg arbetsmiljö för bankpersonal är inte bara bankernas ansvar utan en del av ett bredare samhällsåtagande.

En **insider/möjliggörare** kan utnyttja sin insyn i banken för att genomföra olagliga transaktioner eller manipulera finansiella flöden på uppdrag av kriminella eller en främmande stat. Hotaktörer kan på så sätt även påverka beslut, informationsflöden och affärsstrategier i banken. Främmande stater kan använda insidernätverk för att samla underrättelser, destabilisera ekonomin eller påverka politiska beslut.

Inom området **kontinuitet och civil beredskap** visar aktuella hybridhot och incidenter i närområdet att den säkerhetspolitiska utvecklingen kräver ett långsiktigt beredskapsarbete i Sverige, vilket även innefattar finansiella tjänster. Med ett väpnat angrepp mot Sverige som dimensionerande förutsättning för kontinuitetsarbetet i bankerna ställs mer långtgående krav än vid fredstida kriser. Frågor som evakuering av data och funktioner, omfattande reservarrangemang och skydd av kritiska anläggningar såsom kontorsbyggnader och datacenter, krigsorganisation etc. behöver då hanteras.

Informations- och cybersäkerhetsområdet präglas under perioden av mer avancerade överbelastningsattacker med ökad styrka och omfattning. Det primära syftet med angreppen är informationspåverkan mot samhället och medborgarna genom att angriparna försöker visa att samhällsviktiga finansiella tjänster är i fara. Företag inom finansiell sektor fortsätter att drabbas av ransomware (utpressningsprogram som krypterar sina offers data) utan att för den skull sticka ut i jämförelse med andra sektorer. Under perioden har hoten mot kritisk infrastruktur konkretiserats genom misstänkta sabotage mot el- och kommunikationskablar i Östersjön.

Social manipulering har gjort **bedrägeribrottsligheten** mer riktad och mer personlig. Antal bedrägeriförsök har under 2024 ökat men antalet polisanmälda bedrägerier har minskat. Även brottsvinsterna har minskat 2024 jämfört med 2023. Bankernas åtgärdsprogram för att minska telefonbedrägerier har resulterat i ett 40 procent lägre utfall av brottsvinster 2024 jämfört med 2023 och en tydlig nedgång av det genomsnittliga beloppet per telefonbedrägeribrott.

Penningtvättshoten är fortsatt omfattande och härrör från bland annat bedrägerier, narkotikahandel, brott mot välfärden och skattebrott. Andra riskområden för penningtvätt är till exempel företag som hanterar valutaväxling, kontanthantering, kryptovalutor, fastighetsmarknaden, lyxkonsumtion och spelsektorn.

Företag nyttjas frekvent och storskaligt i brottsliga syften, där målvakter figurerar för att dölja de verkliga verksamhetsutövarna. Företag kan användas för olikartad brottslighet parallellt och brottsutbytet blir ofta stort. Det är vanligt att löst sammansatta brottsliga nätverk bedriver ett stort antal företag och genomför brottsliga transaktioner dem emellan.

Finansiering av terrorism inbegriper många olika tillvägagångssätt såsom crowd funding och nyttjande av kryptovalutor. En riskfaktor är att bankerna ofta saknar tillgång till information från Polisen om hur sådan finansiering går till samt vilka som är inblandade.

I och med tilltagande geopolitiska spänningar har **internationella sanktioner** blivit ett allt viktigare utrikes- och säkerhetspolitiskt påtryckningsmedel. Samtidigt har sanktionernas omfattning ökat i snabb takt och därmed blivit allt svårare att såväl överblicka som tillämpa för verksamhetsutövarna. Här krävs utökad information, samverkan och dialog mellan aktörerna på sanktionsområdet. En särskild utmaning är det alltmer avancerade kringgåendet av sanktioner.

Under 2024 inträffade inga **bank- och värdetransportrån** och inte heller några angrepp mot Bankomat AB:s uttagsautomater. Hotbilden mot bank- och värdetransportrån och angrepp mot uttagsautomater består men antalet rån och angrepp förväntas att ligga på en låg nivå 2025.

Det finns politiska incitament att öka kontantanvändningen i Sverige. För bankerna är **utmaningarna med kontanter** att det skapar risker för de som arbetar med kontanter och att spårbarheten för kontanter är låg eller obefintlig. Eftersom kontanter används i så liten omfattning i normalläget är det heller inte en realistisk lösning att kontanter kan ha en stor betydelse vid kris eller krigshändelse.

Kränkning, personhot och våld mot bankpersonal

Flera medarbetare och chefer i bankerna vittnar om högre tonläge och tuffare bemötande från kunder de senaste åren. Bankerna får signaler om att medarbetare känner sig mer otrygga, och undersökningar från bankerna och Finansförbundet visar att medarbetare utsätts för hot och våld.

Bilden varierar dock: vissa banker anser att hot och kränkningar är på ungefär samma nivå som tidigare, medan andra banker noterar en kraftig utveckling det senaste året. Det är svårt att förklara förändringen. Det kan vara ett resultat av ökad anmälningsbenägenhet eller en konstaterad ökning. För banker med stor kontorsrörelse är ungefär hälften av antalet kränkningar och hot kopplade till fysiska kontor medan andra hälften riktas mot telefonbanken.

Allt fler bokade kundmöten

Allt fler banker kräver att kunder avtalar tid för besök på bankkontoret. Beslutet är ofta affärsdrivet i syfte att öka kvalitén på kundmöten, men förändringen minskar samtidigt hotbilden mot anställda. Kränkningar från kunder via sociala medier förekommer, exempelvis från kunder som avvisats från kontoret eller där kundrelationen avvecklats av olika anledningar.

Omställningen mot mer digitala kundmöten påverkar arbetssättet och förändringen medför att nya typer av hotsituationer kan uppstå. Det är visserligen färre hot vid förbokade möten, men hoten skulle inte försvinna även om alla möten var förbokade. Det händer exempelvis att en obehörig tränger sig in i banklokalen vid in- och utsläpp av en kund.

Verktyg för att hantera hotfulla kunder

Bankerna avvecklar fler kunder i dag jämfört med tidigare. Anledningen är bristande kundkännedom, att banken upptäcker fler oegentligheter och att fler kunder uttrycker hot mot bankens personal. Ett högre antal kundavvecklingar påverkar hotbilden. När banken avvecklar en kundrelation eller nekar en person att bli kund i banken, behövs en intern process för att bedöma och förutse en eventuell hotbild mot både bankens kontor och medarbetare. Den hotbild bankerna tidigare uppskattade relaterat till avveckling av kunder har dock inte blivit verklighet i den omfattning som befarades. Bankerna har varit proaktiva i säkerhetsarbetet, men det finns fortfarande behov av att följa utvecklingen.

Medarbetarna kan hamna i tuffa situationer med ekonomiskt pressade kunder. Banken håller därför utbildningar i konflikthantering med alla medarbetare som arbetar på kontor och telefonbank och bankerna arbetar även med stödfunktioner.

Andra verktyg för att hantera kunder som beter sig illa är att banken ringer upp eller skickar varningsbrev till kunden och förklarar att den inte accepterar kränkande beteende mot bankens personal.

Bankerna försöker utveckla metoder för att kunna förstå och rikta insatserna bättre: är det ett olaga hot eller ”bara” ett onödigt ordval från en upprörd kund? De otrygga situationer som uppkommer i fysiska möten med kunden tenderar att följa med till webb- och telefonmöten. Steget från ett normalt tonläge till att bli otrevlig upplevs vara kort. Samtidigt är gränsen för vad en medarbetare kan acceptera olika för olika individer.

Ett hot kan vara faktiskt eller upplevt. Svårigheten att bedöma och kommunicera ut ett faktiskt hot beror på att det är vanskligt att avläsa hoten utifrån faktiska händelser. Det centrala är att situationer som inte kan definieras som ett hot i lagens mening kan upplevas och uppfattas vara en hotfull situation som bidrar till en otrygg arbetsmiljö.

Bankerna har förmåga att bedöma en hotbild men det finns en svårighet att bedöma graden av allvaret i ett hot. Är det reellt eller inte, kommer det att realiseras eller är det snarare en obehaglig incident. Oron upplevs ändå ha ökat.

Olika delar av banken är olika utsatt för hot

Bor man på en mindre ort och möter kunder fysiskt utanför arbetet i vardagen, är situationen annorlunda jämfört med för anställda som bor i större städer, eller för medarbetare i telefonbanken som inte möter kunden fysiskt.

Avgörande är till stor del om en medarbetare har kundkontakt. Har banken en kontorsrörelse söker sig kunder ofta till ett fysiskt bankkontor. Har banken bara ett synligt fysiskt huvudkontor blir det mer utsatt jämfört med en telefonbank som kan finnas på olika platser i landet. Beslutsfattare i penningtvätts- och bedrägeriutredningar, som ofta återfinns på centrala funktioner, påverkas också av hotbilden och dualitet i beslutsfattande har en hotbildsreducerande effekt.

Beroende på hur hotbilden utvecklas kan förändrade fysiska skyddsåtgärder behövas.

Kontroller och åtgärder skapar frustration hos kunderna

Bankerna får många myndighetsförfrågningar om exempelvis transaktioner rörande brottsutredningar. Det finns indikationer på ökad oro hos medarbetare som arbetar med kundkännedom, penningtvättsanmälningar och bedrägerier. Exponering av enskilda medarbetare, i stället för banken, kan medföra en ökad hotbild mot individen.

Ökade insatser mot brottslighet i form av flera kontroller och uppföljning kan skapa frustration hos kunderna. Vissa åtgärder som bankerna vidtar skapar frustration hos kunder, särskilt de banköverskridande åtgärderna som exempelvis blockering av BankID. Uppdatering av kundkännedom och att kunden vill göra en för kunden ovanlig transaktion eller lägga till en produkt/tjänst är återkommande källor till frustration.

Bankernas åtgärder för att skydda sina medarbetare

För att bemöta hotbilden arbetar bankerna med att skydda medarbetares identiteter på olika sätt. E-post skickas i större utsträckning från centrala funktionsbrevlådor, exempelvis kundkontakt@banken.se. Vidare begränsas bedrägeriutredares externa kundkommunikation. Bankerna har även tankar om att införa system för alias som kan användas av medarbetare vid känsliga åtgärder, som exempelvis avveckling av kund.

Även om handläggaren som avsändare är dold så upplever medarbetare en känsla av hot när påtryckningar riktas mot banken. I rättsliga sammanhang händer det att medarbetare inte vill representera banken, av rädsla för hot. Medarbetare kan tycka att det är jobbigt att polisanmäla hot eller brott de varit utsatta för i sitt arbete, eftersom det kan generera nya hot. I en anmälan blir medarbetaren målsägande och när åtal väckts blir det en offentlig handling. Banken kan inte göra en sådan anmälan, utan den utsatte måste själv göra den. Det blir en avvägning mellan risken att offentliggöra en medarbetares namn i en polisanmälan och att polisanmäla kunden. Det banken kan göra är att säkerställa att det finns stöd vid en eventuell rättegång.

Exponering av enskilda medarbetare kan öka hotbilden mot individen snarare än mot banken.

En trygg arbetsmiljö för bankpersonal är inte bara bankernas ansvar utan en del av ett bredare samhällsåtagande.

Bankerna vidtar kontinuerligt skyddsåtgärder för att enskilda anställda inte i onödan ska exponeras offentligt i samband med vissa typer av beslut eller andra åtgärder. Arbetet motverkas dock av att myndigheter ibland lämnar ut bankanställdas personuppgifter, i kombination med att offentliga söktjänster tillgängliggör detaljerade personliga uppgifter. Om utlämnande av personuppgifter innebär en risk för att personen eller anhöriga utsätts för hot bör det vara tillåtet att i stället använda alias. Personens namn bör inte heller lämnas ut av myndigheter.

Att säkerställa en trygg arbetsmiljö för bankpersonal är inte bara ett ansvar för banken utan en del av ett större åtagande för samhällets olika aktörer att motverka bedrägerier och penningtvätt.

Säkerhetspolisens höjning av terrorhotnivån från 3 till 4 i augusti 2023 har medfört att bankerna har gjort en översyn av sitt befintliga säkerhets- och kontinuitetsarbete, även om bankerna i sig troligen inte är en direkt måltavla.

Flera banker har varit föremål för demonstrationer från grupper som vill protestera mot bankernas verksamhet, exempelvis miljöorganisationer. För bankerna är det inget problem, utan ett naturligt inslag i ett öppet samhälle. Däremot förekommer det protester och aktioner där in- och utgångar blockeras vilket riskerar att försvåra en eventuell evakuering och utsätter personal och kunder för fara.

Behov av åtgärder från politik och myndigheter

- Myndigheternas krav på banken har bidragit till att hotbilden mot bankernas medarbetare har ökat. Bankerna tvingas exponera enskilda medarbetare vid en polisanmälan och andra myndighetskontakter vilket ökar risken för hot. Om hotet gäller ett helt bankkontor kan banken göra en polisanmälan. Det borde vara möjligt för banken att göra en polisanmälan så att medarbetare inte behöver exponeras. Bankerna efterfrågar en centraliserad funktion som kan företräda banken vid exempelvis bedrägeriärenden eller för att i domstol förklara hur exempelvis en betaltjänst fungerar. Anmälaren skulle på så sätt bli neutraliserad, eftersom det är organisationens ställningstagande och inte den enskilde medarbetarens. Banken kan då också välja vilka personer som ska företräda banken och medarbetaren behöver inte känna sig utpekad utöver det hot man tidigare har blivit utsatt för.

Bedömningen är att hotbilden mot bankernas personal påverkas av både samhällets utveckling och myndighetskrav.

Hotbilden från insiders och möjliggörare

Så kallade möjliggörare av brott är en faktor som kontinuerligt gör sig påmind och som kräver vaksamhet och adekvata åtgärder. En möjliggörare av brott är i detta sammanhang en insider som genom sin yrkesroll gör något otillbörligt. Det kan vara för egen vinning, för organiserad brottslighet och kriminella nätverk eller en statlig aktör. Organiserad brottslighet och kriminella nätverk är den dimensionerande hotbilden.

Riskbeteenden och sårbarheter

Incitamenten för en extern antagonist att plantera eller rekrytera en insider på en bank bedöms i allmänhet vara starka eftersom det ger större möjlighet till olika former av bedrägerier, penningtvättsupplägg, beslutspåverkan och tillgång till intern information. En insider kan antingen vara en aktiv möjliggörare, aktivt dela information eller ha en mer rådgivande eller coachande roll. Den anställde kan även vara omedveten om att den används som insider.

Insidern själv är ofta en person med olika riskbeteenden och sårbarheter såsom drogmissbruk, spelmissbruk och/eller privatekonomiska problem. Men han eller hon kan även på annat sätt befinna sig i en utsatt situation genom släktskap eller vänskapsrelationer. Den typen av relation kan medföra att befattningsutövandet, som grundar sig i lämplighet, kan antas påverkas negativt. Även kopplingar till högriskländer eller kriminalitet kan förekomma. Ett annat incitament för illojalt beteende från en anställd är underliggande besvikelse på arbetsgivaren på grund av bristande uppskattning, utebliven befordran eller dålig löneutveckling.

Vissa tillvägagångssätt kräver en möjliggörare på insidan

Vissa tillvägagångssätt kan inte genomföras utan en möjliggörare på insidan. En anställd med kunskap om bankens produkter, tjänster och rutiner och processer, regelsättning vid kreditgivning och regler för transaktionsmonitorering är intressant för externa aktörer. Vid sidan av bankens egen kreditberedningsprocess skapar låneförmedlare, med fler parter i lånekedjan, olika typer av incitament till bedrägerier och penningtvättsupplägg för en insider.

Påtryckningar kan ta olika former

Det förekommer att externa antagonister söker kontakt med bankens personal för att bearbeta och utnyttja dem på olika sätt. Sociala medier som LinkedIn och andra öppna informationskällor används för att kartlägga medarbetare i banken och för att söka efter möjliggörare. Antal kontakter med erbjudande om att genomföra betalda intervjuer, via exempelvis Linkedin, bedöms ha ökat de senaste åren.

Kriminella och andra fientliga aktörer annonserar också efter personer som är beredda att vara behjälpliga från insidan. Social manipulering smälter på så sätt ihop med den fysiska hotbilden genom att otillbörliga kontakter senare kan leda till fysiska hot mot anställda. Det kan handla om påtryckningar, hjälp med skulder, möjlighet att få ersättning för att lämna information eller att insidern upplever sig behövd. Det kan också handla om anställdas kontakter på krogen och olika former av missbruk som kan leda till utpressningssituationer.

Hotaktörer och möjliggörare kan påverka beslut, informationsflöden och affärsstrategier i banken.

Det händer också att en person med anknytning till en extern antagonist söker anställning i bank i syfte att möjliggöra brott.

Bankerna efterfrågar tydligare regler

En fråga som aktualiseras är hur banken kan skydda medarbetare mot otillbörliga kontakter från exempelvis en statsaktör eller organiserad brottslighet. Inom säkerhetsskyddslagstiftningen, som ofta träffar en avgränsad del av bankens verksamhet, är det reglerat hur det ska hanteras, men hotet finns i bredden av verksamheten, från bedrägerier till hur man rundar sanktioner. Bakgrundskontroller, som främst används vid anställningstillfället, ger inte samma möjligheter som en säkerhetsprövning gör.

I detta hänseende är det av intresse att bankerna har tillräckliga kontrollmöjligheter i samband med såväl anställningsförfarandet som under anställningstiden. Det finns en stor mellanmänsklig tillit i Sverige. Detta är i grunden positivt, men kan skapa naiva inställningar. Idag behöver bankerna till stor del förlita sig på den information som den arbetssökande själv lämnar. Sverige har också ett stort fokus på diskriminerings-, arbetsmiljö- och dataskyddslagstiftning som kan fungera motstridigt.

Bankerna efterfrågar tydligare lagar och regler för området löpande kontroller, avseende praxis och bevisnivåer. Hur ska avvikelser som hittas under anställningens gång hanteras och hur ska man ställa sig till ärenden där det finns oegentligheter? Bankerna bör också ges möjlighet att dela information för att gemensamt verka för att en insider efter upptäckt inte kan få anställning i en ny bank och där fortsätta sitt möjliggörande. Den ökade rörligheten på arbetsmarknaden aktualiserar frågan om det borde finnas någon form av meddelanderätt mellan banker för att hantera utmaningen med insiders.

Behov av information från brottsbekämpande myndigheter

Bankerna hindras att upptäcka insiders och att vidta adekvata åtgärder eftersom de i många fall inte får tillräcklig information i rätt tid från brottsbekämpande myndigheter, som misstänker att en insider förekommer i en bank. Eftersom insiders ofta använder privata kommunikationsvägar för att olovligen sprida information och kommunicera med kriminella, är det brottsbekämpande myndigheter som har bäst förutsättningar att upptäcka aktiviteterna. Det är av vikt att myndigheter kan dela information till bankerna så att de kan vidta åtgärder.

Även om Säkerhetspolisen i februari 2024 har pekat ut ett underrättelsehot från i synnerhet Ryssland, Kina och Iran är svårigheten med insiders att det kan vara vem som helst. Angreppsätt för att hantera den hotbilden sträcker sig från tekniska kontrollmöjligheter till att åtgärder vidtas för att samtliga medarbetare ska känna sig trygga med att rapportera avvikande beteenden, med vetskapen att de inte upplevs som angivare.

Hotaktörer som nationalstater (Ryssland, Kina, Iran etc) och kriminella grupper har olika syften. Även om Polisen bedömer att hotet mot bankerna främst kommer från kriminella grupper och inte nationalstater, innebär de nyligen identifierade kopplingarna mellan statsaktörer och kriminella nätverk i Sverige en väsentlig påverkan på insider-problematiken.

Bankernas egna kontrollmöjligheter

Att förebygga, förhindra och upptäcka intern brottslighet är en viktig del av bankens säkerhetsarbete. Det handlar exempelvis om att följa digitala flöden i bankens egna system och på så sätt identifiera olämpliga digitala beteenden och beteendemönster. Bankernas interna kontrollmöjligheter är omfattande och består av in- och utpasseringsloggar, uppföljning av slagningar på kunder, behörigheter, dokumentationskrav med mera. Mest framgångsrikt är att korsbefrukta olika kontrollmiljöer. Anomalier i enskilda system och processer behöver inte betyda något men när flera datapunkter kan slås samman kan bilden bli annorlunda.

För att kunna minska verksamhetens eller individers sårbarheter för risken att bli utnyttjad av kriminella aktörer, behöver flera avdelningar vara involverade i internutredningsprocessen. Det gäller även fall som rör misskötsamhet och regelöverträdelser.

Bedömningen är att insiders/möjliggörare är ett hot som finns internt i bankerna och som kommer att bestå under 2025.

Det säkerhetspolitiska läget, kontinuitet och civil beredskap

Sverige befinner sig i ett besvärligt säkerhetspolitiskt läge vilket också påverkar hotbilden mot den finansiella sektorn. Risken för antagonistiska hybridhot med syfte att påverka banker och finansiell infrastruktur bedöms ha ökat.

Under senare delen av 2024 har svenska banker blivit utsatta för avancerade överbelastningsattacker i syfte att påverka internettjänsters tillgänglighet. Överbelastningsattacker är i sig inget nytt för bankerna. De har förekommit från tid till annan under åtminstone de tio senaste åren. De senaste angreppen visar dock på en ökad styrka och omfattning. Motiven till denna typ av angrepp kan vara flera, men oftast handlar det om att destabilisera och skada förtroendet för finansiella tjänster och de finansiella företag som utför dessa. Bankföreningen noterar också hotet i närområdet mot kritisk infrastruktur som bankerna är beroende av.

Sabotage mot kritisk infrastruktur

I de senaste årens hotbildsbedömningar har bankerna noterat hoten mot kritisk infrastruktur på grund av säkerhetsläget i närområdet. Under rapportperioden har hoten ytterligare konkretiserats genom misstänkta sabotage mot el- och kommunikationskablar i Östersjön. Bedömningen är därför att hotet är än mer relevant för svenska banker.

Dessutom har det i media rapporterats om att främmande makt kartlägger kritisk infrastruktur med hjälp av exempelvis drönare. Det förefaller också som att aktören som ligger bakom detta inte är rädd för att bli upptäckt.

De svenska bankerna behöver ha fortsatt fokus på att se över sina beroenden till kritisk infrastruktur. De måste planera för att kunna öka sina resurser och sin kapacitet, exempelvis elektronisk kommunikation och elförsörjning. Detta gäller oavsett om den senaste tidens misstänkta sabotage skulle visa sig vara en antagonistisk handling eller inte. Det är också i linje med det arbete för totalförsvar och beredskap som nu intensifieras både i finansiell sektor och nationellt.

Samtidigt kan hot och sårbarheter i kritisk finansiell infrastruktur vara svåra att överblicka för den enskilda banken då finansiell sektor på global nivå är starkt integrerad och sammankopplad på operativ- och teknisk nivå. Beroendet till utländska leverantörer av IT-tjänster är omfattande i den finansiella sektorn samtidigt som frågor om digital suveränitet nu lyfts högre på agendan. Bankerna behöver kontinuerligt följa och utvärdera riskerna med att förlita sig på utländska leverantörer för verksamhetskritiska tjänster.

Risken för antagonistiska hybridhot med syfte att påverka banker och finansiell infrastruktur bedöms ha ökat.

Bankernas beredskapsarbete och kontinuitet

Beredskapsarbetet kopplat till civilt försvar har nu adderats till bankernas arbete med kontinuitet och säkerhet. Uppbyggnad och expandering av bankernas kompetens och personalresurser på området kommer ske över tid. Genom att implementera och integrera ramverk för riskhantering i sitt beredskapsarbete, strävar bankerna efter att säkerställa kontinuiteten i samhällsviktiga finansiella tjänster. Målet är att vara förberedd på omfattande digitala och fysiska störningar, inklusive potentiellt väpnat angrepp mot Sverige. Med ett väpnat angrepp mot Sverige som dimensionerande förutsättning för kontinuitetsarbetet ställs samtidigt mycket mer långtgående krav än vid fredstida kriser. Frågor som evakuering av data och funktioner, omfattande reservarrangemang och skydd av kritiska anläggningar såsom kontorsbyggnader och datahallar, krigsorganisation etc behöver då hanteras.

Flera beredskapsinitiativ läggs nu ovanpå bankernas säkerhets- och kontinuitetsfunktioner. Många initiativ inom beredskap och operativ motståndskraft initieras dessutom samtidigt och utan framförhållning, från flera olika myndigheter och regeringen. Initiativen är ofta okoordinerade och överlappande. Dessutom saknar bankerna information om vilka förutsättningar de behöver ta hänsyn till i sin planering och tydlig vägledning om hur säkerhets- och beredskapsarbetet ska prioriteras. Sammantaget medför det att uppbyggnaden av förmågor både på kort och lång sikt riskeras. De konkreta resultat som förväntas av arbetet riskerar att inte uppnås i tid.

Behov av åtgärder från politik och myndigheter

- En tydlig gemensam målbild för finansiella sektorns beredskapsarbete behöver tas fram av sektorns myndigheter tillsammans med företagen. Målbilden ska förankras och kunna förstås av samtliga myndigheter och företag inom sektorn.
- Tydliga sektorsövergripande prioriteringar behöver slås fast och kommuniceras av sektorns myndigheter. Fokusområden som initialt bedöms som särskilt viktiga för att öka den samlade förmågan och effekten i sektorn prioriteras. Fram till nu har beredskapsfrågorna i sektorn endast behandlats ur de enskilda verksamhetsutövarnas perspektiv och Bankföreningen ser behov av att lyfta perspektivet till en strategisk nivå där förmågeuppbyggnad och nödvändiga investeringar i beredskapsåtgärder analyseras på sektorsnivå.
- I sin beredskapsplanering är bankerna i behov av långt mer detaljerade hotbildsbeskrivningar, scenarier och antaganden om händelseutvecklingen vid ett väpnat angrepp mot Sverige. Det rör sig exempelvis om beskrivningar gällande tillgång till elförsörjning, tele- och datakommunikation, särskilt viktiga geografiska områden i Sverige som bankerna behöver ta hänsyn till och antaganden om tidsförhållanden i det väpnade angreppet.

Bedömningen är att Sveriges säkerhetspolitiska läge och den förstärkta hotbilden påverkar bankerna. Eftersom den framtida utvecklingen är svårbedömd både på kort och lång sikt behöver bankerna kontinuerligt övervaka och utvärdera hur läget påverkar hotbilden mot den egna verksamheten. Regeringens förväntan är att bankerna bidrar till totalförsvarets förmåga att försvara Sverige och vår befolkning mot ett väpnat angrepp.

De svenska bankerna behöver ha fortsatt fokus på att se över sina beroenden av kritisk infrastruktur.

Informationssäkerhets- och cybersäkerhetshot

Ransomware

Under perioden har ransomware-attacker, det vill säga utpressningsprogram som krypterar sina offers data tills en lösensumma är betald, fortsatt drabba ett stort antal verksamheter. Antalet försök till attacker ligger fortsatt på en hög nivå jämfört med tidigare år, men färre verksamheter drabbas. En trend är också att attackerna fokuserar mer på intrång via exponerad standardprogramvara som används i verksamheten, till exempel programvara för filöverföring eller VPN (virtuellt privat nätverk). Samtidigt minskar attacker med ingång via medarbetares datorer något då bättre skydd nu finns att tillgå.

Företag inom finansiell sektor fortsätter också att drabbas, utan att för den skull sticka ut i jämförelse med andra sektorer. Bland händelserna märks attacken mot den amerikanska hypotekslångivaren LoanDepot som drabbades av en ransomware-attack som påverkade nästan 17 miljoner kunder i januari 2024. Attacken resulterade i att känslig personlig information stals. Attacken medförde också att LoanDepot tvingades ta sina system offline, vilket orsakade störningar under cirka en vecka. Hotaktören BlackCat/Alphv har tagit på sig ansvaret för attacken. I juni 2024 drabbades Evolve Bank & Trust av en ransomware-attack utförd av hotaktören LockBit. Attacken innebar att personuppgifter för cirka 7,6 miljoner individer stals. Incidenten påverkade även flera fintech-företag som samarbetade med banken, vilket ökade attackens omfattning.

Data krypteras alltså inte bara vid attacker utan data stjäls också, och aktörerna hotar med att lägga ut informationen publikt på internet om inte lösensumman betalas. Bedömningen är att informationsstölderna i samband med ransomware-attacker ökar jämfört med föregående år. I vissa fall lyckas inte hotaktören kryptera informationen i samband med attacken, men lyckas med att stjäla information. Hot om informationsstöld har även gjorts utan att aktörer stulit någon information eller att innehållet av stulen information överdrivits för uppmärksamhet.

Hotaktörer attackerar också tredjepartsleverantörer med ransomware-attacker. På så sätt skapas en hävstångseffekt eftersom kunderna till leverantörer också drabbas. Attacker har också drabbat leverantörer till banker under perioden. Det finns dock inget som tyder på att leverantörerna har attackerats på grund av att de har banker som kunder.

Det finns anledning för bankerna att löpande bevaka och utvärdera ransomware-hotet och att förbättra sina skyddsåtgärder. Om en attack skulle ske måste banken ha utvecklat åtgärder för att kunna upptäcka och hantera den, samt återställa verksamheten. Omfattande ransomware-attacker mot finansiell sektor skulle kunna få mycket stor påverkan. Studier och analyser från Internationella valutafonden (IMF), Europeiska systemrisknämnden (ESRB) och Riksbanken visar att en tillräckligt stor cyberattack mot finansiell sektor skulle kunna hota den finansiella stabiliteten.

Infostealers

En infostealer är en typ av skadlig programvara som är utformad för att stjäla känslig information från it-system. Denna information kan inkludera inloggningsuppgifter, finansiell information och annan personligt identifierbar information. Infostealers används ofta av hotaktörer för att utföra ytterligare brottsliga aktiviteter som bedrägerier och utpressning.

Attacker med hjälp av infostealers bedöms ha ökat kraftigt de senaste åren och inom finansiell sektor märks attacken mot den spanska banken Santander 2024. Hotaktören ShinyHunters lyckades få tillgång till känslig information om både anställda och kunder i Spanien, Chile och Uruguay. Attacken påverkade en stor mängd kunder och anställda, men ingen transaktionsdata eller inloggningsuppgifter för internetbanktjänster stals. Även enskilda bankkunder riskerar att drabbas av infostealers. Detta har noterats i ett antal länder. Sverige har drabbats i mindre omfattning men det finns anledning att övervaka hotet som en del av säkerhetsarbetet.

Destruktiv skadlig kod

Ryssland har under anfallskriget mot Ukraina vid upprepade tillfällen använt sig av destruktiv skadlig kod, wiper malware, med syfte att förstöra system och data i samhällsviktig infrastruktur. Ukraina har varit framgångsrikt i att försvara sig mot detta. Bankerna har under de senaste årens hotbildsbedömningar beskrivit hotet mot svenska banker som att det finns en indirekt riskexponering mot bankerna genom det faktum att attacker riskerar att sprida sig till andra aktörer och geografier än den tänkta träffytan. Denna typ av okontrollerad spridning av destruktiv skadlig kod förefaller inte ha inträffat det senaste året.

Trots det bör inte hotet från wiper malware tonas ner. Risken för direkta attacker eller indirekt spridning av wiper malware bedöms som låg samtidigt som konsekvenserna skulle bli omfattande. Vid en situation där nuvarande säkerhetsläge snabbt försämras kan hotet bli ett faktum och det finns all anledning för bankerna att fortsatt bevaka området.

Överbelastningsattacker

Under senare delen av 2024 har svenska banker blivit utsatta för avancerade överbelastningsattacker av en specifik hotaktör i syfte att påverka internettjänsters tillgänglighet. Överbelastningsattacker är i sig inget nytt för bankerna, de har förekommit från tid till annan under åtminstone de tio senaste åren. De senaste angreppen visar dock på en ökad styrka och omfattning, enligt följande exempel.

- Varaktigheten: Tiden som angreppet pågår har ökat tiofaldigt jämfört med tidigare förhållanden.
- Styrkan: Angreppen har varit cirka 15 gånger kraftigare än tidigare.
- Skadan: Den exakta kostnaden är svår att beräkna men prislappen för angreppen beräknas uppgå till tvåsiffriga miljoner. Angreppen drabbar framför allt förtroendet för verksamheten.
- Geografin: Angreppen har skett även från nordiska IP-adresser, vilket försvårar avvärjning. Majoriteten av IP-adresserna härrör dock från länder utanför Norden.
- Hotaktören har inte publikt uttalat något syfte med angreppen.

Hotaktören för de aktuella angreppen har också förmåga att ändra och anpassa attacktekniker snabbt vilket gör angreppen svåra att stoppa.

Det primära syftet med angreppen är att underminera förtroendet för finansiell samhällsviktig verksamhet. Om desinformation om allvarliga it-incidenter inom finansiella företag får spridning och skapar flockbeteenden hos bankkunder, exempelvis massuttag från bankkonton, kan följderna för den finansiella stabiliteten bli allvarliga.

Risker i it-leverantörsledet

Bankerna använder it-leverantörer, molntjänster och allmänt tillgänglig mjukvara i sin verksamhet. En konsekvens med det är att skadlig kod kan spridas genom etablerade leverantörsled. En annan konsekvens är att sårbarheter upptäcks av hotaktörer som omedelbart använder dem för att angripa system innan de hunnit åtgärdas. Den typen av sårbarhet brukar benämnas zero-day. Under året har sådana sårbarheter återigen uppmärksammats globalt. Några av de uppmärksammade fallen har förekommit i it-säkerhetslösningar så som Fortinet och Ivanti.

Sårbarheterna utgör en betydande risk även för bankerna eftersom de möjliggör attacker där försvarsmekanismer saknas. Antalet sårbarheter förefaller dessutom öka samtidigt som de också utnyttjas snabbare än tidigare, vilket ger bankerna mindre tid att reagera. Bankerna behöver även fortsätta att aktivt övervaka och åtgärda andra sårbarheter än zero-day. Sammantaget ökar det trycket mot bankernas it-funktioner vilket i sin tur medför ett behov av att tillföra resurser för att hantera riskerna.

Den kanske största händelsen under perioden på områden var CrowdStrike-incidenten som inträffade i juli 2024. En felaktig uppdatering av CrowdStrikes Falcon Sensor säkerhetsprogramvara orsakade omfattande problem med Microsoft Windows-datorer. Uppdateringen ledde till att cirka 8,5 miljoner system kraschade och inte kunde starta om korrekt. Incidenten påverkade många branscher och tjänster globalt, vilket visar på de koncentrationsrisker som byggs upp när flera kunder nyttjar samma it-lösning. Incidenten hade påverkan på bankerna i Sverige om än marginellt.

Artificiell intelligens och deep fakes

I och med framväxten av AI-tjänster på internet ökar risken för informationsläckage för bankerna, om anställda använder tjänsterna på felaktigt sätt och matar in känslig information i tjänsterna.

Det finns anledning för bankerna att löpande bevaka och utvärdera ransomware-hotet och att förbättra sina skyddsåtgärder.

Förfalskade videor, bilder eller ljud som är så genomarbetade att de framstår som äkta brukar benämnas ”deep fakes”. Utvecklingen av artificiell intelligens både accelererar utvecklingen av deep fakes och gör dem svårare att genomskåda. Användningen av deep fakes för bedrägliga syften är ett växande hot i samhället. Inom bankverksamhet skulle deep fakes exempelvis kunna användas för att imitera personer i ledande position gentemot exempelvis bankpersonal inom betalningsområdet. Målet skulle kunna vara att genomföra bedrägliga betalningar.

Under året finns också exempel på när ledande personer i bankerna har härmats med hjälp av deep fakes för att lura kunder i banken. Phishing-mejl blir också bättre och bättre och mer realistiska språkmässigt, vilket tyder på att det finns en koppling till AI.

Phishing och banktrojaner

Skadlig kod eller länkar till skadlig kod via e-post till medarbetare i bankerna är ett vanligt förekommande hot. Även spear phishing förekommer, det vill säga nätfiske som riktar sig mot utvalda personer hos bankerna. Spear phishing har bland annat riktats mot medarbetare i bankerna som kan tänkas ha högre it-behörigheter. LinkedIn har använts för att kartlägga bankernas it-medarbetare, vilka sedan har fått falska jobberbjudanden med länkar till skadlig kod. Syftet med denna typ av spear phishing är troligen att hotaktörerna ser detta som ett snabbt sätt att få fotfäste i bankernas infrastruktur.

Samtidigt är det fortfarande vanligt förekommande med phishing som inte riktar sig mot utvalda personer utan som är av mer opportunistisk, slumpmässig karaktär. Phishing mot it-leverantörers personal som ett sätt att potentiellt sätt attackera bankerna förekommer också. Som en vidareutveckling av phishing förekommer nu allt oftare quishing, där QR-koder används för att lura människor att besöka skadliga webbplatser eller ladda ner skadlig kod.

Bedömningen är att skadlig kod via phishing fortsätter vara en hög risk för bankerna. En viss ökning av spear phishing kan skönjas under året. Övningar och utbildning för att personalen ska kunna upptäcka phishing-mejl samt bankens tekniska lösningar för att blockera phishing-mejl är fortsatt viktiga motåtgärder.

Förekomsten av banktrojaner fortsätter och drabbar kunder till banker och finansiella företag runt om i Europa, även i Sverige om än i mindre omfattning. Attacker med banktrojaner förefaller gå i vågor i olika länder och återkommer då också till Sverige när hotaktörerna vill testa nya angrepp mot svenska bankkunder. Banktrojaner som infekterar mobiltelefoner och mobilbankslösningar syftar ofta till att stjäla kundernas inloggningsuppgifter. Banktrojaner utvecklade för Android-telefoner är fortfarande betydligt vanligare än för iOS-telefoner. Bankkunderna har fått sina mobiltelefoner infekterade genom att ladda ner appar som innehållit skadlig kod.

Behov av åtgärder från politik och myndigheter

- Inför snarast förslagen i utredningen ”En ny funktion för krishantering vid allvarliga driftstörningar i den finansiella sektorns digitala infrastruktur” där Riksbanken ges uppdrag att etablera funktionen.
- Tillse att Riksbanken får i uppdrag att definiera tydliga roller och ansvar för funktionen för krishantering samt hur funktionen ska samspela med Nationellt cybersäkerhetscenter, CERT-SE och Försvarets Radioanstalt, FRA, för krishanterande och stödjande åtgärder vid cyberangrepp mot samhällsviktig finansiell verksamhet.
- Tillse att Riksbanken, med stöd av NCSC, CERT-SE och FRA, får i uppdrag att etablera konkreta stödjande åtgärder till verksamhetsutövare av samhällsviktig finansiell verksamhet vid omfattande cyberangrepp.
- Inför det nya brottet datastörning i brottsbalken. Överbelastningsattacker omfattas idag av brottet dataintrång, trots att något intrång i ett visst datasystem inte skett. Vad det i själva verket är fråga om är en tillfällig störning av tillgången till datasystemet, men inte dess innehåll.

Bedömningen är att hotbilden inom informations- och cybersäkerhetsområdet är fortsatt hög och att den påverkas av kriminella grupper och statsstödda hotaktörer. Under perioden märks en ökning av antalet överbelastningsattacker samtidigt som de har blivit mer avancerade och svårare att bekämpa. Inom cyberområdet kan hotbilden också påverkas av en fientlig aktör med uthållig förmåga och vilja, som ser ett tillfälle kopplat till den säkerhetspolitiska utvecklingen.

Bedrägerier och finansiell brottslighet

Minskat antal bank- och värdetransportrån, digitalisering samt samhällets ökade krav på e-handeln att använda bankens säkerhetslösningar har förändrat den finansiella brottsligheten.

2024 anmäldes 227 434 bedrägeribrott i Sverige, enligt Polisen. Det är en minskning med 8 231 brott, eller 3 procent, jämfört med 2023.

Antal bedrägeriförsök ökar men brottsvinsterna minskar

Antalet polisanmälda telefonbedrägerier ökade under 2024 men brottsvinsterna från dem minskade med 40 procent i jämförelse med 2023. Enligt Polisen är förklaringen till minskningen i huvudsak bankernas åtgärdsprogram mot bedrägerier som lanserades i maj 2024.

Brottsvinster för bedrägerier uppskattas enligt Polisen vara cirka 4,2 miljarder kronor år 2020, 4,6 miljarder kronor år 2021, 5,8 miljarder kronor år 2022, 7,5 miljarder kronor år 2023 och 6,3 miljarder kronor år 2024.

Ökningen av brottsvinster för bedrägerier de senaste åren, fram till trendbrottet 2024, kan till stor del förklaras av att bedrägerier med inslag av social manipulering har ökat markant. Som exempel var 2019 antal polisanmälda vishingbedrägerier 5 285 och 2024 hade antalet ökat till 31 155.

Även om bankernas åtgärder begränsar möjligheterna och har haft effekt på att begränsa brottsvinsterna så har bedrägeribrottsligheten utvecklats till att bli väldigt flexibel och anpassningsbar. Organiserad brottslighet med stort våldskapital påverkar idag bankerna på områdena fysisk säkerhet, cyber, bedrägeri och penningtvätt där de olika delarna går i varandra.

Nya produkter och tredjepartsleverantörer

En av utmaningarna i arbetet med att motverka bedrägerier är att tjänsteutveckling och digitalisering går väldigt fort, vilket innebär att hotbilden förändras snabbt. Snabbheten kräver i sin tur ett realtidsskydd avseende informationsdelning och det uppstår ett behov av att dela tekniska uppgifter. Bankerna tar ned falska hemsidor på löpande band, vilket kräver kompetens och resurser. Banken behöver förstå vilka hot och sårbarheter för både bedrägeri och penningtvätt, som nya produkter medför, samt ta fram motverkande åtgärder.

Nya tjänster och produkter utvecklas inte alltid av banken själv utan kan ske i samarbeten med andra aktörer eller av tredje parter. En ständig avvägning måste ske mellan smidighet och kundvänlighet å ena sidan, och tröghet och ökad säkerhet å andra sidan. Utvecklingen är starkt affärsdriven och kunderna förväntar sig att banken erbjuder nya produkter och tjänster i takt med den tekniska utvecklingen. Alla aktörer i betalningskedjan har inte den kontroll mot slutkund som myndigheterna ställer krav på banken att ha. Det kan handla om riskbedömning av kunder, åtgärder för kundkännedom och bedrägerimonitorering samt en process som säkerställer att momenten hänger ihop med varandra.

Med PSD2 och tjänsteleveranser som bygger på tredjeparters access till konton och data, även kallat open banking, har flera aktörer tillkommit i betalningskedjan, vilket medför nya risker och utmaningar. För bankerna kan monitorering bli allt svårare i takt med att det blir fler aktörer. För konsumenter kan det vara svårt att förstå vad man ger sitt samtycke till och vilken aktör som får tillgång till kunduppgifter.

För att åtgärda bristen finns det ett förslag i kommande EU-förordning om betaltjänster att införa en förteckning över enskilda konsumenters medgivanden till tredjepartsleverantörer.

Fler aktörer får tillgång till bankernas information

Just nu finns ett lagförslag från EU att gå från open banking till open finance genom regelverk för Financial Data Access (FiDA). Det politiska målet är att förbättra och skräddarsy finansiella produkter och tjänster för kunder, samt skapa ökad konkurrens inom finanssektorn. Förslaget kan öppna bankernas infrastruktur för fler aktörer inom olika finansiella tjänster utöver betalningar och kontoinformation. Open finance låter fler finansiella aktörer få tillgång till och möjligheten att dela en stor mängd finansiell data. Det innebär att fler av bankens kunduppgifter ska få användas av tredje part, alltså inte bara för betalningar utan även för bolån, lån, sparande, pensioner och försäkringar.

Risker som lyfts är bland annat cybersäkerhetsrisker, bedrägerier och finansiell brottslighet. Viktiga frågor är därför kundernas kunskap och medvetenhet om hur produkter och tjänster fungerar, men också hur data lagras, används och distribueras. Lika viktigt är att det ställs samma krav som på bankerna på samtliga aktörer inom open finance.

Nya regler för betalningar

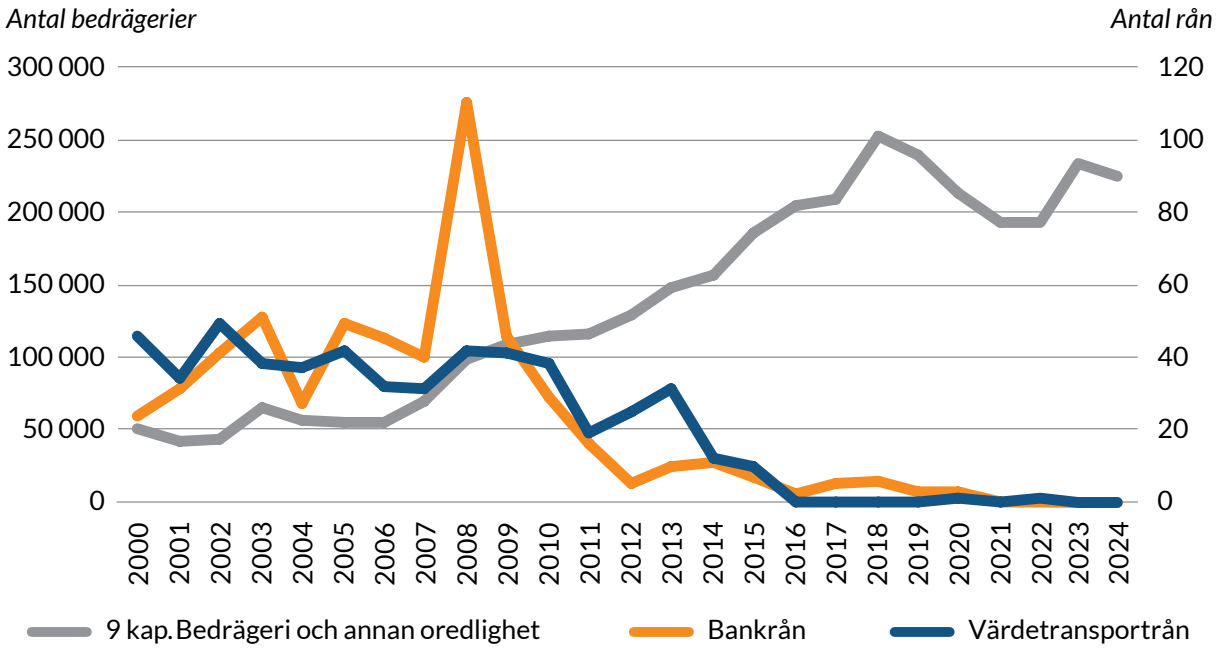
Ett annat lagförslag är EU-kommissionens förslag om ändringar i regelverket för betaltjänster. Det kommer att utmynna i en betaltjänstförordning, Payment Service Regulation, som blir direkt tillämplig i Sverige. Lagförslaget är under förhandling och innehåller såväl förslag för att motverka bedrägerier, som förslag om ökat konsumentskydd där banken föreslås få ett ökat ansvar för återbetalning till kunderna i vissa bedrägerisituationer.

En förskjutning av ansvarsfördelningen till banken, och medföljande krav att ersätta kunder vid bedrägerier, kan leda till en ökning av friendly fraud. Friendly fraud är när kunden som påstår sig vara utsatt för bedrägeri, i själva verket är i maskopi med bedragaren.

Med garanterad ersättning till kunden vid bedrägeri uppstår ytterligare ett problem - kunden kan komma att ta mindre hänsyn till säkerheten. Det tar även bort incitamentet för andra intressenter (telekom och sociala medier/onlineplattformar) att samarbeta med banker, eftersom den fullständiga ekonomiska bördan av bedrägeri alltid kommer att bäras av bankerna. För att effektivt ta itu med problemet bör fokus i stället ligga på förebyggande åtgärder i hela ekosystemet, även aktörer utanför bankerna.

Förskjutningen av ansvarsfördelningen kan också leda till mer tröghet i bankernas tjänster. Oavsett betalinstrument, limit och så vidare kommer bankerna att strypa och anpassa tjänsterna. Bankerna kommer i sådana fall förmodligen att arbeta med mer individualiserad uppdatering av kundkännedom och löpande ha kontakt med sina kunder och begära in underlag. Det kommer också i sådana fall få en större betydelse att bedöma vad kunden vill göra och faktiskt gör, exempelvis kan kunderna i större utsträckning behöva berätta för banken vad de vill göra innan de gör det.

Antal bedrägerier och antal bank- och värdetransportrån (2000–2024).



Källa: Bankföreningen och BRÅ.

En kund kanske endast får överföra till vissa föranmälda konton med en låg beloppsbegränsning. Det är troligt att det kommer att krävas ännu bättre tekniska förutsättningar och fler utredningar av kunder, flöden och att förstå kundernas anknytning till varandra. Bankerna kommer i sådana fall i ökad utsträckning också behöva titta på en bedrägerianmälan från två perspektiv: det första perspektivet är kunden som offer för bedrägeri, det andra är kunden som möjliggörare av bedrägeri.

Inom ramen för den nya betaltjänstförordningen, som för närvarande förhandlas inom EU, diskuteras ett omfattande paket av åtgärder för att motverka bedrägerier. Åtgärderna inkluderar bland annat förbättrad informationsdelning mellan olika aktörer, möjligheten för banker att stoppa transaktioner som misstänks vara bedrägliga, införandet av utgiftstak samt en så kallad ångerperiod för kunder i de fall där utgiftstaket har höjts. Det är mycket positivt att det finns politiska ambitioner att bekämpa bedrägerier, och det är samtidigt av stor vikt att dessa åtgärder i betaltjänstförordningen utformas på ett sätt som både stärker konsumentskyddet och ger bankerna de rätta verktygen för att effektivt motverka bedrägerier.

Nya regler för realtidsbetalningar

Ytterligare förslag från EU är att betalningar ska gå snabbare. Under 2024 trädde nya regler i kraft för betalningar i euro. De innebär krav på betaltjänstleverantörer att erbjuda sina kunder realtidsbetalningar i samma kanaler där de erbjuds vanliga kontoöverföringar i euro. Med kanaler avses framför allt internetbank, mobilbank och telefonbank. Realtidsbetalningar har ett antal utmaningar vad gäller bedrägerier och ekonomisk brottslighet.

Utmaningarna kommer att växa om omedelbara betalningar blir ett tillgängligt alternativ vid fler typer av betalningar. För att balansera utmaningarna och begränsa risken för en ökning av antalet bedrägerier behöver bankerna justera befintliga system och hitta nya arbetsmetoder för att upptäcka och stoppa bedrägerier, samtidigt som kundernas medvetandegrad om riskerna med realtidsbetalningar måste höjas.

Hotbilden förändras

Historiskt sett har bankerna haft förmåga att parera bedrägeribrott, men digitaliseringen i samhället och PSD2 har förändrat förutsättningarna. Kortbetalningarnas affärsmodell, infrastruktur och riskfördelning har tidigare fungerat som ett slags skydd för konsumenter. Men när kraven ökar på att e-handeln ska använda bankens säkerhetslösningar i större utsträckning, ökar samtidigt kraven på kunderna, både att kunna använda de digitala verktygen och att klara av att stå emot social manipulering.

Som en konsekvens av de ökade autentiseringskraven för e-handeln, har brottsligheten drivits mot tillvägagångssätt med större inslag av social manipulering, som exempelvis telefonbedrägerier. Antingen luras kunden att lämna ifrån sig information eller så vilseleds hon eller han till att på bedragarens uppmaning genomföra en transaktion själv, en så kallad behörig transaktion enligt PSD2. Hotbilden har därmed förändrats och då behöver de förebyggande åtgärderna anpassas.

Brottsligheten inom bedrägerier har utvecklats till att bli väldigt flexibel och anpassningsbar.

De största bedrägerihoten

De största bedrägerihoten 2024 har varit vishing-, smishing-, investerings-, romans- och kreditbedrägerier samt BEC-bedrägeri (Business E-mail Compromise). Tillvägagångssätten förklaras nedan.

Vishingbedrägeri (telefonbedrägeri): Bedragaren ringer upp en konsument som under telefonsamtalet blir lurad att antingen lämna ifrån sig koder från sin säkerhetsdosa eller att identifiera sig eller signera uppdrag med sin e-legitimation. Kunderna luras ofta att utföra transaktionerna själva, exempelvis under förevändning att pengar behöver föras över till ett ”säkert konto”.

Smishingbedrägeri (falska sms): Bedragaren skickar ett sms till en kund med information som ska få honom eller henne att göra något. Bedragarens avsikt är att skapa en stressad situation där kunden måste agera snabbt: ringa ett telefonnummer, installera en programvara eller följa en länk och lämna ut information. Vanliga upplägg är sms till kunden med information om ”misstänkt aktivitet på kort eller konto”, eller sms från ”mamma som har bytt telefon och behöver hjälp”.

Romansbedrägeri: Konsumenten blir kontaktad och uppvaktad av en bedragare. För bedragaren handlar det om att nå människor i situationer där de är sårbara, och kärlek är en stark drivkraft.

Investeringsbedrägeri: Bedragaren kontaktar en konsument och erbjuder en påhittad investeringsmöjlighet, alltid med inslag av hög avkastning till låg risk. Ofta pågår kontakterna under lång tid och det är vanligt att konsumenter luras flera gånger.

Kreditbedrägeri: Bedragaren ansöker om ett lån på falska grunder. Utgångspunkten kan vara falska underlag, felaktiga uppgifter eller att kunden inte har någon intention att betala tillbaka lånet. Identiteten kan vara från en utvandrad person, överlåten till någon annan eller fabricerad.

BEC-bedrägeri: Business E-mail Compromise, till exempel vd-bedrägerier, innebär att någon inom ett företag luras att genomföra transaktioner till bedragare.

Men konsumenter och företag är också utsatta för bedrägeriförsök på många andra sätt och det finns flera ingångskanaler. Allt ifrån phishing av inloggningsuppgifter (till exempel e-legitimation och säkerhetsdosa), spridning av skadlig kod, id-kapningar annonsbedrägerier, abonnemangsfällor, påhittade erbjudanden på Facebook och Instagram, ej erhållna varor och falska hemsidor.

Social manipulering fortsätter

Alla banker informerar sina kunder om hur bankens tjänster och produkter fungerar, men enbart information kommer inte att vända brottsutvecklingen med social manipulering. Det finns ingen enskild förändring som kan lösa utmaningarna med social manipulering, utan det handlar, utöver bankernas egna åtgärder, snarare om ett antal förebyggande och samverkande åtgärder.

Den gemensamma nämnaren för bedrägeriupplägen är viljan att påverka och förmå bankkunden att göra något: klicka på en länk, genomföra en betalning eller ringa ett nummer. Brottsligheten har blivit mer riktad och mer personlig och tillvägagångssätten anpassas allt mer efter förutsättningarna. I grunden är det samma modus som utvecklas för att bli mer träffsäkra, exempelvis infogar bedragare oftare det riktiga namnet på förälderns barn i modus ”sms-barn”. Det är idag lönsamt för organiserad brottslighet att investera i den här typen av bedrägliga brottskoncept eftersom andelen uppklarade bedrägerier är låg trots att spårbarheten är hög.

Bedrägerierna drabbar alla målgrupper. Aktuella omvärldshändelser används ofta som bete. En annan trend är ökningen av antalet kunder som blir utsatta för bedrägerier flera gånger. Det vanligast förekommande återvinningsbedrägeriet är att brottsoffer vilseleds att de kan få tillbaka pengar från ett tidigare investeringsbedrägeri.

En växande utmaning är att utsatta kunder förmås att skicka pengarna via andra kunder och/eller institutioner i ett eller flera led innan de når den avsedda slutmottagaren. Det leder till svårigheter gällande ansvarsfördelning, utredning och rapportering.

Hybridmodus dominerar

Hybridformen mellan vishing och smishing dominerar idag, det vill säga ett sms från en fejkad aktör som innehåller ett telefonnummer till en falsk kundservice. Kunden ringer då själv upp bedragaren och luras i det samtalet eller så ”kopplas” kunden vidare till ”sin bank”.

Trenden med bedrägerier där kunden själv godkänt transaktionerna på internet- eller mobilbank medför ett mer komplext problem för banken att både övervaka och förstå. Bankerna behöver få ut riktig information om vad banken och andra aktörer gör och inte gör. Andra aktörer kan exempelvis inte koppla till bankens säkerhetsavdelning och att allt det som bedragaren vill ”hjälpa till med” kan bankerna göra själva om det behövs, bankerna har ju redan all information om kunden.

Både konsumenter och företag utsätts i allt högre utsträckning för bedrägerier vars syfte är att snabbt komma åt och tömma kundens bankkonton. För att kunna genomföra den typen av bedrägerier manipuleras kunden på olika sätt att använda sin e-legitimation eller säkerhetsdosa.

Bankernas åtgärder mot telefonbedrägerier har 2024 minskat brottsvinsterna med 40 procent jämfört med 2023.

Företagare utsätts

När det blir allt svårare för bedragare att få ut stora summor från privatpersoners bankkonton kraftsamlar mer sofistikerade bedragare mot företag. Företagare och användare med tillgång till flera engagemang, som revisorer, har blivit mer utsatta de senaste åren. Exempelvis används ny teknik i syfte att invagga offret i falsk trygghet vilket gör bedragarnas tillvägagångssätt svårare att genomskåda. Brottsbytet kan då bli flera hundra tusen kronor eller mer. Bedrägerierna kan i värsta fall rycka undan mattan för företagens verksamhet och medföra konkurs, eftersom företagare inte har samma grundskydd mot ekonomisk förlust till följd av brott som konsumenter.

Dualitet, det vill säga att två personer måste godkänna en transaktion, skapar en inbyggd tröghet men också en trygghet. Men även om man har dualitet för signering eller dualitetsgräns på ett visst belopp har inte alla företag, föreningar och stiftelser i sin tur interna rutiner som efterföljs. Säkerhetsmedvetandet hos kunderna behöver stärkas. För att få höjda beloppsnivåer kan banken utbilda och skapa medvetenhet så att kunderna förstår. Exempelvis kan bankens kundkännedomsgenomgång behöva visa att kunderna har dualitetsprocessen på plats och att de jobbar efter den, för att banken ska kunna godkänna andra beloppsnivåer.

Fjärrstyrningsprogram

Kunder luras också att installera fjärrstyrningsprogramvara på sin telefon eller dator, vilket ger bedragaren full kontroll över skärm och tangentbord. Kunder är sällan insatta i hur det tekniska fungerar och hur produkter fungerar. Bedragaren kan därmed lägga upp transaktioner i kundens bank som kunden sedan luras att signera.

Utmaningen med fjärrstyrningsprogramvara är att det är en legitim programvara. För att motverka fjärrstyrning försöker bankerna upptäcka och analysera beteendemönster för hur kunder använder datorer och appar.

Det skulle vara verkningsfullt om bankerna hade kunnat upptäcka när fjärrstyrningsprogramvara används på en dator, en tjänst eller en session. Banken skulle då exempelvis kunna neka alla betalningar eller välja att stänga ned tjänsten eller sessionen. Hade bankerna sådana verktyg skulle det avsevärt försvåra för bedragarna, och många bedrägerier hade då stoppats.

Artificiell intelligens

Bedragarna använder sig redan av ett automatiserat och robotiserat arbetssätt, och bankerna behöver följa utvecklingen av bedragarnas användande av AI. Bankerna har också möjlighet att använda den typen av teknologi i sitt brottsförebyggande arbete. Automatiserade konversationer förekommer i vissa bedrägeriupplägg via sociala medier och chat-appar. Bankerna förväntar sig ökad kvalitet på språk och design, och ökad skalbarhet i kommande upplägg av phishing, smishing och vishing.

Risken är att modus mot företagare, exempelvis BEC-bedrägerier som vd-bedrägerier, kommer att förstärkas med AI-inslag, genom röstkloning, inspelade meddelanden eller annat. Bankernas

bedömning är att det kan bli allt svårare för banken att bedöma om en kund, som är drabbad av bedrägeri, kommunicerat med en riktig person eller inte. Den tekniska utvecklingen kommer att medföra ännu större utmaningar både för bankerna och för kunderna att kunna skilja på vad som är bedrägligt och vad som är genuint.

Monitorering av kunderna kräver data

Att kunder idag utför många bankärenden själva medför att det blir allt viktigare för banken att kunna tolka kundernas beteende och upptäcka avvikelser. Bankerna arbetar systematiskt med preventiva metoder, som limiter och begränsningar i produkter. Monitorering av kundernas transaktioner är därför ett viktigt verktyg för banken. Ju fler datapunkter bankerna har tillgång till, desto mer träffsäkra blir deras bedömningar.

Om lagstiftningen skulle tillåta mer datadelning, av exempelvis målvaktsregister och IP-adresser, skulle det bidra till bättre riskbedömningar och monitorering. När banker inte längre kontrollerar det tekniska gränssnittet i exempelvis appar eller betalplattformar får de mindre data att analysera, vilket gör det svårare att övervaka transaktioner och spåra flöden. Bankens bedrägeri- och penningtvättsövervakning försvåras också om transaktioner går till uppsamlingskonton, i stället för direkt till de verkliga mottagarna. Framväxten av realtidsbetalningar ökar ytterligare behovet av precisa riskmodeller och dynamiska begränsningar för att snabbt kunna agera.

För- och nackdelar med ökad datadelning

Den ökade datadelningen inom finanssektorn är både en förutsättning för bättre riskhantering och en källa till nya hot. Regelverk som Financial Data Access (FiDA) syftar till att skapa ett mer sammankopplat finansiellt ekosystem där banker och andra aktörer får tillgång till mer information än tidigare.

Det kan möjliggöra effektivare kreditbedömningar, mer skräddarsydda finansiella tjänster och ökad konkurrens. Samtidigt innebär det att attackytan för cyberkriminella växer, eftersom ett mer öppet dataflöde ger fler parter tillgång till känslig information.

Om säkerheten brister hos en aktör kan det få konsekvenser för hela det finansiella ekosystemet. Cyberkriminella kan utnyttja sårbarheterna för att stjäla eller manipulera data. Manipulation av data, i form av små, osynliga förändringar kan påverka kreditvärderingar och riskanalyser och leda till felaktiga beslut med stora ekonomiska konsekvenser.

Regelverket måste balansera behovet av ökad transparens, med kraven på ansvarsfull datahantering. Med fler aktörer som delar känslig information blir ansvarsfrågor mer komplexa, och tydliga regler krävs för att säkerställa att all data skyddas. Kunderna måste också förstå vem som hanterar deras data och vilka risker som finns.

Bedragare kartlägger sina offer

En trend som har förstärkts de senaste åren är att bedragare blir allt skickligare på att kartlägga sina tilltänkta offer i olika målgrupper. I öppna söktjänster på internet kan bedragarna se en persons personnummer, adress, inkomst och annat. Med hjälp av informationen bygger bedragaren upp en trovärdig historia i syfte att manipulera det tilltänkta offret. Bedragare döljer sig ofta bakom maskerade telefonnummer där bedragaren själv väljer vilket telefonnummer som ska uppvisas i displayen. Det kan då framstå som att det är banken som ringer.

Bedragare kommer också åt uppgifter genom dataintrång. De får då tillgång till mer informationsrik och sanningsenlig information och kan utifrån det rikta sina attacker bättre. Utöver att använda öppna källor för att utsätta en viss grupp för vishing och smishing finns exempel på personer som utför arbete åt teleoperatörers kundstock och som sedan använder de uppgifterna i bedrägligt syfte eller säljer dem vidare. Andra exempel är när ”vårdcentralen” ringer kunden när kunden har varit där som patient tidigare samma dag.

Hembesöken fortsätter

Antal hembesök av bedragare som exempelvis påstår sig vara banktjänstemän, poliser eller hemtjänstpersonal är fortsatt ett problem. Det kan även vara fysiskt uppsökande som falsk färdtjänst. Transparensen i det svenska samhället där personuppgifter är öppna förenklar målsökningen för bedragare.

Bedragarens förevändning är ofta att ”hjälpa till” med något påstått problem, medan syftet med hembesöket är att stjäla värdesaker eller komma åt kundens bankkort och e-legitimation. En indikation på utveckling är att hembesökarna verkar fysiskt tränga sig på i större omfattning idag jämfört med tidigare.

Risken för att antalet hembesök ökar, och därmed att personriskerna ökar när banken täpper till möjligheten till andra tillvägagångssätt, är en realitet som behöver beaktas i arbetet med att motverka bedrägerier. I slutet på 2024 och i början av 2025 ökar antalet hembesök markant.

Kreditbedrägerier

Kreditbedrägerier är sedan lång tid en vanlig företeelse. Att förstå de olika uppläggen av kreditbedrägerier – i alla delar av kreditens förlopp, från ansökan till återbetalning – är utmanande. Antal falska underlag fortsätter att ligga på en hög nivå. Kreditbedrägerier kan utföras på flera olika sätt för varje del och flera delar av kedjan kan vara involverade. Att få en överblick över omfånget av bedrägeriet kan

vara krävande. Om bankerna får felaktiga uppgifter från myndigheter som bankerna i sin tur baserar sina kreditbeslut på påverkas det förebyggande arbetet.

När det gäller företagskrediter handlar det ofta om att ta många parallella olikartade krediter under den tid ett företag kan användas som brottsverktyg. Det kan vara företagslån, snabba företagskrediter, att genomföra stora kreditinköp av dyra varor såsom maskiner, redskap eller fordon. Det är i allmänhet en målvakt som står som företrädare för det bolag som tar krediten.

Eftersom kreditgivare alltid behöver göra någon form av kontroll av personens eller företagets existens, kreditvärdighet och betalningsförmåga gäller det alltså att manipulera systemet så att kreditvärdigheten förefaller bättre än den i själva verket är.

Ett vanligt förekommande upplägg innebär att någon under en kort tidsperiod tar så många och stora krediter som möjligt från olika kreditgivare, utan avsikt att återbetala, ofta med avsikt att hålla sig undan eller lämna landet. Fram till den tidpunkt då uppgifter börjar synas i kreditupplysningarna drar bedragaren nytta av att de olika kreditgivarna inte kan utbyta information. Syftet är att maximera brottvinsten på så kort tid som möjligt.

Ett annat vanligt förekommande upplägg är att någon tar varaktiga krediter, exempelvis bostadslån på falska grunder. Den som saknar kreditvärdighet skapar en falsk bild av sin ekonomiska ställning. Så länge personen följer de avtalade lånevillkoren är möjligheten till upptäckt av bedrägeriet ofta låg. Intresset för kreditbedrägerier ökar när ränteläget är lågt.

Betalning, avbetalning och lösen av krediter är ytterligare ett riskområde, eftersom det kan vara upplägg för penningtvätt. All betalning av krediter bör kontrolleras mot uppgifterna avseende kundkännedom. Om medlens ursprung är tvivelaktigt, hamnar banken i en svår situation för hur kundförhållandet ska hanteras. Dessutom riskerar ärendena att snabbt bli komplexa.

Resurskrävande att hindra kreditbedrägerier

Att motverka kreditbedrägerier kräver mycket resurser och ett omfattande analysarbete. Dessutom krävs hantering av kunder, utbildning av personal, förändrade processer och monitorering. Exempel på kreditbedrägerier inom konsumtionskrediter är så kallade straight rollers/bust out det vill säga personer som tar flera krediter på kort tid utan avsikt att betala. Analyser av straight rollers har resulterat i förändrade onboarding-processer för att tidigt kunna upptäcka varningssignaler. Mäklare agerar allt oftare möjliggörare framför allt i bostadsaffärer på privatsidan men även inom företagssidan.

Om information om återkallade uppehållstillstånd kunde uppdateras och löpande delas med bankerna, skulle de kunna stoppa fler kreditansökningar till personer som försvinner ur landet.

Skatteverkets förändrade sekretessregler 2024 kring inkomst av tjänst och inkomst av näringsverksamhet har gjort det svårare att få reda på var inkomsten kommer ifrån. Tidigare var det specificerat men idag går det inte att särskilja om det är inkomst av tjänst eller inkomst från enskild firma.

Eftersom kreditbedrägerier baseras på en eller flera falska uppgifter har några banker börjat använda externa tjänster för att kontrollera kunders inkomstuppgifter. Men även falska uppgifter om inkomst registreras hos svenska myndigheter, vilket försvårar möjligheten för bankerna att förlita sig på uppgifterna rörande identiteter och familjeförhållanden. Eftersom det är enkelt att ändra inrapporterade uppgifter till myndigheter blir kontrollmekanismerna delvis satta ur spel. Givet utvecklingen bör samtliga aktörer och intressenter öka utbildningsinsatser och därmed höja kunskapsnivån avseende kreditbedrägerier.

Investeringsbedrägerier

Investeringsbedrägerier är ett växande problem. Mörkertalet avseende antal utsatta och brottsvinster är förmodligen stort. Bedragare utnyttjar människors önskan om hög avkastning mot låg risk på sina investerade pengar.

Bedragarna (huvudmännen) befinner sig ofta utomlands, och initial kontakt sker idag främst via annonser i sociala medier, e-post eller genom rekommendation från vänner och ytligt bekanta. Bedrägeriuppläggen förekommer i stor utsträckning via digitala plattformar där kända personers namn och bilder i annonser används för att skapa ett falskt förtroende.

Bedragarna utnyttjar kundernas bristande kunskap om komplexa investeringsformer som kryptovalutor. För att öka trovärdigheten skapar bedragarna falska webbsidor där offren kan logga in och se ”sina investerade pengar” växa. Uppgifterna som visas på skärmen är helt fiktiva. De brottsutsattas pengar har aldrig investerats i några tillgångar utan hamnat direkt i bedragarnas fickor.

Bedragarna har ofta haft kontakt med offret under lång tid. Det kan ta tid innan beteendemönster och transaktioner börjar avvika markant från kundens normala beteende, så att banken börjar ställa frågor. Det är dessutom inte ovanligt att bedragaren förser kunden med ett manus med svar på kommande frågor från banken. Det gör det utmanande för bankerna att upptäcka och stoppa ett pågående bedrägeri. Banken får ju svar på sina kontrollfrågor, likväl som underlag.

En trend som har förstärkts är att bedragare blir allt skickligare på att kartlägga sina tilltänkta offer.

I vissa fall uppmanas offren att ta lån för att finansiera ytterligare investeringar. I andra fall initieras låneansökningar i deras identiteter utan att de är fullt medvetna om vad som sker. Fjärrstyrningsprogram är vanligt förekommande vid investeringsbedrägerier, för att ta kontroll över offrets dator. Genom att signera uppdrag, ibland utan att förstå vad de godkänner, riskerar offren att förlora mycket pengar. Precis som vid övrig social manipulation spelar bedragarna på känslan av att offren behöver agera snabbt.

Kunderna överför pengar i syfte att göra en investering som utlovas vara väsentligt bättre än både bankernas avkastning på konton och den realistiska avkastningen på placeringar. När investeringen ser ut att ha ökat och offret försöker ta ut sina pengar försvårar bedragarna detta genom att påstå att avgifter och skatter behöver betalas. Detta gör att värdet på investeringen plötsligt sjunker drastiskt, vilket ofta gör att offret börjar inse att de har blivit lurade.

I många fall kontaktas offren senare av ytterligare bedragare som utger sig för att komma från myndigheter eller advokatbyråer och som erbjuder hjälp att få tillbaka pengarna. Självklart medför hjälpen en kostnad, vilket leder till att offren utnyttjas en gång till.

Eftersom kontakten med bedragaren ofta pågår länge tenderar offret inledningsvis att lita mer på bedragaren än på den egna banken. Ett negativt tonläge i samhällsdebatten om finansiella företag påverkar relationen mellan bank och kund. Bankerna lägger ned stora resurser på att prata med sina utsatta kunder men det är väldigt svårt att få kunden på andra tankar. Många gånger förnekar de själva hur stora belopp de har skickat i väg och hur lång tid det har pågått. För banken finns också en utmaning att förstå om kunden är bedrägeriutsatt eller om kunden har gjort en dålig investering.

Målvakter möjliggör bedrägerier

Målvakter är i detta sammanhang möjliggörare för finansiell brottslighet, och antalet målvakter i Sverige fortsätter att vara ett problem. Kriminella som upptäcks i en bank byter snabbt till en annan bank och fortsätter sina brottsliga aktiviteter där. Bankerna arbetar strukturerat med att analysera och motverka målvakternas möjligheter till upprepad brottslighet.

Målvakter och målvaktskonton är en förutsättning för bedragarnas verksamhet. Antalet penningmålvakter verksamma i Sverige är stort. Totalt har drygt 80 000 personer registrerats som skäligen misstänkta för bedrägeribrott under perioden 2018–2021, enligt Polisen, men mörkertalet är förmodligen stort. Ett fungerande flöde av information mellan bankerna och Polisen är därför avgörande för att höja effektiviteten i brottsbekämpningen. Utan sådan informationsdelning kommer det att vara svårt för bankerna att motverka målvakters manöverutrymme och förhindra bedrägerier och penningtvätt.

Unga människor utnyttjas och används ofta som målvakter, vilket kan vara en ingång till grövre kriminalitet. Ett upplägg kan vara att den unga personen lockas med löfte om att snabbt tjäna 10 000 kronor mot att ta emot och skicka vidare 250 000 kronor. Det kan senare leda till hotfulla situationer när den unga vill dra sig ur.

Ett annat sätt att rekrytera målvakter är att först utsätta personen för ett investeringsbedrägeri. Personen manipuleras att göra en ”investering” i tron att den kommer att ge hög avkastning. Först luras personen på små belopp som dock ofta snabbt eskalerar till större belopp. När kunden har slut på egna medel uppmanas denne att låna pengar för att investera ytterligare. Kunden riskerar att hamna i en desperat situation där den gör allt för att få sina pengar tillbaka. Till slut riskerar kunden att låta sig utnyttjas som målvakt för att ”rädda investeringen” genom att ta emot och skicka vidare pengar. Pengarna kan komma från andra drabbade kunder, vilket i förlängningen kan innebära penningtvätt. Kryptovalutor används ofta för att flytta pengar i vishing- och investeringsbedrägerier.

Bankföreningens åtgärdsprogram – Kundskydd mot bedrägerier

Telefonbedrägerier ökade markant under 2023 och Bankföreningens styrelse beslutade därför i december samma år att ta fram en rekommendation till bankerna avseende åtgärder för ökat kundskydd mot bedrägerier. Rekommendationen fokuserade på vishing och smishing (bedrägliga samtal och sms) och gjordes i samarbete med Polisen. Den presenterades i maj 2024.

Åtgärderna, som ska införas snarast, men senast under 2025, omfattar bland annat:

- Limiter (beloppsbegränsningar).
- Tidsfördröjning.
- Möjlighet till dualitet (två måste godkänna transaktionen).
- Översyn av produkter som tillhandahålls.
- Kontroll vid nya produkter.
- Förbättrad transaktionsmonitorering.
- Information och utbildning.

Målvakter är en förutsättning för bedragarnas verksamhet och antalet målvakter i Sverige är stort.

De stora bankerna hade vid utgången av 2024 de flesta av åtgärderna på plats. Initiativet har fått positiv återkoppling från kunderna.

Åtgärdernas effekt på bedrägeriutvecklingen följs upp tillsammans med Polisen. Statistik från Polisen visar att brottsvinsterna från vishing sjönk med 40 procent från 2023 till 2024 och en tydlig nedgång av det genomsnittliga beloppet per vishing-brott. Den förstärkta utfärdandeprocessen för Mobilt BankID har resulterat i att antalet obehöriga transaktioner vid utfärdande av Mobilt BankID, i princip, har upphört.

Bristande statistik för bedrägeriområdet

Bankerna arbetar för att bättre förstå vilken åtgärd som får vilken effekt för Sverige. För den enskilda banken är det enkelt att förstå sina egna åtgärder men det är svårare när man vill förstå effekten av en åtgärd på samtliga polisanmälningar i Sverige.

Statistiken från Polisen, Finansinspektionen och Europeiska centralbanken är i första hand till för dem själva och det är svårt att dra någon slutsats om uppgifterna. Polisens statistik åskådliggör varken bankernas eller polisens åtgärder, huruvida det är behöriga eller obehöriga transaktioner, eller om det är konsumenter eller företag som drabbats. Polisens data är komplex och det är svårt att få fram uppgifter om brottsvinster för andra tillvägagångssätt än telefonbedrägerier. Polisen behöver därför utveckla möjligheterna att polisanmäla brott för att stärka analysförmåga och beslutsstöd, steg i den riktningen har tagits.

Bedömningen är att bankernas gemensamma brottsförebyggande ansträngningar har haft stor framgång. Riskerna för bedrägerier och finansiella brott är dock fortsatt hög samtidigt som hotbilden blir alltmer komplex och samverkande genom kombinerande tillvägagångssätt i samma brottsupplägg.

Behov av åtgärder från politik och myndigheter

- Lagstiftaren bör begränsa publicering av personuppgifter på internet. Det är i dagsläget allt för enkelt att söka fram exempelvis ensamstående äldre med god ekonomi. Förändringen behöver samtidigt tillgodose bankers legitima behov av att kunna utföra olika typer av kontroller.
- Teleoperatörer verksamma i Sverige bör åläggas att försvåra/omöjliggöra maskering av telefonnummer genom en anti-spoofing-infrastruktur för telefon och sms.
- Regeringen bör genomföra förslagen i ID-kortsutredningen (SOU 2019:14), att minska antalet utfärdare av fysiska id-kort och förbättra bankers möjlighet att kontrollera id-handlingar. Den fysiska id-handlingen knyter ihop den fysiska identiteten med den digitala identiteten i två riktningar: först när banken utfärdar BankID och därefter som extra kontrollmöjlighet när e-legitimationen används med utgångspunkt från bankens riskmonitorering.
- Bankerna bör få utbyta information med varandra på ett enklare sätt. Ett flöde av information mellan bankerna och Polisen behövs också, exempelvis uppgifter om målvakter. För bankerna är syftet med en effektiv informationsdelning att stärka kundkännedom och riskbedömning av kunderna, samt transaktionsmonitorering.
- Polismyndigheten bör utveckla möjligheterna för brottutsatta att polisanmäla alla de vanligaste bedrägeriformerna på nätet. Dagens begränsade möjligheter att polisanmäla brott, det kan exempelvis ta lång tid att komma fram via 114 14, riskerar att skapa ett mörkertal angående brottslighetens omfattning.
- De viktigaste åtgärderna för att motverka investeringsbedrägerier är:

  1) Att tech-bolagen tar ett större ansvar för det som publiceras på deras plattformar. Plattformar som exempelvis Facebook, WhatsApp och Instagram är stora möjliggörare för falska annonser som publiceras där och som lurar kunderna, exempelvis genom investeringsbedrägerier. Plattformarna bör därför höja minimikraven för att få annonsera i syfte att få bort, eller i vart fall, minska antalet bedrägliga annonser på olika plattformar.

  2) Att bankerna får bättre möjlighet att spåra användningen av fjärrstyrningsprogram. Fjärrstyrning är mycket vanligt vid investeringsbedrägerier. Under förevändning av att hjälpa kunden tar bedragaren kontroll över offrets enhet genom verktyg som Anydesk och TeamViewer, och kan sedan utföra bedrägliga transaktioner. Leverantörer av den här typen av verktyg bör därför åläggas att erbjuda ett API som möjliggör för bankerna att upptäcka om fjärrstyrning används för en kund.

Samhället vill inte ha pengar som härrör från brott. En brottsvinst som inte kan användas saknar i princip värde.

Penningtvätt

Penningtvätt omfattar i praktiken en rad olika så kallade penningtvättsåtgärder. Det kan röra sig om transaktioner av brottsutbyte mellan olika bankkonton eller omsättning genom inköp, men även andra åtgärder som till exempel att använda falska handlingar som representerar ett värde. Penningtvätt kan föregås av relativt enkla brott med enstaka aktörer inblandade och av komplicerade brottsupplägg som ofta involverar en hel kedja av aktörer som agerar i samförstånd. Den som gjort sig skyldig till penningtvätt enligt lagens mening döms för penningtvättsbrott alternativt näringspenningtvätt.

För bankernas del yttrar sig penningtvätt i normalfallet som transaktioner av brottsutbyte mellan olika bankkonton. Goda rutiner för kundkännedom och en ändamålsenlig monitorering av kundbeteende är därför de viktigaste verktygen för att banken ska upptäcka och förebygga penningtvätt. Övervakningen sker löpande i syfte att upptäcka avvikande aktiviteter och transaktioner.

Av all upptäckt penningtvätt i Sverige bedöms en övervägande andel ske genom det reguljära finansiella systemet. I övrigt sker det genom bland annat kryptovalutor, spelmarknaden, hawala-banking (ett alternativt betalningssystem för främst internationell penningöverföring utanför banksektorn, som från och med den 1 juli 2025 omfattas av krav på tillstånd från Finansinspektionen) och handel med varor och tjänster.

Under 2024 lämnades totalt 52 831 rapporter om misstänkta transaktioner (STR) samt 8 509 rapporter om misstänkta aktiviteter (SAR) till FIPO, vilket var en ökning med 4% respektive 54% jämfört med 2023. Banker stod för den överväldigande majoriteten av rapporterna. Totalt sett stod finanssektorn för över 90 % av rapporterna, enligt FIPO:s statistik.

De största penningtvättshoten

Samhället vill inte ha pengar som härrör från brott. En brottsvinst som inte kan användas saknar i princip värde. Penningtvätt uppstår då kriminella försöker dölja härkomsten av sina brottsligt intjänade pengar.

Kriminella uppvisar ofta stor uppfinningsrikedom när det gäller att hitta nya sätt att tvätta pengar. Det kan handla om att investera brottsutbytet där omsättningsmöjligheterna är stora och kontrollerna inte är tillräckliga. Det finns även områden där kontroll av penningtvätt ännu inte kan utövas på ett tillfredsställande sätt, till exempel kryptovalutor.

Det internationella betalningssystemet utnyttjas också för att föra ett brottsutbyte utom kontroll för ett visst lands myndigheter. Överföringar kan ske till eller från länder som inte samarbetar med svenska myndigheter, eller där samarbetet inte fungerar effektivt. Under 2024 har svenska myndigheter trappat upp sina ansträngningar för att utöka det internationella rättsliga samarbetet i brottmål, vilket kan innefatta spårning och säkrande av bortförda tillgångar. Ännu återstår att se effekten av de avtal som tecknats om rättslig hjälp och utlämning av misstänkta.

De främsta hoten mot bankernas arbete mot penningtvätt och finansiering av terrorism utgörs av den organiserade brottsligheten som genom användning av målvakter, bulvaner och juridiska personer utnyttjar bankernas tjänster och produkter i brottsliga syften utan att exponera sig personligen. En annan aspekt av anonymiteten är den begränsade information som kan erhållas om motparter i betalningar som följer av den snabba utvecklingen av alternativa betallösningar. Eftersom penningtvätt kan genomföras på så många olika sätt är det en utmaning att överblicka utvecklingen och snabbt vidta effektiva motåtgärder.

Offentliga kontroller i förhållande till penningtvätt

Den nationella antipenningtvättsregimen har brister, vilket medför att staten i vissa fall kan understödja eller underlätta för kriminellas verksamhet och penningtvätt. Många regler är utformade efter förhållanden som inte längre är aktuella medan existerande företeelser inte omfattas av befintliga regelverk.

Myndigheter och reglering kring företagande är i vissa fall inte tillräckligt anpassade till hotbilden från den organiserade brottsligheten, vilket visar sig till exempel i dåliga eller obefintliga kontroller av verksamheter och enskilda personer, något som möjliggör välfärdsbrottslighet och skattebrottslighet.

Svårupptäckta penningtvättupplägg

Eftersom en bank enbart kan se den del av en transaktionskedja som försiggått hos den själv, är avancerade kedjor av penningtvätt med transaktioner i flera banker, ofta svåra att upptäcka. Bankerna har endast begränsade möjligheter att utbyta information med andra banker.

För att motverka den ökade bedrägeribrottsligheten har svenska banker genomfört tekniska förbättringar men även inskränkningar i förhållande till kunderna. Det har lett till att tillvägagångssätten för penningtvätt ändrats.

Antalet möjliga sätt att genomföra transaktioner har ökat under de senaste åren, en utveckling som förväntas fortsätta under 2025. Effekten av detta är i vissa fall minskad förståelse för pengarnas ursprung samt reducerade möjligheter för bankerna att övervaka och begränsa en kunds tjänster utifrån transaktionstyp. Detta medför att bankerna ställs inför utmaningar för att på ett effektivt sätt kunna övervaka och vidta åtgärder för transaktionstyper som bedömts utgöra en hög risk.

Finansiellt underrättelsecentrum

I december 2024 gav regeringen i uppdrag till Polisen, Ekobrottsmyndigheten och Skatteverket att under 2025 i samråd med näringslivet (banker med flera) inrätta ett finansiellt underrättelsecentrum (Finuc). Finuc kommer att innebära en utökad varaktig samverkan mellan myndigheterna och näringslivet inom bland annat penningtvättsområdet. Det övergripande syftet är att parterna gemensamt ska medverka till att strypa den kriminella ekonomin genom effektiv informationsdelning och konkreta åtgärder.

Finuc är verksamt sedan den 1 april 2025, men uppbyggnaden av centrets verksamhet kommer att ske successivt under en längre tid. Förväntningen på längre sikt är att Finuc ska kunna agera snabbt och effektivt i såväl brottsförebyggande syfte som i förhållande till avancerade penningtvättsupplägg. Initiativet är angeläget, men det återstår att se om de legala förutsättningarna medger tillräckligt effektiv informationsdelning och annan samverkan.

Välfärdsbrottslighet och skattebrott

Så fort nya statliga eller kommunala bidrag eller stöd inrättas drar det till sig intresse från kriminella. Något som tydligt visat sig vid utbetalningar av ekonomiska stöd relaterade till covidpandemin, el och miljöbefrämjande åtgärder.

Kriminella analyserar även skattelagstiftningen och skatteförfarandet i EU och Sverige, för att hitta luckor och brister och skräddarsy brottsupplägg. Sådana brottsupplägg nyttjas av bland andra internationella kriminella organisationer som sätter upp en brottslig bolagsstruktur i Sverige.

Kriminellas utnyttjande av välfärdssamhället och skattesystemet utgör en särskild utmaning för bankerna eftersom utbetalningarna kommer från avsändare med högt förtroende, det vill säga myndigheter. Det är svårt för en bank att kontrollera om det rör sig om en bakomliggande brottslighet där myndigheter har lurats till utbetalning på felaktiga grunder. Mottagarna är dessutom i allmänhet vanliga personer eller företag där det saknas anledning att misstänka att de inte skulle ha rätt att ta emot pengarna.

Kontrollerna måste därför i första hand göras av den beslutande eller utbetalande myndigheten. Från och med 2024 har en ny myndighet, Utbetalningsmyndigheten, inrättats med uppgiften att kontrollera utbetalningar från välfärdssystemen. När myndigheten kommit igång och fullgör sitt uppdrag fullt ut kan man förvänta sig en minskning av felaktiga utbetalningar inom ramen för välfärdbrottslighet. I sin tur minskar detta bankernas risk för överföringar av brottsutbyte och därmed penningtvätt.

Fastighetsmarknaden och bostadsrättsföreningar

Fastighetsmarknaden är attraktiv för penningtvätt eftersom fast egendom kan nyttjas på många olika sätt och kräver en stor investering. En stor mängd brottspengar kan då tvättas med endast ett inköp. Fastigheten kan sedan nyttjas till egen användning, uthyrning eller vidareförsäljning. Ytterligare pengar kan tvättas genom investeringar i form av exempelvis renovering och utbyggnad, vilket dessutom kan bidra till att generera mervärde. Företag i byggbranschen förekommer relativt ofta i bankernas utredningar om misstänkt penningtvätt.

Generellt sett finns ett intresse av att fastighetsaffärer genomförs snabbt, vilket i många fall hamnar i konflikt med kontrollintresset. Fastighetsmäklare kanske underlåter eller gör alltför summariska penningtvättsrelaterade kontroller. Inom en alltmer

pressad och konkurrensutsatt fastighetsbransch är det viktigt att inte frångå kravet på ändamålsenliga kontroller.

Bostadsrättsföreningar är sårbara för penningtvätt. Det förekommer penningtvättsupplägg där värden kan överföras mellan olika individer genom under- eller övervärdering av objektet vid köp eller försäljning. Bostadskrediter givna under felaktiga premisser kan användas för att finansiera dessa upplägg.

Kryptotillgångar samt betalningar och valutaväxling

Kryptotillgångar, inklusive kryptovalutor, är en relativt ny bransch som är mycket sårbar för penningtvätt. Marknaden är global och volatil. Flera av världens största aktörer är registrerade i länder med bristande antipenningtvättsregimer eller med sekretessregler som förhindrar transparens. Kryptovalutor används ofta som betalningsmedel av kriminella vid illegal handel på till exempel Darknet samt vid ransomware-attacker. I de fall inköp av kryptovalutor kan betalas med bankkort uppstår en koppling mellan det traditionella finansiella systemet och kryptomarknaden.

Betalning i kryptovaluta har dessutom blivit ett allt vanligare betalningsmedel såväl i detaljhandeln som mellan enskilda personer, vilket också ökar risken för penningtvätt. I och med ett större fokus på kryptovalutor ökar dock medvetenheten hos näringslivet om risken med att ta emot dem som betalningsmedel.

Särskilda högriskgrupper är de som tillhandahåller tjänster avseende kryptovalutor, som betalningsförmedlare och valutaväxlare. De omfattas idag inte av samma omfattande regelverk som gäller för banker, och vissa aktörer är ännu helt oreglerade. De har i många fall bristfälliga processer och kontroller för att förhindra penningtvätt, samtidigt som de använder bankernas infrastruktur och därigenom överför sina egna risker till banken. Vid transaktioner som rör kryptotillgångar går medlen i stor utsträckning till förmedlare av tjänster vars mottagarkonton finns i forna östblocket.

En alltmer beaktansvärd risk är att länder och andra aktörer utnyttjar kryptovalutor för att kringgå internationella sanktioner. Kryptovalutor har nämligen visat sig vara användbara för att ersätta globalt gångbara valutor som exempelvis amerikanska dollar. Vidare kan handel med kryptovalutor vara ett alternativ för de aktörer som genom sanktioner utestängs från internationella betalningssystem.

Internationellt samarbete med korresponderande regleringar, definitioner och standarder kan bli helt avgörande för kontrollen av kryptomarknaden och därmed minskade penningtvättsrisker framöver.

Samtidigt som omsättning av kryptotillgångar är sårbar för penningtvätt ger den dock större möjligheter till analys än kontanter. Mycket data om transaktioner av kryptotillgångar är nämligen offentlig på internet. Att analysera denna data är både en möjlighet och en växande utmaning för intressenter på marknaden och brottsbekämpande myndigheter.

I december 2024 trädde EU:s nya förordning om marknader för kryptotillgångar (MiCA-förordningen, nedan; MiCA) i kraft. MiCA syftar bland annat till att underlätta rättssäkerheten för företag och att locka fler investeringar till EU-länder. EU är nu den största jurisdiktionen i världen som infört ett omfattande regelverk för kryptomarknaden. Vilken effekt MiCA i praktiken kommer att få återstår att se.

Även betalningsförmedling och valutaväxling som bedrivs yrkesmässigt eller annars i större skala är sårbar för penningtvätt. Det finns exempel på sådana verksamheter som drivs av kriminella. Eftersom de använder sig av bankernas betalinfrastruktur påverkar de sårbarheten i banken. Under senare år har reglering tillkommit i syfte att öka kraven på bland andra valutaväxlare, vilket bör bidra till en minskad risk för penningtvätt.

Avancerade kedjor av penningtvätt med transaktioner i flera banker är ofta svåra att upptäcka.

Lyxvaror och fordon

Marknaden för varor och tjänster i lyxsegmentet såsom smycken, klockor, guld, märkeskläder, resor och hotell har vuxit över tid. Den attraherar kriminella, både som verktyg för att tvätta pengar och som investering av kriminella tillgångar. Ofta sker betalningen kontant eller med andra medel med oklar bakgrund. Många av lyxvarorna är lätta att flytta mellan olika länder och sälja vidare med bibehållet värde. På så sätt kan de användas för att överföra värden utan tillräcklig spårbarhet.

Ett förekommande tillvägagångssätt är att köpa en lyxvara kontant hos en handlare och sedan lämna tillbaka den. Handlaren har då inte så mycket kontanter tillgängliga, utan pengarna återbetalas genom insättning på kortkonto (i strid med kortregelverken). På så vis kommer kontanter med brottslig bakgrund in i det finansiella systemet.

I fråga om handel med fordon, främst personbilar, förekommer olika upplägg av penningtvätt. I vissa fall härrör köpeskillingen från ett brottsutbyte som tvättats i olika led, med hjälp av till exempel falska låneavtal och bankkonton i utlandet. Vidare kan det vara fråga om brottsupplägg där fordon som köpts med brottsutbyte importeras eller exporteras, samt upplägg i syfte att undvika skatter eller avgifter.

Spel och dobbel

Spelsektorn uppvisar en hög risk för penningtvätt. Spelföretagens konton kan användas i penningtvättsyften på så vis att pengarna förvaras och sammanblandas med andra medel. I sin tur innebär detta, när uttag eller överföringar från spelkontona görs, att pengarnas ursprung kan framstå som legitimt. Spelsektorn hanterar även kontanter i relativt stor omfattning, vilket är förenat med särskilt stora penningtvättsrisker.

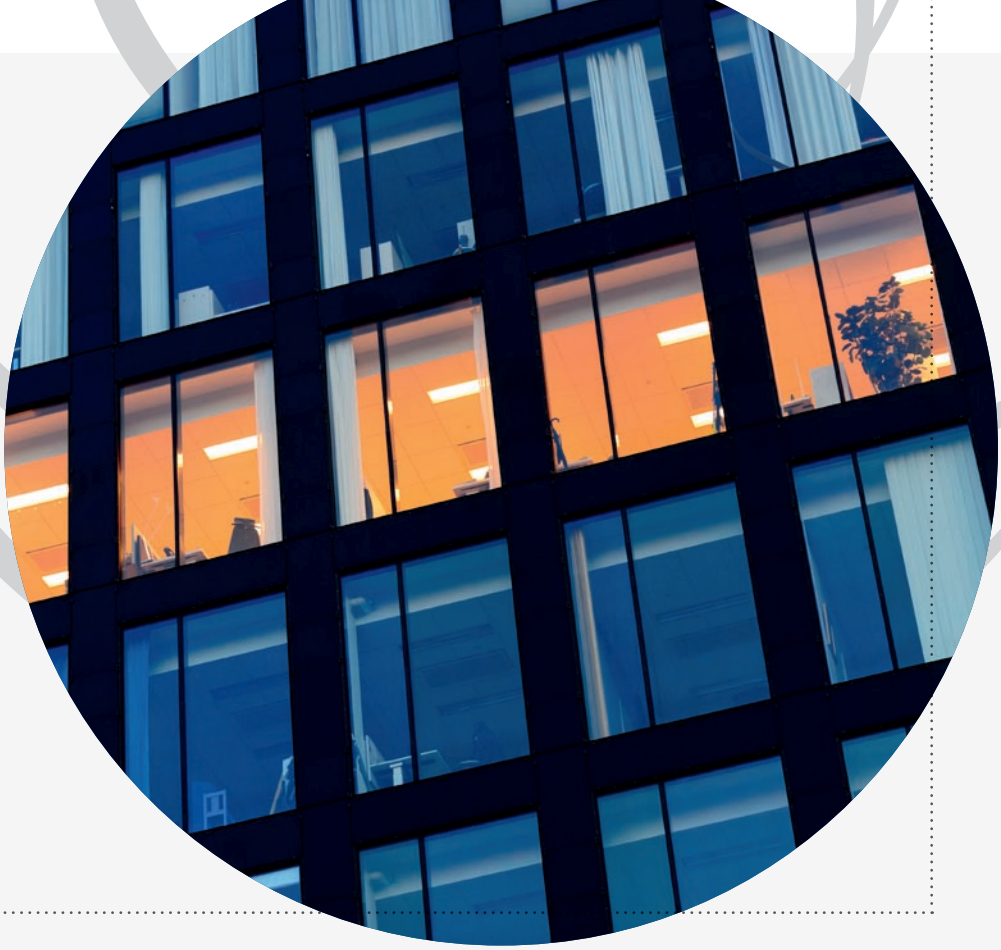
Spelfusk genererar brottsutbyte som utbetalas till involverade personer. Sådan brottslighet har inslag av korruption och torde vara särskilt svårupptäckt för såväl myndigheter som andra aktörer.

Spelföretag kan förekomma som såväl online-baserade som traditionella kasinon på fysiska adresser (i proposition 2024/25:73 föreslås dock en avveckling av statliga kasinon). Online-baserade företag är ofta belägna i lågskatteländer. Även om marknaden är reglerad och omfattas av penningtvättsregelverket finns åtskilliga olicensierade företag. Att spelföretagens intresseorganisationer verkar för goda rutiner och kunskapsspridning bland sina medlemmar bör bidra till att riskerna inom området minskar på sikt.

Behov av åtgärder från politik och myndigheter

- Risker för penningtvätt och finansiering av terrorism behöver omfattas av samma reglering och tillsyn, oavsett var de uppstår. Om banker ska kunna tillhandahålla konton till högriskverksamheter behöver regleringen och kontrollen av sådana verksamheter ökas betydligt.
- För att åtgärderna mot penningtvätt och finansiering av terrorism ska kunna bli effektiva behöver bankerna få bättre möjligheter att dela information om misstänkta kunder, transaktioner och aktiviteter med varandra. Den organiserade brottsligheten utnyttjar det faktum att bankerna idag inte kan dela information sinsemellan. När kriminella upptäcks i en bank byter de omedelbart till en annan bank och fortsätter sina brottsliga aktiviteter där.
- De nya reglerna om samverkan och informationsutbyte mellan banker och brottsutredande myndigheter är ett steg i rätt riktning, men de behöver utvecklas ytterligare. Genom permanenta samverkansformer kan den erfarenhet och det förtroende mellan aktörerna som är nödvändig byggas upp och nå resultat. Inrättandet av Finuc är ett välkommet initiativ för ett effektivare informationsutbyte mellan berörda parter. Finuc behöver dock ges legala förutsättningar att kunna verka på ett ändamålsenligt och effektivt sätt, med en vid deltagarkrets och mot olika typer av ekonomisk brottslighet.
- Finanspolisen behöver tillräckliga resurser för att snabbt hantera och återkoppla avseende alla misstankerapporter som lämnas av de aktörer som omfattas av penningtvättsregelverket. Om beslut om dispositionsförbud inte fattas skyndsamt finns en risk att brottsliga pengar förs utom bankers och myndigheters kontroll.

Bedömningen är att så länge den brottslighet som genererar ett ekonomiskt brottsutbyte fortsätter att ligga på en hög nivå i samhället, är risknivån för penningtvätt fortsatt hög. Bankerna försöker kontinuerligt begränsa sina risker, i huvudsak genom goda rutiner för att uppnå kundkännedom och en ändamålsenlig transaktionsövervakning. Måttet av kontroll inom offentlig verksamhet och välfärdssystemet behöver öka ytterligare i syfte att begränsa förutsättningarna att kunna genomföra den brottslighet som föregår penningtvätt.



Nyttjande av företag i brottsliga syften

Det har alltmer uppmärksammats att kriminella aktörer i stor omfattning nyttjar företag för att begå brott. Även om fenomenet har varit utbrett under lång tid, har en ökning skett under senare år.

I allmänhet är det fråga om ett brottsligt nyttjande av små eller medelstora aktiebolag. Brottsliga inslag kan dock förekomma även i stora välrenommerade företag, där en del av verksamheten kan syfta till exempelvis skatteundandragande och därmed konkurrensfördelar. Att till exempel enskilda näringsverksamheter, handelsbolag, kommanditbolag eller stiftelser nyttjas i brottsliga syften är mindre vanligt, men förekommer. I fråga om stiftelser finns sannolikt ett visst mörkertal.

Anledningarna till att företag är särskilt attraktiva som brottsverktyg är många. Kriminella kan på så sätt gömma sig bakom företagets fasad av legitimitet. Det kan även handla om att företaget öppnar för andra typer av lukrativ brottslighet, genom nyttjande av den säkerhet och stabilitet som ett bolag representerar för samhället eller enskilda. Med hjälp av ett företag kan kriminella aktörer tillskansa sig stora belopp på relativ kort tid. De enskilt mest lukrativa ekonomiska brottsuppläggen ofta drabbar den offentliga sektorn.

Låg upptäcktsrisk

Risken för att dömas till ansvar för brott har länge varit relativt låg, vilket har en mängd olika orsaker. Bland de viktigaste orsakerna återfinns sannolikt bristande möjligheter och skyldigheter till kontroll och informationsdelning mellan myndigheter och andra aktörer som är involverade vid ett företags bildande och löpande drift. Vidare kan en förundersökning om brott inom en verksamhet i många fall syfta till att utreda en viss typ av anmäld brottslighet, medan resurser saknas till en bredare ansats innefattande samtliga typer av brottslighet som upptäcks.

Brottstyper

Ett företag kan användas för att begå olika typer av brottslighet. Vanligt förekommande är exempelvis nyttjande av svart arbetskraft (skattebrott), momsbedrägerier (skattebrott), bedrägerier såsom exempelvis kreditbedrägerier samt olika typer av välfärdsbrottslighet. Vidare kan brottsupplägg som i sig syftar till penningtvätt via företag förekomma.

Mörkertalet kan misstänkas vara fortsatt stort. Man kan utgå ifrån att många fall av penningtvätt samt eller skatte- och välfärdsbrottslighet med hjälp av företag, inte anmäls eller ens upptäcks.

Tillvägagångssätt

Många företag startas i syfte att användas för brott, där svagheter i olika system utnyttjas parallellt. Företaget används intensivt under den tid det tar innan varningssignaler hos myndigheter och banker genererar frågor och åtgärder. Företaget anses då förbrukat och avvecklas eller överges. En sista åtgärd kan vara att utnyttja en konkurs för ytterligare brottslig vinning. När företaget överges är det tömt på tillgångar och bara skulder finns kvar.

De som bedriver den brottsliga verksamheten i ett företag tar sällan hänsyn till andra intressen än sina egna. Tidigare anställda eller aktörer som man gjort affärer med drabbas ofta av långvariga ekonomiska problem. Borgenärer har dåliga utsikter att få tillbaka pengar på sina fordringar.

Ofta blir det målvakten, det vill säga den som figurerat som formell företrädare för företaget, som hålls straffrättsligt ansvarig för brottsligheten. Målvakten kan i vissa fall vara en ung person eller en person med svag anknytning till det svenska samhället.

Olika typer av brottslighet bedrivs ofta inom ett och samma företag, parallellt eller i följd. Det är även vanligt att samma kriminella nätverk driver många olika företag samtidigt och genomför brottsliga dispositioner dem emellan. Det kan till exempel gälla storskaliga och systematiska upplägg för att begå skattebrott eller välfärdsbrott.

Avancerade brottsupplägg

I takt med dels att brottsbekämpande myndigheter blir alltmer effektiva, dels att regleringar skärps, behöver de kriminella utveckla sina brottsupplägg. Följden blir alltmer avancerade brottsupplägg. Legitim och brottslig verksamhet kan kombineras inom samma företag. Till exempel genom avancerade bolagsstrukturer och internationella kopplingar, skickligt förfalskade handlingar och målvakter med mindre förväntad profil. Sådana väl förberedda brottsupplägg är svårare att upptäcka för brottsbekämpande myndigheter och banker.

Avancerade brottsupplägg kan säljas eller administreras av internationella kriminella nätverk. De personer som utför brotten i Sverige begriper inte alltid hur upplägget totalt sett fungerar och hur ett brottsutbyte de facto genereras.

Understödjare och möjliggörare

För att ett företag ska kunna drivas i brottsligt syfte är det nödvändigt att en rad olika initiala åtgärder vidtas. Till exempel behöver ett nytt företag startas upp eller ett befintligt företag förvärvas.

Externa aktörer kan behöva involveras som understödjare eller möjliggörare av brottsligheten.

Till exempel kan det vara fråga om att förvärva ett så kallat historikföretag (företag med en dokumenterad historik av till synes legitim verksamhet) av en företagsförmedlare och därvid genomföra nödvändiga registreringar hos Bolagsverket.

För att skapa en varaktig legitim fasad är det ofta en del i brottupplägg att den löpande bokföringen ska skötas. En redovisningskonsult anlitas då för bokföring och skattedeklarationer till Skatteverket.

Kriminella nyttjar ofta företag för att kunna begå olika typer av brott.

Som underlag för bokföring och som bevisning för betalningar kan osanna fakturor, transporthandlingar eller andra förfalskade skriftliga handlingar behöva införskaffas. Det är vanligt att externa möjliggörare tillhandahåller sådana handlingar mot betalning.

Andra aktörer, såsom legitima affärspartners, kreditgivare och kontoförande banker, behöver kunna lita på att bland annat registreringar hos Bolagsverket, uppgifter från Skatteverket och upprättad bokföring motsvarar verkliga förhållanden. Motparter behöver kunna veta vem man gör affärer med eller ger krediter till och under vilka premisser. Likaså behöver myndigheter veta exempelvis vem som driver en verksamhet, vilka som är anställda och i vilken omfattning arbete bedrivs.

Risker i förhållande till bankverksamhet och företagskonton

Ett företag utan tillgång till företagskonto är inte användbart, vare sig i legitima eller brottsliga syften. En del av brottsplanen innebär således ofta att få tillgång till konto i en svensk bank i många fall även valutakonto. Konto i en svensk bank innebär såväl låga transaktionskostnader, som förespeglar legitimitet i verksamheten.

Bankärenden genomförs ofta av målvakter, eller andra befullmäktigade personer som inte väcker misstankar.

Ur bankens synvinkel framstår förfarandet i allmänhet som normalt och väcker därför inga misstankar under en pågående bankförbindelse. Att till exempel genomföra förändringar i styrelse och verksamhet är normala åtgärder även för legitima verksamhetsutövare, och ger inget misstänkt utslag i bankens kundkännedomsanalys (KYC).

Först då den brottsliga verksamheten avviker från det normala och till exempel ger utslag inom bankens transaktionsövervakning påbörjar banken en utredning och eventuell process för att avsluta kundrelationen. Vid det laget är det inte ovanligt att företaget redan tjänat sitt brottsliga syfte och anses som förbrukat.

När det gäller brottslighet med längre varaktighet, där ett företag eller en bolagsstruktur kontinuerligt används i såväl legitima som brottsliga syften är brottsligheten än svårare för banken och andra aktörer att upptäcka. Inom ramen för sådana verksamheter, som i vissa fall kan bedrivas av stora välrenommerade bolag, kan de brottsliga transaktionerna över företagskonton eller internationella betalningar utgöra endast en viss andel av de totala pengaflödena.

Att förhindra att personer med brottsliga syften får tillgång till ett företaget är en utmaning för samhället.

Behov av åtgärder från politik och myndigheter

- Banker måste kunna lita på uppgifter och betalningar från svenska myndigheter. Staten behöver därför ta ansvar för att kontrollera och verifiera de uppgifter som finns i statliga register för att minska risken för att myndigheterna utnyttjas av den organiserade brottsligheten.
- Bolagsverket måste skärpa sina kontroller för att uppnå tillräcklig effektivitet och precision i de registrerade uppgifterna. Bankföreningen välkomnar det arbete som påbörjats inom ramen för regeringens nya uppdrag till Bolagsverket.
- Redovisningskonsulternas verksamhet måste regleras. Statlig auktorisation bör bli obligatorisk, för att motverka kriminellas tillgång till bokföringstjänster.
- Företagsförmedlare måste regleras. Statlig auktorisation eller motsvarande reglering bör bli obligatorisk, för att motverka att kriminella får snabb och alltför enkel tillgång till befintliga eller nya företag.
- Finuc behöver ges legala förutsättningar att kunna genomföra förebyggande arbete i förhållande till brott med hjälp av företag. Det är till exempel fråga om att kunna inkludera viktiga aktörer som Bolagsverket, Kronofogden och Utbetalningsmyndigheten i samverkan.

Bedömningen är att det för bankerna innebär en utmaning att genom bland annat informationsutbyte och avancerade tekniska lösningar förfina sina metoder för att upptäcka risker för brottslighet med hjälp av företagskonton. Ändamålsenliga och fördjupade granskningar i samband med att affärsförbindelser inleds med företag, särskilt inom högriskbranscher, kan verka brottsförebyggande.

Det finns ofta samband mellan organiserad brottslighet och terrorfinansiering.

Finansiering av terrorism

En viktig riskfaktor i fråga om finansiering av terrorism är att bankerna saknar tillgång till tillräcklig och aktuell information om hur sådan finansiering går till samt vilka personer och företag som är inblandande. Vet bankerna inte vad de ska reagera på eller leta efter blir det svårt att upptäcka misstänkt terrorfinansiering.

De senaste åren har antalet fall av misstänkt finansiering av terrorism via kryptovalutor ökat. För banker som inte erbjuder tjänster relaterade till kryptovalutor ökar dock inte riskerna annat än indirekt.

En ökande överlappning mellan organiserad brottslighet och terrorfinansiering noteras i omvärldsbevakningen. Omfattande och komplex internationell skattebrottslighet (till exempel momskaruseller som under senare år har drabbat det svenska skattesystemet i stor omfattning), kräver avsevärd organisation och stora initiala investeringar. Inte sällan är det fråga om tio- eller hundratals miljoner kronor. Investeringarna kan komma från internationella kriminella nätverk som i sin tur kan misstänkas ha kopplingar till terrorism. Brottsvinsterna går på olika sätt tillbaka till de internationella kriminella nätverken i utlandet och är därmed svåra att spåra.

För bankernas del är riskerna svåra att upptäcka, bland annat eftersom omsättningen normalt sett förefaller legitim och utbetalaren i detta fall är Skatteverket.

Andra finansieringsformerna för terrorism är organiserad välfärdsbrottslighet, kreditbedrägerier, missbruk av humanitär hjälp och kontantsmuggling.

Även crowdfunding används för finansiering av terrorism. En stor grupp individer finansierar då med små summor en verksamhet eller ett projekt. Plattformar för crowdfunding möjliggör för privatpersoner att starta olika typer av insamlingar på internationell nivå via internet. För banken är det mycket svårt att skilja legitima insamlingar från sådana som sker med bakomliggande intentioner att finansiera terrorism.

Internationell terrorism är den grundläggande orsaken till många av världens sanktionsregimer. Tillämpning av sanktioner utfärdade av till exempel Office of Foreign Assets Control (OFAC; USA:s primära sanktionsmyndighet) medför i praktiken starkt minskade risker för banker att oavsiktligt medverka till finansiering av terrorism.

Bedömningen är att genom ökad informationsdelning om tillvägagångssätt samt relevanta aktörer för finansiering av terrorism kan bankernas risker minskas för att medverka till transaktioner som utgör sådan finansiering.

Internationella sanktioner

Internationella sanktioner – eller restriktiva åtgärder – är en del av EU:s gemensamma utrikes- och säkerhetspolitik. I och med en mer komplex konfliktbild och tilltagande geopolitiska spänningar i olika delar av världen har sanktioner med tiden blivit ett allt viktigare utrikespolitiskt påtryckningsmedel.

Syftet med att utfärda sanktioner är att påverka beteendet hos den som sanktionerats enligt en viss agenda hos den som sanktionerar. Det kan gälla exempelvis mänskliga rättigheter eller fredsbevarande syften. Sanktionerna kan skapa förändringar på politisk eller statlig nivå.

Sanktioner är ett alternativ till mer ingripande åtgärder såsom väpnad intervention. De kan även vara ett förstadium till mer ingripande åtgärder, det vill säga om sanktionerna inte fått önskad effekt.

En rad olika länder utfärdar sanktioner. Viktiga internationella aktörer är FN, EU, USA och Storbritannien. Sverige utfärdar i dagsläget inga egna sanktioner, utan genomför sanktioner som är beslutade av FN eller EU. I praktiken behöver svenska banker även ta hänsyn till sanktioner utfärdade av tredje land, såsom USA, för att undvika allvarliga affärsrisker, och i förlängningen risker för det svenska samhällets behov av en fungerande bankverksamhet.

Större geopolitiska spänningar medför alltmer omfattande och komplexa sanktioner.

Sanktioner kan riktas mot

- regeringar i länder utanför EU
- enheter (företag) som finansiellt stöder den politik som sanktionerna är riktade mot
- grupper eller organisationer, till exempel terroristgrupper
- enskilda personer som antingen stöder den politik som sanktionerna är riktade mot, eller är inblandade i terrorist-verksamhet etc.

Sanktioner omfattar inte bara listade enheter, utan även enheter med anknytning till listade enheter. För att efterleva internationella sanktionerna behöver bankerna därför analysera vem som äger eller har kontroll över en sanktionerad enhet. Sanktioner kan också ta sikte på en viss typ av vara eller tjänst som i sig är legitim men som den som sanktionerats kan använda i oönskade syften.

Utvecklingen inom sanktionsområdet och Rysslandssanktionerna

Sanktionerna har under senare år blivit allt svårare att överblicka och tillämpa på ett enhetligt och effektivt sätt. Det är inte bara bankerna som behöver förhålla sig till sanktionerna. Till exempel behöver industrisektorn ständigt vara uppmärksam för att inte riskera att bryta mot sanktioner.

Sedan Rysslands olagliga annektering av Krimhalvön 2014 och invasionskrig i Ukraina 2022 har EU i aldrig tidigare skådad omfattning utfärdat sanktioner mot ryska intressen. Sanktionerna är avsedda att på olika vis begränsa bland annat Rysslands militära förmåga och markera att landets beteende är oacceptabelt. Sanktionerna omfattar bland annat reseförbud, frysningar av betydande ryska tillgångar och ett oljepristak för rysk oljeexport. När denna rapport skrivs (maj 2025) har EU beslutat om sammanlagt 16 sanktionspaket mot Ryssland. Under 2025 förväntas fortsatta utökningar av Rysslandssanktionerna, bland annat i syfte att begränsa den så kallade spökflottan av oljetankers och misstänka sabotage mot kablar i Östersjön.

Ryssland kringgår dock systematiskt sanktionerna. Ryska aktörer har med hjälp av utländska intressen hittat sätt att till exempel importera avancerad teknologi som kan användas inom krigsindustrin eller få ut marknadspris på olja. Genom namnbyten på bolag, förfalskningar av handlingar, bulvaner, med mera försöker man dölja vem eller vilka personer som i själva verket äger eller styr företag. Rysslandssanktionerna syftar nu i mångt och mycket till att försöka komma till rätta med undandraganden och kringgåenden, vilket sannolikt kommer fortsätta vara prioriterat inom EU under 2025.

Samverkan inom sanktionsområdet

Storskaliga och systematiska sanktionsöverträdelser ställer ökade krav på såväl verksamhetsutövare som myndigheter inom EU. Förståelse för problemet är grundläggande. Alltmer omfattande sanktioner och en alltmer komplex och riskabel kontext medför stora utmaningar när det gäller samverkan kring sanktionerna.

För att verksamhetsutövare ska förstå sin riskexponering och kunna tillämpa sanktionerna på ett ändamålsenligt sätt, behöver de både stöd från myndigheter och ha möjlighet till dialog sinsemellan.

Internationella sanktioner kan dessutom samverka med komplicerade strukturer av handels- och exportrestriktioner i allt högre grad, vilket kräver information och analys.

Bedömningen är att en ökad konfliktbild och allt större geopolitiska spänningar i olika delar av världen medför alltmer omfattande och komplexa sanktioner. För att tillämpningen av sanktionerna ska vara effektiv och syftet med sanktionerna ska uppnås samt att överträdelser av sanktionerna ska kunna bekämpas krävs utökad samverkan och dialog mellan aktörerna på sanktionsområdet.

Bank- och värdetransportrån och angrepp mot uttagsautomater

Sedan 2020 har det inte inträffat något bankrån i Sverige. En sådan lång period utan denna typ av angrepp har inte tidigare noterats under den 45 år långa mätperioden. Förklaringen till den varaktiga nedgången är att kontanthanteringskedjan från depå via värdetransportbolag till uttagsautomat har stärkts, att banker har minskat den manuella kontanthanteringen över disk och att kunder använder alltmer elektroniska betalningar.

Under 2024 inträffade heller inga värdetransportrån. De tio senaste åren har inneburit en markant minskning av antal värdetransportrån jämfört med decenniet innan. Förklaringen till minskningen är effektivare skyddssystem, sedelinfärgning, färre transporter samt bättre samverkan och förebyggande åtgärder mellan värdetransportbolagen och Polisen.

Inga angrepp mot Bankomat AB:s uttagsautomater inträffade heller under 2024. Statistiken omfattar sprängda och uppsågade uttagsautomater, däremot inte skimming av kort.

Bedömningen är att hotbilden avseende bank- och värdetransportrån består men att antalet rån kommer fortsätta att ligga på en låg nivå 2025, liksom antalet angrepp mot uttagsautomater.

Det senaste bankrånet i Sverige inträffade 2020.

Mer kontanthantering i samhället ökar riskerna för personalen och penningtvättsriskerna eftersom spårbarheten är låg.

Utmaningarna med kontanter

Sverige återfinns bland de länder som har allra lägst efterfrågan och faktisk användning av kontantbetalningar. En väl utbyggd kortinfrastruktur och digitala betallösningar, som exempelvis Swish, har en extremt hög nyttjandegrad. Kontantanvändandet i Sverige bedöms fortsätta som det har gjort de senaste åren, det vill säga en minskning på cirka 10 procent årligen.

Det förs i allt större utsträckning diskussioner om en ökad kontantanvändning i samhället. Reglering (främst lagstiftningen om kontanter i betaltjänstlagen), Riksbankens ansvar (exempelvis föreskriftsrätten inom beredskap för betalningar i RBFS 2023:3) samt olika utredningar (Betalningsutredningen och Kontantutredningen, Fi2024/00068) har ambitionen att säkerställa kontanternas fortlevnad för olika syften.

Kontanter som beredskapslösning

Eftersom kontanter används i så liten omfattning i normalläget är det inte en realistisk lösning att kontanter kan ha en avgörande betydelse vid kris eller krigshändelse. Kontantutbud och kontantinfrastruktur kommer helt enkelt inte att kunna skalas upp för att snabbt ersätta stora digitala betalningsvolymer. De slutsatserna har dragits av utredningar i såväl Danmark som Norge, samt av erfarenheterna från Ukraina.

Fokus för kontinuitets- och beredskapslösningar behöver därför ligga på ökad motståndskraft i de betalsystem som faktiskt används och i grundläggande infrastruktur som elförsörjning och telekommunikation.

Säkerheten för personalen

Kontantintensiv verksamhet skapar risker för de som arbetar med kontanter. För bankerna är säkerheten för personalen den viktigaste aspekten av kontantfrågan. Senaste bankrånet i Sverige skedde 2020, och antalet värdetransportrån har också minskat markant det senaste decenniet. Kontantutredningen undervärderar de säkerhetsrisker som kontanter medför. Om kontantanvändandet ökar hos vissa handlare kommer både rånrisken och risken för internbedrägerier att öka.

Kontanter skapar penningtvättsrisker

Kontantintensiv verksamhet är också förknippad med hög risk för penningtvätt. Spårbarheten för kontanter är låg eller obefintlig, vilket är en avgörande nackdel i de flesta typer av brottsbekämpning. Kontanter är därför fortfarande ett attraktivt betalningsmedel i den illegala ekonomin. Stora delar av handeln med narkotika och illegala tjänster betalas med kontanter. Trots att kontantanvändningen överlag minskar i hela EU så ökar behovet av sedlar, vilket visar att kontanter fortfarande är ett viktigt verktyg som värdebevarare.

Bankerna har generellt sett bra kontroll över de direkta insättningar och uttag som sker till banken, men så fort placeringsfasen ligger utanför banken, till exempel genom kontantköp hos handlare, grossister, spelbolag, och restauranger, har banken svårare att förstå var insättningarna kommer ifrån.

När kontanter växlas in i länder med stor kontantanvändning och dåliga kontroller och sedan förs över till ett svenskt bankkonto är det mycket svårt för banken att kunna göra nödvändiga kontroller. Vid misstankar om penningtvätt kan bankerna behöva vidta åtgärder såsom att vägra ta emot kontanter från vissa utländska valutaväxlare.

Svårigheten består i att det i princip är omöjligt att spåra transaktionsflöden bakåt och påvisa misstänkta transaktioner och transaktionsflöden. Med olika typer av legala skyldigheter att acceptera kontanter kommer alltså risken för penningtvätt att öka, och möjligheten att hitta kriminella aktörer kommer att minska.

Bedömningen är att en ökad kontanthantering ökar riskerna för personalen och ökar risken för penningtvätt.

Svenska
Bankföreningen
Finance Sweden

Telefon: 08-453 44 00
E-post: info@financesweden.se
www.financesweden.se

Formgivning och grafisk produktion: www.luxlucid.com Stockholm, maj 2025