Hotbildsbedömning för Sveriges banker

Publicerad maj 2024

Svenska Bankföreningen
Swedish Bankers' Association

Hotbildsbedömning för Sveriges banker

Publicerad maj 2024

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 och säkerhetsskydd bidrar till rapporten.

Sedan flera år har det säkerhetspolitiska läget försämrats. Rysslands markinvasion av Ukraina i februari 2022 har ritat om hotbilden. Bankerna påverkas av invasionen inom flertalet områden i sitt säkerhetsarbete och har satt ett ökat fokus på civilt försvar och beredskapsfrågor.

Hotbildsbedömningen är uppdelad i nio olika områden enligt innehållet nedan.

Sammanfattning

Under 2023 inträffade inga **bank- och värdetransportrån** men det skedde fem angrepp mot Bankomat AB:s uttagsautomater.

Inom området **kränkning, personhot och våld mot bankpersonal** rapporterar bankerna om ökad spänning och tuffare bemötande från kunder de senaste åren. Många medarbetare är rädda för att representera banken i rättsliga sammanhang. Exponering av enskilda medarbetare kan öka hotbilden mot individen snarare än 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.

Informations- och cybersäkerhetsområdet har under året präglats av hot från kriminella och statsstödda aktörer, särskilt efter Rysslands angrepp mot Ukraina. Antalet finansiella företag som drabbas av ransomware-attacker har ökat, dock från låga nivåer. Överbelastnings-attackerna mot bankerna har fortsatt, men med begränsad effekt. Sabotage mot gasledningar och telekommunikationskablar i närområdet har förtydligat hotbilden mot kritisk infrastruktur. Ett växande hot är hotaktörers snabba utnyttjande av tekniska sårbarheter, liksom att AI används i bedrägliga syften mot både kunder och bankpersonal.

Enligt Polisen är nästan hälften av **bedrägeribrotten** kopplade till organiserad brottslighet och gängkriminalitet. Konsumenter och företag har under året blivit än mer utsatta för bedrägerier, med än större konsekvenser, vilket även påverkar bankerna. Social manipulering har gjort brottsligheten mer riktad och personlig. Bankkunder och företag utsätts för en mängd bedrägeri-metoder och under 2023 har vishing-, smishing-, investerings-, romans- och kreditbedrägerier ökat. Antalet målvakter som möjliggör bedrägerierna fortsätter att vara ett problem.

Penningtvättshoten kvarstår och har sin bakgrund i bland annat bedrägerier, narkotikahandel och skattebrott. Företag används allt oftare som verktyg för ekonomisk brottslighet, där målvakter figurerar för att dölja de verkliga verksamhetsutövarna. Andra riskområden för penningtvätt är utnyttjande av välfärdsystemet, valutaväxling, kontanthantering, kryptovalutor, fastighetsmarknaden, lyxkonsumtion och spelsektorn.

De senaste åren har antalet fall av misstänkt **finansiering av terrorism** via kryptovalutor ökat. En riskfaktor är att bankerna ofta saknar tillgång till information om hur sådan finansiering går till samt vilka som är inblandade.

I och med de tilltagande geopolitiska spänningarna har **internationella sanktioner** blivit ett allt viktigare utrikes- och säkerhetspolitiskt påtryckningsmedel. Samtidigt har sanktionerna blivit allt svårare att överblicka och tillämpa för verksamhetsutövarna. Här krävs utökad information, samverkan och dialog mellan aktörerna på sanktionsområdet.

Bankrån, värdetransportrån och angrepp mot uttagsautomater

Inga bankrån inträffade under 2021, 2022 och 2023. Sådant nollresultat har inte tidigare noterats under 40 års mätningar. Förklaringen till minskningen och det bibehållna nollresultatet 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.

2023 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 och bättre samverkan och förebyggande åtgärder mellan värdetransportbolagen och Polisen.

Angrepp mot Bankomat AB:s uttagsautomater inträffade fem gånger 2023. Det omfattar sprängda eller uppsågade uttagsautomater, däremot inte skimming av kort.

Bedömningen är att hotbilden mot bank- och värdetransportrån består men att antalet fortsatt kommer att ligga på en låg nivå 2024, liksom antalet angrepp mot uttagsautomater.

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 enkätundersökningar från Finansförbundet visar att medarbetare utsätts för hot och våld. Bilden varierar: vissa banker anser att hot och kränkningar är på ungefär samma nivå som tidigare, medan andra banker noterat en kraftig utveckling det senaste året. Det är svårt att förklara förändringen, det kan vara ett resultat av vidtagna förebyggande åtgärder, ökad anmälningsbenägenhet eller en konstaterad ökning. För de banker med stor kontorsrörelse är ungefär hälften av antal kränkningar och hot kopplade till fysiska kontor medan andra hälften riktas mot telefonbanken.

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 avvisas från kontoret eller där kundrelationen avvecklats av olika skäl.

Verktyg för att hantera hotfulla kunder

Bankerna avvecklar fler kunder i dag. Anledningen är att fler kunder uttrycker hot mot bankens personal och att banken upptäcker fler oegentligheter. 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 hålla beredskap.

Banken håller utbildningar i konflikthantering med diskussionsmaterial för alla medarbetare som arbetar på kontor och telefonbank. Medarbetarna kan hamna i tuffa situationer med ekonomiskt pressade kunder, och bankerna arbetar därför 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, ett onödigt uttryck, en höjd röst, en upprörd kund eller en obehaglig situation? 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.

Olika delar av banken är olika utsatt för hot

En hotbild kan vara faktisk eller upplevd. Svårigheten att bedöma och kommunicera ut en faktisk hotbild beror på att det är vanskligt att avläsa hoten utifrån faktiska händelser, men oron bedöms ändå ha ökat. Bor man på en mindre ort och möter kunder fysiskt i vardagen utanför arbetet är situationen annorlunda jämfört med en medarbetare i telefonbanken.

Medvetenheten om den faktiska hotbilden bedöms vara större på bankkontor än på huvudkontor, eftersom personal på bankkontoren möter kunder fysiskt. Men det kan också vara det omvända för banker som har en telefonbank och ett huvudkontor, vilket då gör huvudkontoret mer utsatt. Det har till stor del att göra med vilka kontaktvägar som finns för missnöjda kunder. 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.

Beroende på hur hotbilden utvecklas kan utökade fysiska skyddsåtgärder behöva införas.

Allt fler myndighetsförfrågningar

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

För att bemöta hotbilden arbetar bankerna med att skydda medarbetares identiteter. E-post skickas i större utsträckning från centrala funktionsbrevlådor, exempelvis sakerhetsavdelningen@banken.se eller kundkontakt@banken.se. Vidare begränsas bedrägeriutredares externa kundkommunikation. Bankerna har alternativa alias som kan användas beroende på känslighet, exempelvis vid avveckling av kund, och det finns tankar om att införa system för alias samt rutiner för det. Det är väldigt lätt att hitta en person som har ett unikt namn i Sverige och frågan är om en banktjänsteman behöver skylta med sitt namn.

Ökade insatser mot brottslighet i form av fler kontroller, bättre medvetenhet och uppföljning kan skapa frustration hos kunderna.

Medarbetare vill inte representera banken i rättsliga sammanhang. Det finns en rädsla för att bli hotad och förföljd. 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. Banken kan inte göra en sådan anmälan, utan det måste göras av den medarbetare som drabbats av hotet. En anmälan blir en offentlig handling med medarbetaren som målsägande. Banken kan säkerställa att det finns stöd vid en eventuell rättegång, men många medarbetare upplever ändå stor otrygghet i dessa situationer.

Ökade insatser mot brottslighet i form av flera kontroller, bättre medvetenhet och uppföljning kan skapa frustration hos kunderna. 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.

Med anledning av Säkerhetspolisens höjning av terrorhotnivån från 3 till 4 i augusti 2023 har bankerna uppmanat sina medarbetare till ökad vaksamhet och påpekat vikten av att följa myndigheternas råd. Även om bankerna i sig troligen inte är en direkt måltavla, har bankerna gjort en analys av de kontor/platser i stora städer som ligger i anslutning till potentiella mål. Det har medfört en översyn av kontinuitetsplaner och alternativa resvägar för nyckelpersonal. Vissa aktiviteter har påskyndats med anledning av den förändrade terrorhotnivån, med utgångspunkt från bankernas befintliga säkerhets- och kontinuitetsarbete.

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 individer blockerar in- och utgångar vilket riskerar att försvåra en eventuell evakuering. Därmed utsätts personal och kunder för fara.

BEHOV AV ÅTGÄRDER

Med anledning av utvecklingen ser Bankföreningen behov av följande åtgärd och initiativ 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 vilket ökar risken för hot. Det borde därför vara möjligt för banken att göra en polisanmälan om en medarbetare av någon anledning inte vill göra det. Anmälaren blir på så sätt neutraliserad, eftersom det är organisationens ställningstagande och inte den enskilde medarbetarens. Banken kan då välja vilka personer som ska företräda banken.
- Banker bör som egen juridisk person också ges möjlighet att polisanmäla målvakter till polisen.

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

Hotbilden från insiders och möjliggörare

I förhållande till problematiken kring möjliggörare av brott är insiders en faktor som kontinuerligt gör sig påmind och som kräver vaksamhet och adekvata åtgärder.

Incitamenten att plantera en insider / möjliggörare på en bank bedöms i allmänhet vara starka eftersom det ger större möjlighet till dels bedrägerier och penningtvättsupplägg för kriminella, dels påverkan för en antagonist. En insider / möjliggörare kan vara en person med behörigheter i banken som möjliggör för en extern antagonist (kriminell gruppering, främmande makt, etc) att genomföra transaktioner och aktiviteter.

En insider kan alltså antingen vara en aktiv möjliggörare, aktivt dela information eller ha en mer rådgivande, coachande roll. En insider är ofta en yngre person med koppling till högrisländer genom anhöriga, semester eller ursprung. Personen presterar bra och könsfördelningen bland möjliggörare är jämn. Personen har ofta konton i annan bank, har andra inkomster än lön samt eget mobilabonnemang.

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 negativa kontakter exempelvis med erbjudande om att genomföra betalda intervjuer på Linkedin, bedöms ha ökat det senaste året. Kriminella och andra fientliga aktörer annonserar exempelvis också efter personer som är beredda att injicera skadlig kod i bankens system. Social manipulering smälter på så sätt ihop med den fysiska hotbilden genom otillbörliga kontakter som senare kan leda till fysiska hot mot anställda. Det kan även förekomma att en person med anknytning till en extern antagonist söker anställning i bank i syfte att möjliggöra brott.

Att bygga säkerhet tar tid

En fråga som aktualiseras är hur banken kan skydda medarbetare från otillbörliga kontakter från exempelvis en statsaktör eller organiserad brottslighet. Inom säkerhetsskyddslagstiftningen, som i regel 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. Idag behöver bankerna i mångt och mycket förlita sig till den information som den arbetssökande själv lämnar.

En insider / möjliggörare kan vara en banktjänsteman som tar emot betalning från kriminella för att säkerställa att de kriminellas transaktioner och aktiviteter kan genomföras utan problem. Det kan också var en banktjänsteman som är utsatt för ett hot. Sårbarheter kan också finnas genom släktskap vilket gör att befattningsutövandet, som grundar sig i lämplighet, kan antas påverkas negativt.

Att förebygga, förhindra och upptäcka intern brottslighet är en viktig del av bankens säkerhetsarbete.

Vissa tillvägagångssätt kräver en möjliggörare på insidan

Vissa tillvägagångssätt kan inte genomföras utan en möjliggörare på insidan som har kunskap om bankens produkter, tjänster och rutiner. Möjliggöraren bistår den kriminella med sekretessbelagd information som underlättar genomförandet av brottsupplägget. Det kan handla om information om rutiner och processer, regelsättning vid kreditgivning och regler för transaktionsmonitorering. Vid sidan av bankens egen kreditberedningsprocess skapar låneförmedlare, med fler parter i låneked-jan, olika typer av incitament till bedrägerier och penningtvättsupplägg för en insider / möjliggörare vid återbetalning.

Risken för att insiders används är något som bankerna kan behöva bli mer vaksamma på. Bankerna kan också 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

Ett problem i förhållande till upptäckt och adekvata åtgärder är att bankerna 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 beror på att det inom förundersökningar ofta finns tillgång till bland annat tömningar av mobiltelefoner/datorer och hemliga tvångsmedel. Det är av vikt att denna information (som kan vara så kallad överskottsinformation inom förundersökningen), så snart det finns legala förutsättningar, kommer till bankernas kännedom. Utan denna information blir det väsentligt svårare för bankerna att vidta adekvata åtgärder.

Även om Säkerhetspolisen i februari 2024 har pekat ut en hotbild 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.

Bankernas egna kontrollmöjligheter

Att förebygga, förhindra och upptäcka intern brottslighet är en viktig del av bankens säkerhetsarbete. Bankernas interna kontrollmöjligheter är omfattande och består av in- och utpasseringsloggar, uppföljning av slagningar på kunder, behörigheter, dokumentationskrav med mera. För att kunna minska verksamhetens eller individers sårbarheter och skydda, såväl verksamhet som anställda, mot risken att bli utnyttjad av kriminella aktörer, behöver säkerhetsavdelningarna vara involverade i internutredningsprocessen även i de fall det rör misskötsamhet och regelöverträdelser.

Bedömningen är att insiders / möjliggörare är ett hot från organiserad brottslighet som finns internt i bankerna och som kommer att bestå under 2024. Givet en ökad internationell konfliktbild och politiska spänningar i förhållande till svenska intressen under senare år, har vissa statsaktörer ett förhöjt intresse av insiders / möjliggörare.

Den säkerhetspolitiska utvecklingen och beredskapen

Sedan Rysslands olagliga annektering av ukrainska Krim 2014 har Sveriges säkerhetspolitiska läge successivt försämrats. Svensk säkerhetspolitik har vilat på en regelverksbaserad ordning som har sitt ursprung i folkrätten, regler och avtal. I och med Rysslands invasion av Ukraina i februari 2022 har den europeiska säkerhetsordningen upphört som ett gemensamt system.

Gråzonen

Hotbilden från främmande makt karaktäriseras idag till stor del av så kallad gråzonsproblematik med en krigföring som kan beskrivas som kontaktlös, det vill säga via fjärrstridsmedel och global spaning. Gråzon är ett konceptuellt begrepp där vare sig ”krig” eller ”fred” råder. Gråzonsaktiviteter är ett samlingsnamn för antagonistiska påverkansaktiviteter exempelvis att manipulera information, projicera makt på olika sätt, avsiktligt kränka ett lands luftrum, cyberattacker och så vidare. Syftet med gråzonsaktiviteter mot Sverige är att försöka påverka svenskt beslutsfattande och minska vår handlingsfrihet. Det kan handla om att skada tilliten, undergräva våra värderingar, splittra oss och försvaga vår motståndskraft eller att störa samhällsviktiga funktioner som bankverksamhet.

Svenska banker utgör idag en stor del av de baltiska ländernas finansiella infrastruktur vilket också påverkar hotbilden. Risken för antagonistiska gråzonsaktiviteter med syfte att påverka banker och finansiell infrastruktur bedöms därför ha ökat. Bankerna är vana vid att skydda verksamheten mot olika hot och att planera och öva för att kunna hantera och återta verksamheten vid störningar och incidenter. Rysslands invasion av Ukraina visar hur snabbt det kan gå och att utvecklingen utanför Sverige kräver ett långsiktigt beredskapsarbete i Sverige.

Sektorns beredskapsarbete

Bankerna deltar aktivt i redan existerande samverkansstrukturer såsom Finansiella Sektorns Privat-Offentliga Samverkan (FSPOS), men även i de beredskapshöjande aktiviteter som har startats av Finansinspektionen och Riksbanken.

I Sverige har även ett nationellt cybersäkerhetscenter skapats med syfte att stärka Sveriges förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot, och främja ett utökat informationsutbyte mellan privata och offentliga aktörer. Den finansiella sektorn har sedan 2022 ett samarbete med centret. Syftet är att stärka cybersäkerheten inom finanssektorn och tillsammans öka Sveriges motståndskraft mot cyberhot. Bankerna har ett behov av att ta del av underrättelser och information om den säkerhetspolitiska hotbilden mot Sverige och den svenska finansiella sektorn.

Bedömningen är att Sveriges säkerhetspolitiska läge och den försämrade hotbilden påverkar bankerna.

BEHOV AV ÅTGÄRDER

Med anledning av utvecklingen ser Bankföreningen behov av följande åtgärder och initiativ från politik och myndigheter.

- Styrningen och ledningen av beredskapsarbetet i sektorn behöver förbättras. Sektorns myndigheter behöver tillsammans med företagen ta fram en tydlig gemensam målbild för den finansiella sektorns beredskapsarbete. Målbilden ska förankras och kunna förstås av samtliga myndigheter och företag inom sektorn så att alla utgår från samma antaganden i det fortsatta arbetet.
- Den identifiering av samhällsviktig verksamhet inom sektorn som gjordes 2023 under ledning av Finansinspektionen behöver konkluderas och tydligt kommuniceras till sektorns alla aktörer, inte endast till dem som ingått i arbetet. Planen för 2024 behöver också tydligt kommuniceras ut. Det finns idag många företag i sektorn som är osäkra på vilket beredskapsarbete som egentligen pågår. Tydliga sektorsövergripande prioriteringar behöver därför slås fast och kommuniceras. Fokusområden som bedöms som särskilt viktiga för att öka den samlade förmågan och effekten i sektorn bör prioriteras.

Informationssäkerhets- och cybersäkerhetshot

Hotbilden inom informations- och cybersäkerhetsområdet har under 2023 fortsatt att drivas av hotet från kriminella grupper och statsstödda aktörer, inte minst på grund av Rysslands anfallskrig mot Ukraina. Den digitala krigsföringen och andra typer av hybridhot är en del av det nya normala för bankerna. Cyberattacker slår brett och opportunistiskt mot företag och organisationer och ofta finns ingen direkt måltavla. De som drabbas hårdast är de som inte arbetat långsiktig och strukturerat i sitt cybersäkerhetsarbete.

Ökning av ransomware-attacker mot svenska verksamheter

Under 2023 och inledningen av 2024 har ransomware-attacker, d v s utpressningsprogram som krypterar sina offers data tills en lösensumma är betald, drabbat ett stort antal verksamheter och därmed fått stor publik uppmärksamhet. Bland de drabbade är Svenska kyrkan, it-bolaget TietoEvry och svenska kommuner. Attacken mot TietoEvry drabbade ett stort antal kunder till bolaget och exemplifierar vad som kan inträffa när koncentrationer av kritiska tjänster byggs upp hos enskilda leverantörer. Svenska banker behöver ha en god förståelse över vilka koncentrationsrisker de är utsatta för om de har lagt ut delar av sin it-verksamhet.

Inom bankområdet märks ransomware-attacken mot den kinesiska storbanken ICBC och deras amerikanska filial i november 2023. Attacken påverkade marknaden för statsobligationer i USA, och ICBC behövde tillföra verksamheten 9 miljarder dollar för att kunna hantera oreglerade affärer. Andra exempel på ransomware-attacker mot finansiell sektor är attacken mot ION som påverkade derivathandeln i februari 2023 och attacken mot Equilend i januari 2024 som påverkade värdepappershandeln. Flera europeiska banker råkade tillsammans med andra företag ut för informationsförluster i samband med de sårbarheter som uppmärksammandes i mjukvaran MoveIT i juni 2023.

Det har alltså varit en viss ökning av fall där finansiella företag drabbas av ransomware-attacker. Ökningen sker dock från låga nivåer och bedömningen är fortfarande att banker har högre säkerhet och en mer utvecklad förståelse för cybersäkerhetsrisker och hot än andra typer av företag och myndigheter. Bankerna har arbetat med frågorna under många år, då hotbilden har förflyttats från den fysiska till den digitala världen. En annan förklaring kan vara att en framgångsrik ransomware-attack som låser bankens system också försvårar kriminellas möjligheter att utpressa banken på pengar.

Trenden fortsätter att kriminella inte behöver utveckla sitt eget ransomware utan kan köpa en färdig lösning, ”ransomware as a service”, och sedan använda denna för att attackera sina mål. Dessutom krypteras inte bara data utan kriminella stjäl också data i samband med ransomware-attacken och hotar med att lägga ut informationen publikt på internet om inte lösensumman betalas. Denna typ av organiserad brottslighet utvecklar sig mot att efterlikna legitima företag. Bland de aktörer som använder ransomware kan det vara svårt att skilja mellan statsstödda aktörer och kriminella grupper. Det är också troligt att kriminella grupper ibland agerar på staters uppdrag.

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, hantera och återställa verksamheten. Omfattande ransomwareattacker 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.

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. I 2023 års hotbildsbedömning beskrevs 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 under perioden. Det har inte heller rapporterats om att ryska hotaktörer genomfört destruktiva cyberattacker mot västerländska banker och finansiella företag. Trots detta finns det all anledning för bankerna att fortsatt bevaka området.

Överbelastningsattacker

Under perioden har svenska banker fortsatt blivit utsatta för överbelastningsattacker i syfte att påverka internettjänsters tillgänglighet. Aktörer med anknytning till främmande makt och kriminella organisationer har genomfört överbelastningsattacker mot verksamheter och företag i Nato-länder och dess allierade, vilket innefattar Sverige och bankerna. Attackerna har ofta haft en mycket begränsad effekt. Syftet med attackerna bedöms vara informationspåverkan mot samhället och medborgarna genom att försöka visa att samhällsviktiga finansiella tjänster är i fara. Bedömningen är fortsatt att bankernas skydd fungerat väl, och attackerna har inte fått någon större påverkan på de digitala kanalerna.

Sabotage mot infrastruktur

I 2023 års hotbildsbedömning noterades sabotaget mot gasledningarna Nord Stream 1 och 2 i september 2022, vilket visade på hoten mot kritisk infrastruktur på grund av säkerhetsläget i närområdet. Under rapportperioden har hoten ytterligare konkretiserats genom det misstänkta sabotaget mot gasledningen Balticconnector mellan Finland och Estland, och en telekommunikationskabel mellan Sverige och Estland. Dessutom har det i media rapporterats om att främmande makt kartlägger kritisk infrastruktur i Östersjöområdet. De svenska bankerna behöver ha ett fortsatt fokus på att se över sina beroenden till kritisk infrastruktur. De måste planera för att eventuellt ytterligare öka sina resurser och sin kapacitet, exempelvis elektronisk kommunikation och elförsörjning. Det är också i linje med det totalförsvars- och beredskapsarbete som nu intensifieras både i finansiell sektor och nationellt.

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

Risker i it-leverantörsledet

Bankerna använder it-leverantörer, molntjänster och allmänt tillgänglig mjukvara i sin verksamhet. Risker med det innefattar skadlig kod som kan spridas genom etablerade leverantörsled, men också 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 ett antal sådana sårbarheter uppmärksammats globalt. Några av de uppmärksammade fallen har förekommit i mjukvara så som MOVEit, VMware och Citrix NetScaler. Zero-days drabbar också mjukvara som bankernas it-funktioner använder i sin supportverksamhet.

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-days. Sammantaget ökar det trycket mot bankernas it-funktioner vilket i sin tur medför ett behov av att tillföra resurser för att hantera riskerna.

Artificiell intelligens och deep fakes

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 än svårare att genomskåda. Användningen av deep fakes för bedrägliga syften är ett växande hot i samhället.

Inom bankverksamhet skulle deep fakes exempelvis kunna användas som ett verktyg för social manipulation genom att imitera personer i ledande position gentemot exempelvis bankpersonal inom betalningsområdet. Målet skulle kunna vara att genomföra bedrägliga betalningar.

Detta hotområde är sannolikt bara i sin linda och kommer att utvecklas de kommande åren. Bankerna behöver utveckla sina förmågor för att kunna hantera hotet. Det kan exempelvis handla om utbildning av personalen och om att använda teknik för att upptäcka deep fakes.

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”, det vill säga nätfiske som riktar sig mot utvalda personer hos bankerna förekommer. 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 etablera fotfäste i bankernas infrastruktur. Samtidigt är det fortfarande vanligt förekommande med phishing som inte riktar sig mot utvalda personer hos bankerna utan som är av mer opportunistisk karaktär. Phishing mot it-leverantörers personal som ett sätt att potentiellt sätt attackera bankerna förekommer också.

Bedömningen är att skadlig kod via phishing fortsätter vara en hög risk för bankerna. Övningar och utbildning för att personalen ska kunna upptäcka phishing-mejl samt tekniska lösningar för att blockera phishing-mejl är fortsatt viktiga motåtgärder.

Förekomsten av banktrojaner har ökat något under året men bedömningen är att svenska banker och bankkunder inte har drabbats i någon större omfattning. Banktrojaner som infekterar mobiltelefoner och mobilbankslösningar syftar ofta till att stjäla kundernas inloggningsuppgifter. Banktrojaner utvecklade för Android-telefoner är fortfarande vanligare än för iOS-telefoner. Bankkunderna har fått sina mobiltelefoner infekterade genom att ladda ner appar som innehållit skadlig kod.

BEHOV AV ÅTGÄRDER

Med ett försämrat säkerhetspolitiskt läge och ökat cyberhot ser Bankföreningen behov av ett antal samordnade åtgärder och initiativ från politik, myndigheter, näringsliv och andra delar av samhället:

- Utbytet och användningen av information mellan myndigheter och näringsliv behöver vidareutvecklas. Bankerna behöver fler och snabbare underrättelser om potentiella cyberhot och sårbarheter. Samtidigt är bankerna beredda att bidra med sina förmågor på området. Bankföreningen ser mycket positivt på att samarbetet med Nationellt cybersäkerhetscenter och Finansforum har permanentats. Det är dock tydligt att myndigheternas samarbete har försvårats på grund av avsaknaden av en tydlig huvudman för centret. Bankföreningen ser därför positivt på den utredning som under våren 2024 ska lägga förslag på FRA, Försvarets radioanstalt, som huvudman för centret.

- Bankföreningen ser betydande utmaningar för bankerna när regleringar, såväl inom EU som nationellt, kommer att gälla överlappande för samma områden inom säkerhet, beredskap och motståndskraft. Fokus i bankernas arbete riktas då mot administration och uttolkning av terminologi och definitioner, kartläggning och rangordning av olika regelverk, snarare än mot praktisk verksamhet för att stärka motståndskraften. Det är viktigt att liknande aktiviteter inte ska omfattas av flera olika regelverk.

Bedömningen är att hotbilden inom informations- och cybersäkerhetsområdet blir allt mer sofistikerad och att den påverkas av kriminella grupper och statsstödda hotaktörer. Den it-brottsrelaterade hotbilden blir mer komplex och samverkande. Under perioden märks ökningen av antalet ransomware-attacker och sårbarheter som zero-days. 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.

2023 anmäldes 235 665 bedrägeribrott i Sverige, enligt Polisen, vilket är en ökning med 42 274 brott, eller 22 procent, jämfört med 2022.

Brottsvinsterna från bedrägerier ökar

Innan det senaste årets ökning av antal polisanmälda bedrägeribrott hade antalet polisanmälda bedrägeribrott minskat med cirka 25 procent under fyra år. Förklaringen till minskningen är framför allt genomförandet av PSD2 (det andra betaltjänstdirektivet). Kravet på stark kundautentisering i PSD2:s tekniska standard som trädde i kraft den 1 januari 2021 resulterade i en markant minskning av antal kortbedrägerier, mestadels så kallad Card Not Present, när det fysiska kortet inte är närvarande vid transaktionen. Ökningen av antal polisanmälda bedrägeribrott det senaste året består i en bred ökning av flera modus, samtidigt som vissa brottstyper minskar, enligt Polisen.

Även om antal polisanmälda bedrägerier minskade med 25 procent 2018–2022 så ökar bedrägerivinsterna över tiden, enligt Polisen (rapporten De dödliga bedrägerierna, sid. 11, Dnr: A554.314/2022). Ökningen av bedrägerivinster kan till stor del förklaras av att bedrägerier med inslag av social manipulering, exempelvis telefonbedrägerier, har ökat markant. Brottsvinster för bedrägerier uppskattades vara cirka 4,2 miljarder kronor år 2020, cirka 4,6 miljarder kronor år 2021, cirka 5,8 miljarder kronor år 2022 och cirka 7,5 miljarder kronor år 2023 enligt Polisen (rapporten Brottsvinsterna för bedrägeribrottsligheten 2022, sid. 2, Dnr: A232.846/2023 och rapporten Brottsvinsterna för bedrägeribrottsligheten 2023, sid. 2, Dnr: A233.272/2024).

År 2019 var antal polisanmälda vishingbedrägerier 5 285. År 2023 hade antalet stigit till 29 347, en ökning med 555 procent. Samtidigt har antalet större utredningar mot de brottskluster som misstänks stå för en stor del av dessa vishingbedrägerier minskat från tio utredningar 2019 till en (1) utredning 2022, enligt Polisen (det saknas uppgifter om antal större utredningar för 2023).

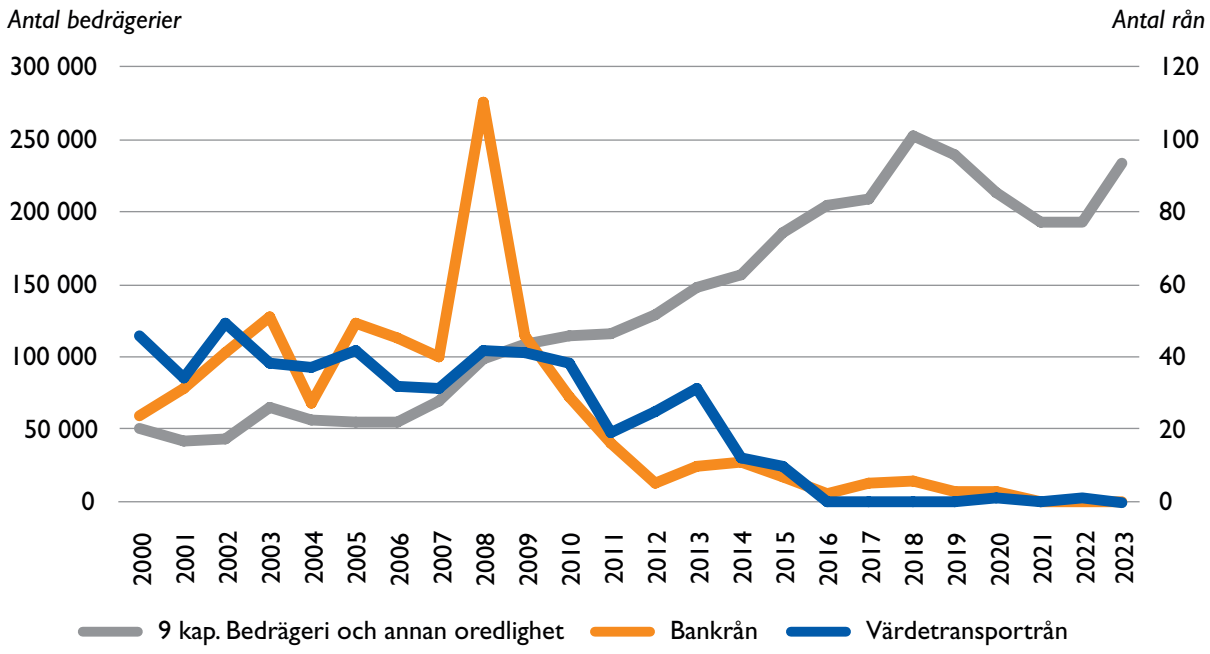
Organiserad brottslighet med stort våldskapital påverkar idag bankerna genom att agera som en ”fullsortiments-brottsorganisation” med påverkan på områdena fysisk säkerhet, bedrägeri och penningtvätt där de olika delarna går i varandra. Enligt Polisen kan närmare hälften av bedrägeribrotten kopplas till organiserad brottslighet och gängkriminalitet. Medlen används för investeringar i både kriminella miljöer och i den lagliga ekonomin.

Nya produkter och tredjepartsleverantörer

En av huvudutmaningarna är att tjänsteutveckling och digitalisering går väldigt fort, vilket innebär att även hotbilden förändras snabbt. Snabbheten kräver i sin tur ett realtidsskydd avseende informationsdelning. Det uppstår ett behov av att dela tekniska uppgifter som cookies, IP-adresser, information om sårbarheter och riktade attacker. Bankerna tar ned falska hemsidor på löpande band, vilket kräver ytterligare kompetens och resurshantering.

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.

Antal bedrägerier och antal bank- och värdetransportrån (2000–2023).



Källa: Bankföreningen och BRÅ.

Utvecklingen påverkas också av politiska incitament, exempelvis PSD2, som ger banken sämre möjligheter att hinna vidta relevanta motåtgärder.

Med PSD2 och tjänsteleveranser som bygger på tredjeparters access till konton och data, hos banker kallat ”open banking”, har flera aktörer tillkommit i betalningskedjan vilket medför nya risker och utmaningar. För konsumenter kan det vara svårt att förstå vad man ger sitt samtycke till och vilken aktör som får tillgång till kunduppgifter. Det saknas idag tydlig kravställning mot tredje parter. Alla 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.

Lagstiftningen påverkar området

Just nu finns ett lagförslag från EU om att gå från ”open banking” till ”open finance”, vilket kan öppna bankernas infrastruktur för ännu 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 inom en rad finansiella tjänster inom EU med kundernas samtycke, alltså inte bara för betalningar utan även för bolån, lån, sparande, pensioner och försäkringar. Det politiska målet är att förbättra och skräddarsy finansiella produkter och tjänster för kunder samt skapa ökad konkurrens inom finanssektorn.

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 på samtliga aktörer inom ”open finance”.

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. Här föreslås obligatorisk återbetalning från banken för bedrägerier där bedragaren utger sig för att vara en bankanställd. En förskjutning av ansvarsfördelningen till banken att ersätta mer bedrägeri kan leda till en ökning av ”friendly fraud” där kunden påstår sig vara utsatt för bedrägerier. Ett ytterligare problem blir om bevisbördan ligger på banken, där all teknisk och annan data pekar på att transaktionen är behörig.

Med garanterad återbetalning vid bedrägeri, kan betaltjänstanvändare komma att ta mindre hänsyn till säkerheten. Minskad uppmärksamhet på onlinerisker skulle kunna spilla över på användning av alla typer av digitala tjänster och göra betaltjänstanvändare mer utsatta för cyberrisker. Det tar även bort incitamentet för andra intressenter (telekom

och sociala medier / onlineplattformar) att samarbeta med banker, eftersom den fullständiga ekonomiska bördan då bärs av bankerna. För att effektivt ta itu med problemet bör fokus i stället ligga på förebyggande åtgärder.

Ytterligare förslag från EU är att betalningar ska gå allt snabbare. Under 2024 träder nya regler ikraft för betalningar i euro. De innebär krav på betaltjänstleverantörer att erbjuda sina kunder omedelbara betalningar i samma kanaler där de erbjuds vanliga kontoöverföringar i euro. Med kanaler avses framför allt internetbank, mobilbank och telefonbank. Det är en oroväckande utveckling, eftersom omedelbara betalningar 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 dessa utmaningar och begränsa risken för en ökning av antalet bedrägerier behöver bankerna införa nya system och nya arbetsmetoder för att upptäcka och stoppa bedrägerier, samtidigt som kundernas medvetandegrad om riskerna med omedelbara betalningar måste höjas.

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 olika former av bedrägeriförsök. 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 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.

De största bedrägerihoten

Svenska konsumenter och företag är idag utsatta för bedrägeriförsök på många olika sätt. Allt ifrån phishing av inloggningsuppgifter (till exempel e-legitimation och säkerhetsdosa) till spridning av skadlig kod via e-post, sms och hemsidor. Konsumenter och företag utsätts också för romans-, investerings-, vishing-, smishing, kredit- och BEC-bedrägerier (Business E-mail Compromise, till exempel vd-bedrägerier) samt id-kapningar och annons- och sociala medier-bedrägerier.

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.

De största bedrägerihoten 2023 har varit vishing-, smishing-, investerings-, romans- och kreditbedrägerier. 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 idag ofta att utföra transaktionerna själva, exempelvis under förevändning att pengar behöver föras över till ett ”säkert konto”.
- **Smishing-bedrägeri (falska sms):** Bedragaren skickar ett sms till en konsument med information som ska få kunden att göra något. Bedragarens avsikt är att skapa en stressad situation där kunden måste agera snabbt. Antingen ska kunden ringa ett telefonnummer, installera programvara eller följa en länk och lämna ut information. Vanliga upplägg är sms 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.
- **Kreditbedrägeri:** Bedragaren ansöker om ett lån på falska grunder. Exempel 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.

Social manipulering ökar

Den gemensamma nämnaren för bedrägeriupplägen är försöket och 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. Konsumenter och företag har blivit mer utsatta för bedrägeribrottslighet, samtidigt som konsekvenserna för offren har blivit större, vilket även påverkar bankerna.

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.

Trenden att bedragare försöker förmå kunder att genomföra autentiserade transaktioner, genom telefon, e-post eller sms, har det senaste året förstärkts. Bedrägerierna drabbar alla målgrupper och aktuella omvärldshändelser används ofta som bete.

En annan trend är en ökning av kunder som blir återutsatta för bedrägerier. En av anledningarna till detta är att uppgifter om dessa kunder sprids mellan olika kriminella organisationer eller helt enkelt återanvänds. Det vanligast förekommande återvinningsbedrägeriet är att brottsoffer vilseleds att de kan få tillbaka pengar från ett tidigare investeringsbedrägeri, men bankerna noterar även en ökning av återutsatta kunder som blivit lurade genom telefonbedrägerier.

En växande utmaning är att utsatta kunder av olika skäl inte utför de bedrägliga transaktionerna direkt till den avsedda slutmottagaren, utan antingen självmant eller efter anmodan, skickar pengarna via andra kunder och/eller institutioner i ett eller flera led. 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 lägger ned mycket tid och resurser på att prata med sina utsatta kunder.

En annan trend det senaste året är att företagare och användare med tillgång till flera engagemang, som revisorer, har blivit mer utsatta. Bedragarnas tillvägagångssätt blir allt svårare att genomskåda för den som utsätts. Exempelvis används ny teknik i syfte att invagga offret i falsk trygghet. Brottsbytet är ofta flera hundra tusen kronor eller mer. Bedrägerierna kan i värsta fall rycka undan mattan för företagens verksamhet och medföra konkurs. I bakgrunden ligger det faktum att företagare inte åtnjuter samma grundskydd mot ekonomisk förlust till följd av brott som konsumenter.

Kunder luras också att installera fjärrstyrningsprogramvara på sin telefon eller dator, vilket ger bedragaren full access och kontroll över skärm och tangentbord. Bedragaren kan därmed lägga upp transaktioner i kundens bank som kunden sedan luras att signera. För att motverka detta arbetar bankerna med analyser av beteendemönster för hur kunder använder datorer och appar.

För kortbedrägerier är utvecklingen liknande, det vill säga att allt fler bedrägerier sker där transaktionerna rent tekniskt godkänts av betalaren. Ett exempel där kunder utsätts för social manipulering är vid anslutning av digitala plånböcker. Tillvägagångssättet är att kunder luras att dela information om koder för autentisering och signering till bedragare som i stället ansluter ett kort till en digital enhet under bedragarens kontroll. Bedragaren utger sig via e-post och sms ofta att vara från bank, myndighet, polis eller fraktföretag, och hänvisar kunderna till ett gränssnitt där uppgifterna ska fyllas i av kunden.

Artificiell Intelligens (AI)

Bedragarna använder sig redan av ett automatiserat och robotiserat arbetssätt, och bankerna behöver följa utvecklingen av bedragarnas användande av AI . Bankerna ser att automatiserade konversationer förekommer i vissa bedrägeriupplägg via sociala medier och chat-appar.

Bankerna förväntar sig dels ökad kvalitet på språk och design, dels 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.

Alla banker informerar sina kunder om hur bankens tjänster 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 (se avsnittet ”Behov av åtgärder” längre ned).

Bedragare blir allt skickligare på att kartlägga sina tilltänkta offer.

Bättre datadelning ger bättre riskbedömningar

Att kunder idag utför många bankärenden själva medför att det blir allt viktigare för banken att kunna tolka kundernas beteende och upptäcka ett avvikande beteende. Bankerna arbetar systematiskt med preventiva metoder, som limiter och begränsningar i produkter, samt aktiv monitorering utifrån kundernas beteende för att hantera de risker som finns.

Om lagstiftningen skulle tillåta mer datadelning mellan aktörer i samhället, av exempelvis målvaktsregister och IP-adresser, skulle det bidra till en bättre monitorering genom bättre riskbedömningar i både det preventiva arbetet och i bankernas monitorering. Ju mer information och datapunkter bankerna kan dela sinsemellan desto större preventiv effekt.

När bankerna inte hanterar det tekniska gränssnittet genom app eller hemsida får bankerna mindre data till sin bedrägeriövervakning. Transaktioner till uppsamlingskonton är svårare att övervaka jämfört med betalningar och överföringar. Om banken inte kan se mottagarkonton försvåras bankens penningtvätts- och bedrägeriövervakning.

Utvecklingen inom realtidsbetalningar innebär delvis samma och delvis nya risker. Realtidsbetalningar kräver förmåga att både anpassa limiter och blockera transaktioner samt att balansera smidighet, säkerhet och tröghet. Eftersom monitorering endast kan eliminera en liten del krävs också precisa preventionsverktyg.

Att kunder idag utför många bankärenden själva medför också att det blir allt viktigare för kunden att kunna hantera de digitala verktygen. Banken måste utbilda och informera kunden om hur produkter och tjänster fungerar.

Hembesöken fortsätter

Antal hembesök av bedragare som påstår sig vara banktjänstemän, poliser eller hemtjänstpersonal fortsätter vara ett problem. Bedragarens förevändning är ofta att ”hjälpa till” med något påstått problem, medan syftet med hembesöket är att stjäla värdesaker eller komma åt kundens bankkort, säkerhetsdosa eller e-legitimation.

Risken för att antalet hembesök och personrisker ökar när banken täpper till möjligheten till andra tillvägagångssätt är en realitet som behöver beaktas i arbetet med att motverka bedrägerier.

Fler människor med svagare tekniska kunskaper exponerades för högre risk under covid-pandemin, eftersom de då i större utsträckning var tvungna att använda digitala verktyg. Det har inte nödvändigtvis med ålder att göra, utan också bristen på sociala sammankomster där man kan prata om dessa frågor vilket resulterar i att okunskapen blir större. Även om hembesök ökar är det ett mindre antal.

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. Genom information från söktjänster 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 ”spoofade” telefonnummer, det vill säga maskerade nummer där bedragaren

själv väljer vilket telefonnummer som ska uppvisas i displayen, för att försöka framstå som att det verkligen är banken som kontaktar sina kunder.

Kunderna är sällan insatta i hur det tekniska fungerar, inklusive vad fjärrstyrningsprogram är. 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.

En trend i kölvattnet av teknikutvecklingen är ”crime as a service” där information delas och säljs mellan kriminella aktörer. Brottsupplägg, skadlig kod, länkar, webbsidor och kunduppgifter säljs vidare i flera led och bedragaren behöver inte besitta gedigen teknisk kompetens för att kunna använda brottsverktygen. Därutöver föreligger ökade risker för bedrägerier som föregås av intrång hos extern part där kundens uppgifter manipuleras. Om en bank baserar sin riskbedömning på den externa partens data blir den felaktig.

Kreditbedrägerier

Kreditbedrägerier är sedan lång tid en mycket vanligt förekommande företeelse, som numera underlättas av snabba digitala förfaranden för låneansökning, ofta inom ramen för de framväxande snabb- och blancolånemarknaderna. Att knyta samman förståelsen för de olika upplägen av kreditbedrägerier – i alla delar av kreditens förlopp, från ansökan till återbetalning – är utmanande.

Antalet falska arbetsgivarintyg, lönespecifikationer, manipulerade kontoutdrag och andra åtgärder som syftar till att påverka utfallet av en kunds kreditansökan, fortsätter att ligga på en hög nivå.

När det gäller företagskrediter handlar det ofta om att ta många parallella olikartade krediter under den tid ett företag kan användas som brottsverktyg, det vill säga under den tid som felaktiga uppgifter om kreditvärdighet uppges i de kontroller som genomförs av kreditgivare. Det är fråga om att ta regelrätta företagslån, andra snabbare företagskrediter, 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 och 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. Bedragaren drar nytta av att de olika kreditgivarna inte kan utbyta information, det vill säga före den tidpunkt uppgifter börjar synas i kreditupplysningarna. Det kan gälla såväl regelrätta lån som kreditköp.

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.

Betalning, avbetalning och lösen av krediter är ytterligare ett riskområde. All betalning av krediter bör kontrolleras mot uppgifterna avseende kundkännedom. När det handlar om kundens betalning av krediten finns risk för att banken tar emot medel från penningtvättsupplägg om medlens ursprung är tvivelaktigt, och då hamnar banken i en svår situation för hur kundförhållandet ska hanteras. Dessutom riskerar ärendena att snabbt bli komplexa.

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 exempelvis 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.

Eftersom kreditbedrägerier baseras på en eller flera falska uppgifter har några banker börjat använda externa tjänster för att kontrollera kunders inkomstuppgifter. Idag registreras även falska uppgifter om inkomst hos svenska myndigheter, vilket försvårar möjligheten för bankerna att förlita sig på och bedöma tillförlitligheten i 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 intressenter öka utbildningsinsatser och därmed höja kunskapsnivån avseende kreditbedrägerier.

Målvakter möjliggör bedrägerier

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

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 bara man tar emot och skickar vidare 250 000 kronor. Det kan senare leda till hotfulla situationer när den unga vill dra sig ur.

Antalet penningmålvakter som är verksamma i Sverige är stort. Totalt har drygt 80 000 personer registrerats som skäligen misstänkta för bedrägeribrott under perioden 2018–2021, enligt Polisens rapport De dödliga bedrägerierna, men mörkertalet är sannolikt ännu större. Det står helt klart att det krävs ett fungerande flöde av information mellan bankerna och Polisen för att höja effektiviteten i brottsbekämpningen.

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

Antalet penningmålvakter som är verksamma i Sverige är stort.

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.

Tillvägagångssätten förändras

Tillvägagångssätten anpassas hela tiden efter förutsättningarna. Under 2023 skedde en ökning av kortbedrägerier och förklaringen är att bedragare hittar sätt att komma runt stark kundautentisering genom kortinlösare utanför EU. Andra återkommande problem är abonnemangsfällor, påhittade erbjudanden på annonssidor på Facebook och Instagram, ej erhållna varor och att det finns många falska hemsidor. Under de första månaderna 2024 verkar det som att antal kortbedrägerier stabiliseras.

Den förstärkta utfärdandeprocessen av Mobilt BankID (genom en online-kontroll mot Polisens id-handlingar pass och nationellt id-kort) har resulterat i att antal obehöriga transaktioner har minskat väsentligt under 2023.

Bedömningen är att riskerna för bedrägerier och finansiella brott är fortsatt hög och ökande, och att hotbilden blir alltmer komplex och samverkande genom kombinerande tillvägagångssätt i samma brottsupplägg.

BEHOV AV ÅTGÄRDER

För att bryta utvecklingen ser Bankföreningen behov av ett antal åtgärder och initiativ från politik och myndigheter (utöver de åtgärder bankerna kan vidta själva).

- Lagstiftaren bör begränsa publicering av personuppgifter på internet. Det är i dagsläget exempelvis allt för enkelt att kartlägga ensamstående äldre med god ekonomi.
- Teleoperatörer verksamma i Sverige bör åläggas att försvåra / omöjliggöra maskering av telefonnummer genom en anti-spoofinginfrastruktur för telefon och sms, liknande det som redan finns för telefon i Finland samt de förslag som planeras för sms.
- Förslagen i ID-kortsutredningen (SOU 2019:14), att minska antalet utfärdare av fysiska id-kort och att förbättra bankers möjlighet att kontrollera id-handlingar, bör genomföras. Den fysiska id-handlingen knyter ihop det fysiska med det digitala i två riktningar: först när banken utfärdar BankID och därefter som extra kontrollmöjlighet när e-legitimationen används med utgångspunkt från bankens riskmonitorering.
- Bankerna bör också få utbyta information med varandra på ett enklare sätt. Ett flöde av information mellan bankerna och Polisen krävs för en förebyggande effekt, till exempel en målvaktsförteckning där uppgifter från bland annat Polisens penningtvättsregister bör ingå. Syftet är att minska målvakters manöverutrymme.
- Polismyndigheten bör tillhandahålla ett API mot RES-systemet för bankerna att använda i sin identitetskontroll på bankkontor och i sin roll som utfärdare av e-legitimation (BankID).
- Polisen bör tillhandahålla information om risker och brottsmodus som de känner till och som de vill att bankerna ska använda sig av i sin transaktionsmonitorering.
- Polismyndigheten bör utveckla möjligheterna för brottutsatta att polisanmäla brott digitalt. Dagens begränsade möjligheter att polisanmäla brott riskerar att skapa ett mörkertal angående brottslighetens omfattning, då många brottsutsatta är hänvisade till att ringa 114 14 där väntetiderna kan vara långa.
- Polisen behöver säkerställa en högre uppklarningsnivå av bedrägerier. Antal uppklarade bedrägerier har sjunkit de senaste tio åren och var 2023 cirka 2,5 procent. Idag arbetar cirka 1 procent av polisens resurser med bedrägerier trots att bedrägeribrott utgör mer än 16 procent av all brottslighet. Analytiska polisresurser behöver därför prioriteras för denna volymbrottslighet.
- Regeringen bör utveckla och implementera en nationell strategi mot bedrägerier. Strategin bör innefatta olika sektorer som bank, telekom, internet-teknologi, polisresurser och system, ny lagstiftning och reglering med mera. Exempelvis bör Finansinspektionen aggregerat publicera den statistik om bedrägerier som bankerna med flera inrapporterar.

Ett brottsutbyte som inte kan omsättas saknar i princip värde.

Penningtvätt

Penningtvätt omfattar i praktiken en rad olika så kallade penningtvättsåtgärder. Det kan röra sig om pengatransaktioner mellan olika bankkonton men även andra åtgärder som till exempel att använda falska handlingar som representerar ett värde. Det är inte ovanligt att komplicerade brottsupplägg föregår penningtvätt. 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 och uppdaterad övervakning av kontotransaktioner är därför det viktigaste verktyget 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 kryptovalutor, spelmarknaden, ”hawala-banking” (ett alternativt betalningssystem för främst internationell penningöverföring utanför banksektorn) och handel med varor och tjänster. Statistiken är sannolikt förknippad med viss osäkerhet, bland annat till följd av mörkertalet när det gäller mer komplicerade brottsliga tillvägagångssätt inom till exempel handelssektorn.

Under 2023 gjordes 56 136 misstankerapporter till Finanspolisen, FIPO, vilket var 24 procent fler än 2022 (45 113) och drygt dubbelt så många som 2020, enligt FIPO:s statistik. Bankerna står för en överväldigande majoritet av antalet rapporter. Totalt svarade den finansiella sektorn för 90 procent av rapporterna 2023 medan spelsektorn stod för 9 procent.

De största penningtvättshoten

Eftersom penningtvätt är ett brett begrepp som samlar all omsättning av brottsutbyte styrs penningtvättsproblematiken i mångt och mycket av vilken brottslighet som vid en viss tidpunkt drabbar samhället. Vissa typer av brott generar traditionellt ett omfattande brottsutbyte. Ett brottsutbyte som inte kan omsättas saknar i princip värde.

Kriminella uppvisar ofta stor uppfinningsrikedom och kreativitet när det gäller att hitta nya sätt att tvätta pengar. Det kan handla om att investera brottsutbytet där omsättningsintresset är stort och kontrollerna inte är tillräckliga. Det finns även oreglerade områden såsom till exempel kryptovalutor, där kontroll av penningtvätt i princip inte kan utövas. Vidare förekommer det att det internationella betalningssystemet utnyttjas 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. Eftersom bankerna enbart kan se en viss del av en transaktionskedja och har begränsade möjligheter att utbyta information sinsemellan är denna typ av penningtvätt svår för bankerna att upptäcka.

De kontinuerliga penningtvättshoten kvarstår – det är fråga om tvätt av brottsutbyte från bland annat bedrägerier, narkotikabrott och skattebrott. Som framgått kan det ske på ett många olika sätt och det

är en utmaning att överblicka utvecklingen. De beloppsmässigt största penningtvättshoten står den organiserade brottsligheten för. Den organiserade brottsligheten har andra förutsättningar att med avancerade upplägg och på ett mer systematiskt sätt tvätta pengar jämfört med personer som tvättar mindre belopp någon enstaka gång.

Den nationella antipenningtvättsregimen innehåller brister, vilket medför att staten i vissa fall agerar som möjliggörare för kriminellas verksamhet och penningtvätt. Många regler är utformade efter förhållanden som inte längre är relevanta medan existerande företeelser inte omfattas av befintliga regelverk.

Inte heller myndigheter är tillräckligt anpassade till hotbilden från den organiserade brottsligheten, vilket visar sig till exempel i dåliga eller obefintliga kontroller, något som möjliggör välfärdsbrottslighet.

Penningtvätt med hjälp av företag

Det har under senare år blivit allt vanligare att företag används som brottsverktyg inom ramen för den organiserade ekonomiska brottsligheten. Nya företag registreras eller befintliga företag förvärvas. Ofta placeras en målvakt i företagets styrelse. Målvakten saknar i många fall helt kännedom om företagets verksamhet. I stället styrs företaget av andra personer som inte vill figurera offentligt och därmed riskera att hållas ansvariga för de ekonomiska brott som begås med hjälp av företaget. Verksamheten i företaget kan vara helt eller delvis brottslig. Om brottsligheten endast utgör en andel av en annars legitim verksamhet är den särskilt svår att upptäcka för såväl banker som brottsbekämpande myndigheter.

För att ett utåt sett legitimt företag ska kunna drivas krävs att en rad olika initiala åtgärder vidtas. Exempelvis behöver företagets företrädare och verksamhet registreras hos Bolagsverket. Det är också i allmänhet en förutsättning att företagskonto öppnas i en svensk bank och att bokföringskonsult anlitas, i vart fall om den brottsliga verksamheten ska ha viss varaktighet. Penningtvätt över företagskonto kan i ett sådant fall vara svår att upptäcka.

Välfärdsbrottsligheten

Så fort nya bidrag eller stöd inrättas drar det till sig intresse från kriminella – något som tydligt visat sig vid utbetalningarna av ekonomiska stöd under covidpandemin, elstöd samt olika ekonomiska stöd relaterade till miljöbefrämjande åtgärder.

Kriminellas utnyttjande av välfärdssamhället, sammantaget mycket stora summor, 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 göras av i första hand den beslutande eller utbetalande myndigheten. Från och med 2024 har en ny myndighet, Utbetalningsmyndigheten, inrättats. Utbetalningsmyndigheten ska kontrollera utbetalningar från välfärdssystemen och kan därmed förväntas bidra till en minskad penningtvätt som föregåtts av välfärdbrottslighet.

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.

Det finns risk för att fastighetsmäklare till följd av omsättningsintresset underlåter eller gör alltför summariska penningtvättsrelaterade kontroller. Generellt sett finns ett intresse av att fastighetsaffärer genomförs snabbt, vilket i många fall hamnar i konflikt med kontrollintresset. 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 (det icke-indexerade internet) samt vid ransomwareattacker. På flera handelsplatser för kryptovalutor är det möjligt att betala med bankkort, vilket medför en koppling mellan det traditionella finansiella systemet och kryptomarknaden.

En penningtvättsrisk som har ökat i omfattning är förknippad med att betalning i kryptovaluta blivit ett allt vanligare betalningsmedel såväl i detaljhandeln som mellan enskilda personer. I och med ett ökat fokus på kryptovalutor ökar också riskmedvetenheten i förhållande till att ta emot sådan som betalningsmedel.

Särskilda högriskgrupper är de som tillhandahåller tjänster avseende kryptovalutor, inkluderande betalningsförmedlare och valutaväxlare. Dessa aktörer omfattas idag inte av samma omfattande regelverk som gäller för banker, och vissa aktörer är ännu helt oreglerade. De har i många fall dåliga 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 aktuell risk som är svår att överblicka 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.

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

Samtidigt som omsättning av kryptotillgångar är sårbar för penningtvätt ger den även större möjligheter till analys än vad som gäller för exempelvis omsättning av kontanter. Detta då mycket data om transaktioner av kryptotillgångar är 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 kommer EU:s nya förordning om marknader för kryptotillgångar (MiCA-förordningen) att träda i kraft. MiCA syftar bland annat till att underlätta rättssäkerheten för företag och att locka fler investeringar till EU-länder. EU blir nu den stora jurisdiktionen i världen som inför omfattande regler för kryptomarknaden. Vilken effekt MiCA i praktiken kommer att få i förhållande till EU:s och den globala kryptomarkanden 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.

Kontanter

Kontantintensiv verksamhet är förknippad med hög risk. Kontanter är fortfarande ett attraktivt betalningsmedel i den illegala ekonomin eftersom spårbarheten är mycket dålig. Stora delar av handeln med narkotika och illegala tjänster betalas med kontanter. Trots att kontantanvändningen generellt 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 vidta åtgärder.

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 återtagande av kontanter från vissa utländska valutaväxlare.

Kontanter är fortfarande ett attraktivt betalningsmedel i den illegala ekonomin.

Lyxvaror

Marknaden för varor och tjänster i lyxsegmentet såsom bilar, smycken, klockor, guld, märkeskläder, resor och hotell har vuxit över tid. Den attraherar kriminella, både som verktyg för att omsätta eller 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 vanligt upplägg 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 detta vis kommer kontanter med brottslig bakgrund in i det finansiella systemet.

Spel och dobbel

Spelsektorn uppvisar en hög risk för penningtvätt. Spelkonton 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. Inom spelsektorn hanteras även kontanter i relativt stor omfattning, vilket som framgått ovan är förenat med särskilt stora penningtvättsrisker.

Spelföretag kan vara både online-baserade och traditionella kasinon på fysiska adresser. Online-baserade företag är ofta belägna i lågskatteländer. Även om marknaden är reglerad och omfattas av penningtvättsregelverket finns åtskilliga olicensierade företag.

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 att begränsa sina risker, i huvudsak genom goda rutiner för att uppnå kundkännedom och en ändamålsenlig transaktionsövervakning.

BEHOV AV ÅTGÄRDER

Med anledning av utvecklingen inom penningtvättsområdet ser Bankföreningen behov av ett antal åtgärder och initiativ 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.
- Den organiserade brottsligheten utnyttjar det faktum att bankerna inte kan dela information sinsemellan. När de kriminella upptäcks i en bank byter de omedelbart till en annan bank och fortsätter sina brottsliga aktiviteter där. För att åtgärderna mot penningtvätt och finansiering av terrorism ska kunna bli effektiva behöver bankerna därför få bättre möjligheter att dela information om misstänkta kunder, transaktioner och aktiviteter med varandra.
- 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.
- Banker måste kunna förlita sig 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 de utnyttjas av den organiserade brottsligheten. Det gäller till exempel Bolagsverkets register över företrädare och verklig huvudman till juridiska personer, men även andra register som verket för.
- Åtgärder behöver genomföras för att begränsa förekomsten av möjliggörare. Det kan till exempel handla om att Bolagsverket skärper sina kontroller, att företagsförmedlare får svårare att överlåta företag till kriminella eller att kriminella inte ges tillgång till bokföringstjänster.
- Finanspolisen behöver tillräckliga resurser för att snabbt hantera och återkoppla avseende alla misstankerapporter som lämnas av de aktörer som omfattas av penningtvättsregelverket. Om frysningsbeslut inte fattas skyndsamt finns en risk att brottsliga pengar förs utom bankers och myndigheters kontroll.

Kryptovalutor är attraktiva för finansiering av terrorism.

Finansiering av terrorism

En viktig riskfaktor i fråga om finansiering av terrorism är att bankerna saknar tillgång till tillräcklig information om hur sådan finansiering går till samt vilka personer och företag som är inblandande. Bristande information om vad bankerna ska reagera på och leta efter medför svårigheter att upptäcka misstänkt terrorfinansiering.

De senaste åren har antalet fall av misstänkt finansiering av terrorism via kryptovalutor ökat. Sådana valutor är attraktiva för finansiering av terrorism, bland annat på grund av frånvaron av en enhetlig och universell reglering och tillsyn av kryptobranschen.

Vissa mer omfattande och komplicerade brottsupplägg, bland annat internationell skattebrottslighet (till exempel momskaruseller, vilka under senare år har drabbat Sverige i stor omfattning), kräver omfattande organisation och stora initiala investeringar. Inte sällan är det fråga om tio- eller hundratals miljoner kronor. Brottsliga investeringar i denna omfattning kan komma från internationella kriminella nätverk som i sin tur kan misstänkas ha kopplingar till terrorism och finansiering av sådan. 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.

Ytterligare en riskfaktor i förhållande till finansiering av terrorism är så kallad crowdfunding. Det är en investeringsform där en stor grupp individer med små summor finansierar en verksamhet eller ett projekt. Plattformar för crowdfunding möjliggör för privatpersoner att på internationell nivå starta olika typer av insamlingar på internet. För banken är det mycket svårt att skilja legitima insamlingar från sådana som sker med bakomliggande intentioner att finansiera terrorism. Av naturliga skäl framgår inte detta syfte utåt.

Bedömningen är att en ökad informationsdelning innefattande kunskaper om tillvägagångssätt för finansiering av terrorism kan minska bankernas risker för medverkan 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 ökad 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. Sanktioner riktas mot regeringar eller statsapparater, en identifierad grupp/organisation, fysiska individer eller företag. Detta kan i sin tur leda till att sanktionerna skapar förändringar på politisk eller statlig nivå. Sanktioner kan vara ett alternativ eller förstadium till mer ingripande åtgärder, det vill säga om sanktionerna inte får önskad effekt.

Sanktioner utfärdas av en rad olika länder. 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.

Sanktioner kan riktas mot

- regeringar i länder utanför EU
- enheter (företag) som tillhandahåller medel för den politik som sanktionerna är riktade mot
- grupper eller organisationer, till exempel terroristgrupper
- enskilda personer som stöder den politik som sanktionerna är riktade mot eller är involverade i terroristverksamhet

Sanktioner omfattar ibland inte bara listade enheter, utan även enheter med anknytning till de listade enheterna. Det kan innebära att ägarstrukturer och informella strukturer för kontroll av en sanktionerad enhet behöver analyseras för att sanktionerna ska efterlevas. Vidare kan sanktioner ta sikte på en viss typ av vara eller tjänst som i och för sig är legitim men som den sanktionerade kan använda i oönskade syften för att stärka sin förmåga eller ekonomi.

Sanktioner har blivit ett allt viktigare utrikespolitiskt påtryckningsmedel.

Utvecklingen inom sanktionsområdet och Rysslandssanktionerna

Sanktionerna har under senare år blivit allt svårare att överblicka och tillämpa på ett enhetligt och effektivt sätt för de många verksamhetsutövare som måste efterkomma sanktionerna. Det är inte bara bankerna som behöver förhålla sig till sanktionerna. I stort sett hela industrisektorn behöver ständigt vara uppmärksam för att inte riskera att bryta mot sanktioner.

Sedan Rysslands 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 Rysslands förmåga och markera att landets beteende är oacceptabelt. Sanktionerna omfattar bland annat reseförbud, frysningar av betydande ryska tillgångar och ett oljepristak för rysk oljeexport. Vid utgången av 2023 hade EU beslutat om sammanlagt tolv sanktionspaket mot Ryssland. Under 2024 förväntas ytterligare utökningar av rysslandssanktionerna.

Samtidigt kan man konstatera ett ökat storskaligt och systematiskt undandragande och kringgående av sanktionerna från rysk sida. 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, m.m. 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 2024.

Samverkan inom sanktionsområdet

Storskaliga och systematiska sanktionsöverträdelser ställer ökade krav på såväl verksamhetsutövare som myndigheter inom EU. Medvetenhet om och förståelse för problemet är grundläggande. Alltmer omfattande sanktioner och en alltmer komplex och riskabel kontext medför stora utmaningar när det gäller samverkan inom sanktionsområdet. Utan stöd från relevanta myndigheter och dialog mellan aktörerna på sanktionsområdet, är det till exempel svårt för verksamhetsutövare att förstå sin riskexponering och få nödvändig information för att kunna tillämpa sanktionerna på ett ändamålsenligt och effektivt sätt, så att de politiska syftena ska kunna uppnås.

Bedömningen är att en ökad konfliktbild och allt större geopolitiska spänningar i olika delar av världen medför alltmer omfattande och komplexa sanktioner. Detta ställer ökade krav på banker och andra verksamhetsutövare. För att tillämpningen ska vara effektiv och överträdelser av sanktionerna bekämpas behövs utökad samverkan mellan aktörerna på sanktionsområdet.

Formgivning och grafisk produktion: www.luxlucid.com Stockholm, maj 2024

Svenska
Bankföreningen
Swedish Bankers' Association

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