Rapport 2016:9

Bedrägeribrottsligheten i Sverige

Kartläggning och åtgärdsförslag

brå

Bedrägeribrottsligheten i Sverige

Kartläggning och åtgärdsförslag

Rapport 2016:9

Brå – kunskapscentrum för rättsväsendet

Myndigheten Brå verkar för att brottsligheten minskar och tryggheten ökar i samhället. Det gör vi genom att ta fram fakta och sprida kunskap om brottslighet, brottsbekämpning och brottsförebyggande arbete, till i första hand regeringen och myndigheter inom rättsväsendet.

ISSN 1100-6676
ISBN 978-91-87335-65-5
URN:NBN:SE:BRA-651

Produktion: Ordförrådet AB
Författare: David Shannon, Klara Hradilova Selin, Johanna Skinnari och Linda Hörnqvist
Omslag: Maimi Laks
Tryck: Lenanders Grafiska AB

Brottsförebyggande rådet, Box 1386, 111 93 Stockholm
Telefon 08–527 58 400, e-post info@bra.se, www.bra.se

Denna rapport kan beställas hos bokhandeln eller hos Wolters Kluwer, 106 47 Stockholm
Telefon 08–598 191 90, fax 08–598 191 91, e-post kundservice@wolterskluwer.se

Förord

Brottsförebyggande rådet fick 2014 i uppdrag av regeringen att genomföra en studie om bedrägerier och arbetet mot sådan brottslighet. Bakgrunden är att både anmälningar till polisen och frågeundersökningar till befolkningen talar för att bedrägerierna ökar. Mot bakgrund av detta krävs enligt regeringen ny kunskap för att stärka arbetet mot bedrägerier. Studien baseras på ett stort och varierat empiriskt material: Nationella trygghetsundersökningen (NTU) och den officiella kriminalstatistiken; granskning av polisärenden (urval av anmälningar och förundersökningar); tingsrättsdomar samt intervjuer med berörda aktörer och gärningspersoner. En referensgrupp har varit knuten till arbetet och träffats vid ett par tillfällen.

Rapporten ringar in ett antal utvecklingsområden som är angelägna när det gäller att motverka bedrägeribrottslighet samt bidragsbrott. En rad förslag på åtgärder för att förebygga dessa brott, stoppa de brott som redan pågår och förbättra utredningsarbetet gällande brott som redan ägt rum ges också.

Rapporten har författats av David Shannon, Klara Hradilova Selin, Johanna Skinnari och Linda Hörnqvist, samtliga verksamma vid Brå. Alexandra Skarp, Mikael Altemark och Peter Zvejnieks vid Brå har deltagit i arbetet med kodning respektive transkribering.

Rapporten har vetenskapligt granskats av professor Per Ole Träskman, Lunds universitet och professor Sven-Åke Lindgren, Göteborgs universitet. En rad andra sakområdesexperter har också granskat olika delar av rapporten.

Brå vill rikta ett varmt tack till de personer som intervjuats och de representanter för myndigheter och näringsliv som bidragit med sina kunskaper och erfarenheter. Brå vill slutligen särskilt tacka polisens Nationella bedrägericenter (NBC) som varit en viktig samarbetspartner genom hela arbetet.

Stockholm i mars 2016

Erik Wennerström
Generaldirektör

Annika Eriksson
Enhetschef

Innehåll

Sammanfattning[1]

Brås uppdrag och metod

Brå fick 2014 i uppdrag av regeringen att genomföra en studie av bedrägerier och arbetet mot sådan brottslighet. Bakgrunden är att både anmälningar till polisen och frågeundersökningar till befolkningen talar för att bedrägerierna ökar. En viktig anledning är att den tekniska utvecklingen gjort det möjligt att begå dels nya former av bedrägeribrott, dels mer storskaliga bedrägeribrott. Mot bakgrund av detta krävs enligt regeringen ny kunskap för att stärka arbetet mot bedrägerier. Det gäller hur brottsligheten ser ut, hur rättsväsendet arbetar och vilka förebyggande åtgärder som kan ha effekt.

Något förenklat innebär ett bedrägeri enligt brottsbalkens 9 kap. att gärningspersonen vilseleder en utsatt till att göra en förmögenhetsöverföring. En särskild typ av bedrägeri är bidragsbrotten, som behandlas i en egen lag (bidragsbrottslagen 2007:612).

För att genomföra uppdraget har Brå analyserat fyra huvudmaterial:

- Nationella trygghetsundersökningen (NTU) och den offentliga kriminalstatistiken för perioden 2008–2014/2015.[2]
- Granskning av polisärenden (urval av anmälningar och förundersökningar).
- Tingsrättsdomar.
- Intervjuer med berörda aktörer från rättsväsendet, övriga myndigheter och näringslivet samt gärningspersoner.

Bedrägeribrotten ökar enligt flera källor

Under åren sedan 2008 har det skett en ökning i bedrägeribrottsligheten, både i termer av självrapporterad utsatthet (enligt NTU)

[1] En engelsk version av denna sammanfattning finns på Brås webbplats, www.bra.se. Klicka där på fliken Publikationer, och skriv sedan in rapportnumret i sökfältet.

[2] Statistik avseende antalet polisanmälda bedrägeribrott redovisas även för 2015. I skrivande stund är dock denna statistik fortfarande preliminär.

och i antalet ärenden som hanteras av rättsväsendet. År 2015 anmäldes drygt 173 000 brottsbalksbedrägerier till polisen. Enligt både NTU och kriminalstatistiken observeras stora ökningar av bedrägerier med hjälp av internet respektive kortbedrägerier. NTU, som fångar utsattheten bland privatpersoner, visar att det framför allt är kvinnor som i ökande grad uppger att de blivit utsatta för någon typ av bedrägeri. I den senaste mätningen som avser händelser under år 2014, var andelen utsatta ungefär lika stor bland kvinnor som bland män (cirka 3 procent).

Utvecklingen har varit mer stabil för antalet anmälda bidragsbrott, där drygt 9 300 brott anmäldes till polisen år 2015. Det innebär i stort sett lika många anmälningar som år 2008. En väsentlig skillnad från brottsbalksbedrägerierna är att antalet bidragsbrott som anmäls helt beror på hur stora resurser de utbetalande myndigheterna och organisationerna lägger på kontroll och vad de väljer att polisanmäla.

Fem huvudtyper av anmälda brottsbalksbedrägerier

Utifrån ett urval av polisens utredningsakter från 2013 har fem huvudkategorier av bedrägerier enligt brottsbalken identifierats. Sammantaget kan cirka tre fjärdedelar av samtliga granskade brottsbalksbedrägerier sägas tillhöra en form av köp- eller säljprocess. *Kortbedrägerier* är den enskilt största kategorin (22 procent av urvalet). Vid kortbedrägerier använder gärningspersonen någon annans – vanligtvis stulna eller skimmade – kontokort, alternativt elektroniska kortuppgifter, för att olovligen genomföra köp eller uttag.

Den näst största kategorin (17 procent) är *kreditbedrägerier*, som innebär att gärningspersonen köper en vara eller en tjänst, alternativt tar ett lån, i någon annans namn. I de flesta fall förutsätter dessa brott identitetsmissbruk, och vid mer storskaliga brottsupplägg används kreditvärdiga bolag.

En tredje, ungefär lika stor kategori utgörs av *annonsbedrägerier*. Vid dessa brott vilseleder gärningspersonen en intresserad köpare genom att på en annonssida på internet erbjuda en önskad vara eller tjänst till försäljning eller uthyrning. Efter att betalning ägt rum uteblir dock leveransen.

Ytterligare en typ av brottsbalksbedrägerier är *fakturabedrägerier* (12 procent), då målsägaren vilseleds att betala en faktura för en vara eller en tjänst som denne inte har beställt. Det kan röra sig om rena bluffakturor, alternativt fakturautskick som föregåtts av någon form av kontakt (exempelvis telefonförsäljning), där fakturamottagaren t.ex. blivit vilseledd att ingå ett avtal med avsändaren.

Den femte kategorin kallas här *övriga telefon- och internetbedrägerier*. Dessa omfattar flera olika typer av upplägg där gärningspersoner använder skadlig kod eller kontaktar den utsatte via telefon eller internet. Upplägggen tillhör inte någon av de tidigare beskrivna kategorierna av bedrägeribrott men kan ibland utgöra ett försteg. Exempelvis innebär nätfiske ofta ett försök att komma åt den utsattes kort- eller kontouppgifter. Många av dessa anmälningar avser inte fullbordade bedrägerier, men däremot försöks- eller förberedelsebrott.

Det typiska upplägget vid bidragsbrott är att gärningspersonen, genom att ha lämnat felaktig information, har vilselett den utsatte – som i detta fall är en myndighet eller organisation – att betala ut bidrag eller förmåner som denne inte var berättigad till. En variant är att personen inte underrättat den utbetalande myndigheten eller organisationen om ändrade förhållanden, och därigenom fått en för hög utbetalning. Den största utbetalande myndigheten, Försäkringskassan, är också den som anmäler flest brott. Därpå följer kommunerna och arbetslöshetskassorna. Bidragsbrotten omfattar enbart bidrag och förmåner till enskilda, men det finns också en del brottsbalksbedrägerier som drabbar de utbetalande aktörerna. Det handlar då om stöd till företagare, som framför allt betalas ut av Arbetsförmedlingen, men även vissa typer av bedrägerier mot Försäkringskassan.

Internet centralt i många bedrägeribrott

Brås studie visar att internet som brottsforum eller som en form av möjliggörare förekommer inom alla typer av bedrägerier. Vid annonsbedrägerierna är internet en självklar förutsättning för brottsligheten. I kredit- och kortbedrägerierna blir internets roll tydligast i de brott som begås inom ramen för e-handeln, men det framgår att internet även används som ett verktyg både före och efter brottet. Till exempel används datorintrång för att komma åt kortuppgifter, och det finns en nätbaserad svart marknad för stulen information där bland annat olovligen åtkomna kortuppgifter erbjuds till försäljning.

Vid fakturabedrägerierna syns internets betydelse för brotten bland annat i att vissa bedragare utnyttjar mejlkontakter för att lura de utsatta till att tro att de ingått ett avtal med fakturaavsändaren. Vidare avser många av de granskade anmälningarna om fakturabedrägeri fakturor som skickats till företag med krav på betalning för olika former av tveksamma eller obefintliga internetrelaterade tjänster.

När det gäller kategorin övriga telefon- och internetbedrägerier utgör internet ett centralt verktyg. Här använder bedragarna exempelvis olika former av skadlig kod eller nätfiske för att, som

ett första steg, skaffa sig information som används för att komma åt andras bankkonton. En annan variant är datorintrång i mejlkonton eller konton på sociala media, med hjälp av vilka man kan vilseleda en person att skicka pengar eller känsliga uppgifter genom att låtsas vara en vän.

Identitetsmissbruk som ett led i bedrägeribrottsligheten

Någon form av identitetsmissbruk förekommer i alla typer av bedrägerier som identifierats i studien. Enligt en skattning ingår det som ett led i drygt sex av tio polisanmälda ärenden gällande brottsbalksbedrägerier. Även vid bidragsbrott och andra välfärdsbedrägerier kan osanna identiteter missbrukas, exempelvis genom falska namnteckningar på diverse intyg eller genom ansökningar om olika bidrag till företag med falska identiteter på lönelistor.

Uppgifter från flera aktörer inom näringslivet liksom från polisen, visar att olovligt bruk av andras identiteter i ett bedrägligt syfte är ett växande problem. Vid bedrägerier används inte bara stulna identiteter, utan även helt falska identiteter utan kopplingar till existerande personer. Gärningspersonen låtsas helt enkelt vara någon annan. Syftet är vanligtvis att dölja spåren till gärningspersonen, eller att etablera ett förtroende genom att exempelvis låtsas vara en närstående. Vilseledandet kan ske med hjälp av falska, stulna eller manipulerade identitetshandlingar (köp i annans namn vid kreditbedrägerier) eller utan några identitetshandlingar (t.ex. falska kontaktuppgifter vid annonsbedrägerier). Utöver privatpersoners identiteter missbrukas även olika organisationers eller företags identiteter vid bedrägerier.

Yngre mer utsatta, men äldre en särskilt sårbar grupp

Bedrägerier drabbar privatpersoner, men även näringslivet och myndigheter. Enligt NTU har det skett en utjämning när det gäller både ålder och kön bland dem som uppger att de blivit utsatta för bedrägerier. Kvinnor uppger i dag samma grad av utsatthet som män och fler något äldre personer (45–54 år) har rapporterat utsatthet – efter att utsattheten tidigare varit högst i yngre ålderskategorier. Även om yngre tycks vara mer utsatta generellt är äldre personer en särskilt sårbar grupp för vissa typer av bedrägerier. Det gäller främst vissa fakturabedrägerier och kortbedrägerier.

Bedragare: från personer i behov av snabba pengar till kunniga företagare

De granskade ärendena innehåller lite information om gärningspersoner. Endast vid annonsbedrägerier är gärningspersonen ofta känd. Ett vanligt motiv är snabba pengar oavsett konsekvenser,

vilket gör att brottsupplägget är enkelt och upptäcktsrisken relativt stor. Kriminalstatistiken visar att de personer som lagförs för bedrägerier och bidragsbrott överlag är något äldre än de lagförda för samtliga brott mot brottsbalken. Beträffande bidragsbrott är andelen kvinnor betydligt högre än vid andra brottstyper (över 40 procent). De som lagförs för bidragsbrott är dessutom mer sällan tidigare straffade jämfört med dem som lagförs för andra brott.

I Brås intervjumaterial skildras flera olika typer av bedragare, bland annat personer med kunskaper i exempelvis juridik och företagsekonomi. Dessa är inte sällan involverade i avancerade bedrägeriupplägg, och rör sig i gråzoner mellan legal och illegal verksamhet. De som i bästa fall lagförs för sådana brott är dock vanligtvis målvakter och olika typer av medhjälpare.

Näringslivets ansvar

Företag har en viktig roll i bedrägerisammanhang. Förutom att de själva blir utsatta för dessa brott fungerar de inte sällan som verktyg vid mer organiserade och systematiska bedrägerier. I det studerade materialet framkommer flera exempel på företag som skickar ut bedrägliga fakturor eller begår kreditbedrägerier.

Eftersatt kontroll i exempelvis finansiella system eller fraktkedja innebär också att näringslivet får en roll som möjliggörare för andras bedrägerier. Den stora utmaningen för näringslivet är nämligen att balansera krav på försäljning mot kontroll- och säkerhetsfrågor. Intervjuerna med näringslivsföreträdare visar att många företag ser dessa som oförenliga motsatser, och att försäljningssidan prioriteras medan man räknar med vissa förluster till följd av bedrägerier. Det finns också en bild av att hederliga kunder tycker att kontroller är krångliga, och att ökad kontrollnivå gör att de väljer att handla hos konkurrenter. Intervjuer med näringslivsrepresentanter respektive gärningspersoner talar också för att bedragarna riktar in sig på företag som uppfattas ha sämre säkerhet än konkurrenterna. Näringslivet har ett tydligt ansvar och stor förbättringspotential när det gäller att motverka bedrägeribrottsligheten.

Begränsade resurser hos rättsväsendet men även positiv utveckling

Under perioden sedan 2008 har polisen ägnat ökade resurser åt utredning av bedrägeribrottsligheten. Men enligt Brås intervjupersoner finns alltjämt en stor obalans mellan brottsvolymen och de tillgängliga utredningsresurserna. Det bidrar till långa utredningstider och en press att snabbt lägga ner svårutredda ärenden.

Samtidigt visar Brås olika material att det skett flera förbättringar i rättsväsendets arbete med bedrägerier. En viktig utveckling på området har varit inrättandet av polisens Nationella bedrägericenter (NBC) i syfte att göra arbetet mot bedrägerier mer effektivt och strukturerat. Intervjupersoner från både näringslivet och rättsväsendet betonar att det har skett stora förbättringar i polisens samordning av bedrägeriärenden, och rättsväsendet visar också på en ökad förmåga att ta sig an och driva stora, resurskrävande bedrägeriutredningar med flera gärningspersoner och många målsägare. Antalet bedrägeribrott som lett till åtal har ökat. Statistiken tyder också på en ökning sedan 2008 i andelen lagföringar som avser ett större antal bedrägeribrott. Och andelen lagföringar för brottsbalksbedrägerier som resulterat i en fängelsedom har ökat successivt.

De insamlade tingsrättsdomarna visar på den uttalade seriebrottskaraktären av den lagförda bedrägeribrottsligheten. I drygt 40 procent av domarna avseende brottsbalksbedrägerier hade det väckts åtal för fler än 20 bedrägeribrott, och drygt tio procent av de granskade domarna avsåg åtal för mer än 100 bedrägeritillfällen.

Förutsättningar för personuppklaring varierar stort

Samtidigt som det skett en ökning i antalet bedrägeribrott som lett till åtal visar resultaten att ökningen sannolikt inte är jämnt fördelad över olika typer av bedrägerier. Förutsättningarna för utredning och lagföring varierar stort mellan olika bedrägerimodus. De är relativt goda om det finns möjlighet att spåra överföringar till ett bankkonto som kopplas till gärningspersonen, vilket framför allt är fallet vid annonsbedrägerier och fakturabedrägerier.

Förutsättningarna för att utreda kortbedrägerier och kreditbedrägerier är däremot sämre. Det finns sällan en möjlighet att följa pengarna till ett bankkonto, och många anmälningar läggs ner antingen som icke utredningsbara eller för att det inte varit möjligt att identifiera en misstänkt person. Detsamma gäller för anmälningar i kategorin övriga telefon- och internetbedrägerier. Dessa bedrägerier begås oftast via internet antingen från utlandet eller via utländska servrar. Gärningspersonerna utnyttjar dessutom ofta tekniska möjligheter för att försvåra de brottsbekämpande myndigheternas spårningsarbete. När det gäller bidragsbrotten är gärningspersonen typiskt sett redan känd när anmälan görs, och andelen anmälningar som leder till ett personuppklaringsbeslut är relativt hög. Vid dessa ärenden ligger den främsta utmaningen i att styrka uppsåt.

Ett brottsområde i snabb förändring

Bedrägerier är ett brottsområde i snabb utveckling, med nya modus som används för att vilseleda personer, företag och den offentliga sektorn för egen vinning. Enligt de intervjuade är det framför allt bedrägerier med elektroniska kortuppgifter som ökar mycket snabbt. Enligt uppgifter från polisen har flera omfattande dataintrång ägt rum de senaste åren, och dessa har lett till att en stor mängd kortuppgifter hamnat i bedragarnas händer. Dessa bedrägerier är särskilt svåra att förebygga då de kräver ett internationellt samarbete, särskild it-kompetens och en större ambition från berörda aktörer att öka säkerheten. En annan tydlig trend, enligt experter, är att bedragarna i allt större utsträckning kartlägger andras profiler på sociala medier och använder informationen till mer riktade bedrägerier.

Brås bedömning

Utvecklingspotential hos rättsväsendet: effektivisera hanteringen av stora utredningar

Som nämnts ovan har det skett förbättringar i rättsväsendets arbete med bedrägerier de senaste åren. Samtidigt vill Brå lyfta fram några områden där det finns en utvecklingspotential.

Vissa bedrägerier resulterar i stora utredningar som är mycket krävande för rättsväsendet att hantera. Det handlar särskilt om fakturabedrägerier och assistansbedrägerier. Vid fakturabedrägerier skulle införandet av brottet grovt fordringsbedrägeri enligt Egendomsskyddsutredningens förslag (SOU 2013:85) innebära stora effektiviseringsvinster för utredningsarbetet. Vissa åtgärder för att effektivisera handläggning av stora assistansbedrägeriutredningar har föreslagits av Åklagarmyndigheten (Åklagarmyndigheten 2015). Det är viktigt att kunskap om dessa åtgärder sprids inom rättsväsendet och att de tillämpas även vid andra typer av utredningar än assistansbedrägerier. Det är också viktigt med ett fortsatt arbete att identifiera ytterligare åtgärder som kan ge effekt. En faktor som lyftes av Brås intervjupersoner var ett behov av en ökad kapacitet hos polisens it-forensiska funktioner.

Bättre kompetensförsörjning, kunskapsutbyten och metodutveckling

Brås resultat visar på en utbredd uppfattning att det finns en brist på vissa viktiga kompetenser inom polisens bedrägeriutredningsverksamhet. Det handlar dels om personer med specialkompetens avseende välfärdsbedrägerier, dels om kompetenser som behövs vid analyser av olika typer av bevisningsunderlag, bland annat revisorer. Överlag tyder resultaten på att det kan finnas behov av

att se över den sammansättning av kompetenser som finns inom polisens bedrägeriutredningsverksamhet.

Vid bedrägerier som begås med hjälp av företag kan det bli särskilt svårt att utreda vilka som ligger bakom bedrägeriet, eftersom de personer som syns framför allt är medhjälpare och målvakter. Här tyder Brås intervjuer på att det finns ett behov av ett kunskapsutbyte mellan polisen, som är relativt ovana vid att utreda brott som begås med företag, och Ekobrottsmyndigheten respektive Skatteverket, som har större erfarenhet av att kartlägga företag som används för brott. Dessa myndigheter behöver samverka för att få en god helhetsbild av bedrägeribrotten. Av samma skäl är det viktigt att arbeta mer underrättelsebaserat mot bedrägerier, för att identifiera särskilt aktiva bedragare, nya modus och de företag som ofta används. Här har också näringslivet viktig kunskap och information att delge myndigheterna. Förbättringar i rättsväsendets möjligheter att utreda välfärdsbedrägerier kan också uppnås genom samarbeten i syfte att höja kvaliteten på polisanmälningar från utbetalande myndigheter och organisationer.

När polisen tidigt lägger ner många ärenden inom vissa svårutredda bedrägerityper, exempelvis kort- och kreditbedrägerier, blir det svårt att identifiera utvecklingsmöjligheter för utredningsarbetet. Därför bör man prioritera metodutvecklingsinsatser inom dessa områden, bland annat för att hitta nya möjligheter att identifiera okända gärningspersoner. Det kan också finnas anledning att se över de bedrägeribrottskoder som används i kriminalstatistiken. Mer ändamålsenliga brottskoder skulle underlätta för rättsväsendets aktörer att dels följa utvecklingen av viktiga bedrägerityper, dels identifiera områden som kan behöva prioriteras.

Bedrägeriproblemet går inte att enbart lagföra bort

Även om rättsväsendets arbete mot bedrägerier kan förbättras ytterligare är en viktig slutsats att problemen med bedrägeribrottslighet inte kan lösas enbart genom rättsväsendets utrednings- och lagföringsverksamhet. Brottsvolymen är helt enkelt så omfattande att ökade resurser inte kan stå i proportion till den. De viktigaste insatserna för att minska bedrägeribrottsligheten är därför det förebyggande arbetet i samhället i stort.

Bedrägeribrottsligheten påverkar många samhällsaktörer som har stora möjligheter att arbeta brottsförebyggande, men andra intressen tycks i dagsläget väga tyngre. Det gäller både näringslivet och den offentliga sektorn.

Smidig försäljning och god service versus kontroll och säkerhet

Både utbetalande myndigheter och företag utsätts för samma dilemma mellan å ena sidan ambitionen att erbjuda snabb, smidig service eller försäljning, och å andra sidan garantera säkerhet och minska bedrägerier. För att inte förlora kunder till konkurrenter prioriteras inte säkerheten tillräckligt inom näringslivet. Att sträva efter branschgemensamma säkerhetslösningar, för att undvika överflyttning av kunder till företag med lägre säkerhet, är därför en av de mest centrala åtgärderna för näringslivets del. Det kräver en större medvetenhet om att företagen också har ett socialt och etiskt ansvar, inte minst då det finns indikationer på att en del av bedrägerivinsterna finansierar fortsatt brottslighet. Tänkbara lösningar som innebär att konflikten mellan smidighet och säkerhet inte behöver finnas bör ses över; en större användning av biometriska data vid betalningar är ett exempel. När det kommer till myndigheternas utbetalningar från välfärdssystemet föreslås en utvidgning och ökad användning av de regler som finns för informationsutbyte (lagen om underrättelseskyldighet). Vissa av de intervjuade representanterna för myndigheter och näringsliv ser ett hinder i att det, trots viss kontrollverksamhet, inte ligger i deras huvudsakliga arbetsbeskrivning att förebygga och bekämpa bedrägerier. I sitt dagliga arbete ser de många luckor och upplever att de skulle kunna vidta fler åtgärder.

Fraktkedjan: att stoppa i ett tidigt skede

En stor andel av de anmälda bedrägerierna, cirka tre av fyra, är en del av en köp- eller säljprocess. Allt större andel av handeln sker via internet, vilket innebär att varan fraktas till köparen. I samtliga steg av fraktkedjan – från beställning, via eventuell kreditprövning, frakt och utlämning av varan – finns det säkerhetsluckor som kan utnyttjas av bedragare. I intervjuer med både representanter för rättsväsendet och näringslivet framgick att huvudfokus i det förebyggande arbetet inom fraktkedjan främst inriktas på säker utlämning av varan. Det är där som förutsättningarna finns för den fysiska identitetskontrollen.

Samtidigt är det angeläget att stoppa bedrägerierna i ett så tidigt skede som möjligt, och satsningar på säkra internetbeställningar bör utgöra en större del av det förebyggande arbetet riktat mot bedrägliga köp. En ökad användning av e-legitimationer vid köp på internet förespråkas av flera aktörer inom näringslivet. Samtidigt kommer det även i fortsättningen att vara nödvändigt att säkerställa att den person som hämtar ut varan verkligen representerar den som beställt och betalat för den. Även vid utlämningsställen behöver man alltså i högre grad prioritera säkerhetsåtgärder. En nyckel till att skapa incitament för bättre

säkerhetskontroller hos olika aktörer inom fraktkedjan är en tydligare ansvarsfördelning mellan inblandade aktörer.

En parallell kan dras till myndigheterna och organisationerna inom välfärdssystemet. Vissa myndigheter, exempelvis Försäkringskassan, har kommit längre i att utarbeta inte enbart efterkontroll, utan har ett system för att i ett tidigt skede fånga upp misstänkta bidragsbrott. Syftet är att upptäcka och stoppa felaktiga utbetalningar innan de sker. Att fortsätta arbeta i den riktningen är angeläget.

Samlat grepp behövs kring identitetsfrågan

Det finns inslag av olovligt bruk av falska eller stulna identiteter i alla typer av bedrägerier, och även i bidragsbrott. Att låtsas vara någon annan är en vanlig vilseledande strategi. Som bakomliggande faktorer, typiska för Sverige, anges ett högt antal godkända identitetshandlingar, något som försvårar kontroller, samt det faktum att det är relativt lätt att på laglig väg ta del av andras personuppgifter. Brå gör samma bedömning som en del representanter för näringslivet, nämligen att en central aktör bör få ansvar för hantering av identitetshandlingar i alla faser, från ansökningsprocess, bakgrundskontroll av den sökande, tillverkningsprocess av handlingen – till utlämningsprocess och möjlighet att verifiera äkthet av utgivna identitetshandlingar. En personlig inställelse bör krävas både vid ansökan och utlämning av handlingarna. Att se över regleringen av när personuppgifter får lämnas ut är en annan viktig åtgärd, enligt berörda aktörer.

Regeringens lagrådsremiss för att kriminalisera olovlig identitetsanvändning träffar vissa av de gärningar som utgör ett led i bedrägeribrotten, men bruk av helt falska identiteter (utan koppling till en existerande person) täcks inte av den föreslagna bestämmelsen. I kartläggningen har det framkommit att det exempelvis förekommer ett bruk av multipla identiteter; det är därför grundläggande att garantera en säker ursprungsidentifiering, det vill säga att när personer registreras hos Migrationsverket eller Skatteverket ska enbart en person kunna kopplas till en identitet.

Kortbedrägerier: ett särskilt problemområde

Bedrägerier med stulna elektroniska kortuppgifter har enligt flera källor ökat snabbt under den senaste tiden. Som många internetrelaterade brott är dessa särskilt svåra att förebygga. Gärningspersonerna är inte sällan tekniskt kunniga, och kortuppgifterna skaffas fram genom avancerade dataintrång. Representanter för rättsväsendet betonar att e-handeln och bankväsendet behöver ta ett större ansvar på området. Några förslag är krav på elektronisk identifiering vid köp, något som behandlas i ett reviderat

EU-direktiv (PSD2) publicerat i slutet av 2015. Direktivet trädde i kraft i januari 2016 och ska implementeras inom två år. Den innebär större krav på så kallad stark kundautentisering med hjälp av en kombination av flera faktorer. En annan åtgärd som är under utveckling är möjligheten att som kund spärra sitt kontokort för internetköp eller köp utomlands (s.k. geoblocking), och öppna det bara vid köptillfällen. Allmänheten behöver också informeras om hur man skyddar sig mot dataintrång och hur man handlar säkert på internet – även om det tar några extra sekunder. Mycket tyder på att bedrägerier med hjälp av kortuppgifter är ett område där framtida förebyggande insatser behöver fokuseras, och där internationellt samarbete är nödvändigt.

För samtliga slutsatser och förslag, se rapportens två avslutande kapitel.

Del 1. Inledning, metod och bakgrund

I denna inledande del beskrivs först Brås uppdrag och de frågeställningar som formulerats utifrån uppdraget. Kort sammanfattas hur de studerade brotten definieras enligt lagen och hur rapporten disponeras. I ett påföljande kapitel redovisas de material och metoder som har valts för att besvara frågeställningarna och i ett tredje kapitel redogörs för de senaste årens bedrägeriutveckling enligt befintliga datakällor, det vill säga Nationella trygghetsundersökningen och kriminalstatistiken.

Inledning

Brås uppdrag

Brottsförebyggande rådet fick 2014 i uppdrag av regeringen att genomföra en studie om bedrägerier och arbetet mot sådan brottslighet. Bakgrunden är att både anmälningar till polisen och frågeundersökningar till befolkningen talar för att bedrägerierna ökar. En viktig anledning till ökningen sägs i uppdraget vara den tekniska utvecklingen, som har gjort det möjligt att begå dels nya former av bedrägeribrott, dels mer storskaliga bedrägeribrott. Mot bakgrund av detta krävs enligt regeringen ny kunskap för att stärka arbetet mot bedrägerier. Det gäller hur brottsligheten ser ut, hur rättsväsendet arbetar och vilka förebyggande åtgärder som kan ha effekt.

Enligt uppdraget skulle Brå

- beskriva bedrägeribrottslighetens omfattning och struktur
- redovisa utvecklingen av lagföringar och påföljder
- belysa tillvägagångssätt vid bedrägeribrott, med särskilt fokus på användning av datorer och internet, samt beskriva hur identitetsstölder kan användas som ett led i brottsligheten
- studera hur polis och åklagare arbetar med bedrägeribrott
- lämna rekommendationer för rättsväsendets arbete med bedrägeribrott
- föreslå förebyggande insatser som inbegriper såväl rättsväsendet som andra samhällsaktörer.

Studiens frågeställningar

Med utgångspunkt i regeringens uppdrag har följande frågeställningar formulerats:

- Hur ser bedrägeribrottslighetens utveckling ut enligt Nationella trygghetsundersökningen (NTU) och kriminalstatistiken?

- Vad finns det för olika typer av tillvägagångssätt vid bedrägeribrott och hur används internet och identitetsstölder vid bedrägeribrottslighet?
- I vilken utsträckning resulterar olika typer av anmälda bedrägerier i åtal och lagföring? Vilka motiveringar anges vid nedläggning respektive när åtal ogillats i domstolen?
- Vilka problem stöter rättsväsendet på när det gäller att utreda och lagföra bedrägeribrott?
- Vilken roll har näringslivet och myndigheter i samband med bedrägeribrottsligheten?
- Vad finns det för möjligheter att förebygga bedrägeribrott – mot bakgrund av studiens resultat?

Bedrägeribrottet enligt BrB 9 kap.

Enligt brottsbalkens 9 kap. 1 § 1 st. döms den ”som medelst vilseledande förmår någon till handling eller underlåtenhet, som innebär vinning för gärningsmannen och skada för den vilseledde eller någon i vars ställning denne är”, för *bedrägeri* till fängelse i högst två år. Centrala aspekter av brottet är således dels att det sker ett vilseledande, dels att detta vilseledande resulterar i någon form av förmögenhetsöverföring som är till gagn för gärningspersonen och till skada för den utsatte eller någon annan i dess ställe.

Enligt BrB 9 kap. 1 § 2 st. ska samma brottsrubricering gälla för den som genom bland annat oriktiga uppgifter påverkar en automatisk informationsbehandlingsprocess, det vill säga någon form av dator, så att det innebär vinning för gärningspersonen och skada för någon annan. Exempel på handlingar som kan leda till ett straffansvar enligt denna del av bedrägeribestämmelsen är att man gör olovliga bankomatuttag med någon annans kontokort eller att man olovligen genomför ett kortköp på internet med någon annans kortuppgifter.

För bedrägeribrott som med hänsyn till skadans omfattning och övriga omständigheter anses som ringa döms i stället för *bedrägligt beteende* enligt BrB 9 kap. 2 § till böter eller fängelse i högst sex månader. Enligt samma rubricering döms även den som uppsåtligen smiter från till exempel en taxi-, hotell- eller restaurangnota.

Straffskalan för *grovt bedrägeri*, som framgår av BrB 9 kap. 3 §, är fängelse i lägst sex månader och högst sex år. Vid bedömande av om brottet är grovt beaktas bland annat om gärningspersonen missbrukat allmänt förtroende eller utnyttjat att den utsatta personen varit särskilt sårbar (till exempel om gärningspersonen utnyttjat att den utsatte har någon form av funktionshinder

eller är en äldre person) eller om gärningspersonen begagnat falsk handling (till exempel ett förfalskat identitetskort). Andra faktorer som domstolen tar hänsyn till vid bedömning av brottets grovhet är om bedrägeriet skett med systematik, varit organiserat, ansetts påverka allmänhetens eller näringsidkares förtroende för betalningssystem eller avsett betydande värde. Enligt praxis ligger värdegränsen för ett grovt bedrägeri, om brottet inte anses som grovt på grund av andra omständigheter, på fem förhöjda prisbasbelopp.[3]

Enligt BrB 9 kap. 11 § är bedrägeri och grovt bedrägeri straffbara vid såväl försöks- som förberedelsestadiet, däremot inte bedrägligt beteende.

Bedrägeribrott mot välfärdssystemet har två olika lagrum

Bedrägeribrott kan begås mot privatpersoner, företag och andra organisationer samt mot myndigheter, till exempel mot Försäkringskassan eller Centrala studiestödsnämnden (CSN). Tidigare var alla bedrägerier mot välfärdssystemet del av brottsbalkens bestämmelse. Sedan bidragsbrottslagen trädde i kraft år 2007 faller dock de flesta bedrägerier mot välfärdssystemet under bidragsbrottslagen, som beskrivs nedan. Ett undantag är Arbetsförmedlingen vars företagarstöd fortfarande ryms under brottsbalkens bedrägeribestämmelse. Det finns också rättsliga avgöranden där vissa assistansbedrägerier ska rubriceras som bedrägeri, även om andra fall utgör bidragsbrott (Åklagarmyndigheten 2015). Samtliga sådana välfärdsbedrägerier beskrivs för enkelhetens skull under samma rubrik i kapitlet Bidragsbrott och andra välfärdsbedrägerier.

Brott mot bidragsbrottslagen

Vid sidan av bedrägeribestämmelsen finns således sedan år 2007 en särskild lag som riktar in sig på utbetalningar från välfärdssystemet: bidragsbrottslagen (2007:612). Om den är tillämplig har den företräde framför det ovan beskrivna bedrägeribrottet.

Bidragsbrottslagen rör ekonomiska förmåner som betalas ut för *personligt ändamål* och som beslutas av Försäkringskassan, Pensionsmyndigheten, CSN, Migrationsverket, Arbetsförmedlingen, de 290 kommunerna eller 28 arbetslöshetskassorna. Begränsningen till personligt ändamål är skälet till att vissa välfärdsbrott faller under den generella bedrägeribestämmelsen, exempelvis de olika former av anställningsstöd till arbetsgivare (företag) som Arbetsförmedlingen beslutar om.

[3] År 2016 ligger värdet på ett förhöjt prisbasbelopp på 45 200 kr.

En förklaring till att en särskild lag skapades för dessa bedrägeribrott var att bidragsfusket började uppfattas som ett växande problem (Korsell m.fl. 2008). Problemet uppfattades vara *enskilda* bidragstagare som inte anmälde ändrade förhållanden eller som till och med fått bidraget på felaktiga grunder vid första beslutstillfället. Företagens eller kriminella grupperingars bidragsfusk fanns ännu inte med i problembeskrivningen (se exempelvis SOU 2008:74, jfr ISF och Brå 2011:12). Även om omfattningen var okänd och det endast fanns uppskattningar – som visade på låga andelar felaktiga utbetalningar – är systemen av sådan storlek att låga andelar motsvarar stora belopp (SOU 2008:74). För att kunna ha kvar gällande ersättningsnivåer infördes därför en särskild lag – bidragsbrottslagen (prop. 2006/07:80). Det handlade alltså om att skydda skattepengarna från bedragare.

Ett centralt syfte var att minska antalet felaktiga utbetalningar och att stärka tilltron till välfärdssystemen (prop. 2006/07:80). Dessutom ansåg man att den generella bedrägeribestämmelsen inte riktigt fångade upp ”de särskilda förutsättningar” som finns vid utbetalningar av bidrag (och andra ekonomiska förmåner) från välfärdssystemen. Systemen behövde ett effektivt straffrättsligt skydd.

I bidragsbrottslagens 2 § framgår att ”Den som lämnar oriktiga uppgifter eller inte anmäler ändrade förhållanden som han eller hon är skyldig att anmäla enligt lag eller förordning, och på så sätt orsakar fara för att en ekonomisk förmån felaktigt betalas ut eller betalas ut med ett för högt belopp, döms för bidragsbrott”. Det finns ringa brott som har böter eller fängelse i högst sex månader i straffskalan. Brott av normalgraden har fängelse i högst två år, och grovt bidragsbrott har lägst sex månader och högst fyra år i straffskalan.

För att det ska röra sig om grovt brott ska det särskilt beaktas om det handlar om ett stort belopp, om falska handlingar använts eller om det är del av en systematisk eller omfattande brottslighet (3 §). Värdegränsen i praxis är precis som vid bedrägeri fem prisbasbelopp (Åklagarmyndigheten 2013). Straffskalan för grovt brott är dock lägre än vid den generella bedrägeribestämmelsen. En förklaring anges vara att lagstiftaren inte förväntade sig lika grova och organiserade bidragsbrott som vid bedrägerier generellt (Åklagarmyndigheten 2015).

I rapporten används termen bidrag även om det i strikt mening kan handla om förmåner eller ersättningar.

Uppsåtsfrågan: grov oaktsamhet räcker

Med andra ord finns stora likheter i straffskala och innehåll med den generella bedrägeribestämmelsen. I denna lagtext slår man

dock tydligare fast att den som söker bidrag är skyldig att anmäla ändrade förhållanden. Lagstiftaren gör inte heller någon skillnad mellan en faktisk utbetalning och fara för en sådan – detta eftersom skillnaden kan uppfattas som en slump – om den utbetalande myndigheten eller organisationen upptäcker brottet innan utbetalningen hunnit äga rum (prop. 2006/07:80). Brottet är med andra ord fullbordat redan innan utbetalningen har genomförts, det finns inget krav på en förmögenhetsöverföring. Till detta kommer att åklagaren inte behöver styrka att det skett ett vilseledande, fokus ligger på att den sökande lämnat oriktiga uppgifter.

En skillnad är också att grov oaktsamhet är straffbelagd – brottet heter vårdslöst bidragsbrott och ger böter eller fängelse i högst ett år. Bakgrunden är att välfärdssystemets myndigheter och organisationer snabbt ska fatta beslut om utbetalningar. Genom att kriminalisera grov oaktsamhet läggs ett tydligare ansvar på den sökande att lämna korrekta uppgifter och att upplysa om ändrade förhållanden. I realiteten är de anmälda fallen av grov oaktsamhet mycket få i förhållande till anmälningarna om uppsåtliga bidragsbrott.

Det finns också en särskild paragraf som säger att de i lagen uppräknade myndigheterna och organisationerna är *skyldiga* att anmäla misstänkta brott till polisen eller Åklagarmyndigheten (6 §).

Rapportens disposition

Rapporten är uppdelad i fyra huvuddelar. I den första har vi hittills beskrivit Brås uppdrag, studiens frågeställningar samt vilka brott som studeras. I nästa avsnitt redogörs för vilka metoder och material som använts för att besvara frågeställningarna. Därefter presenteras en redovisning av de senaste årens bedrägeriutveckling enligt befintliga statistiska källor.

I rapportens andra del presenteras en typologi över polisanmälda bedrägeribrott, med fem fördjupande avsnitt gällande de huvudkategorier av brottsbalksbedrägerier som kunnat identifieras i det granskade materialet, samt ett sjätte avsnitt avseende bidragsbrott.

Den tredje delen innehåller en fördjupande analys av olika aktörer och verktyg inom bedrägeriområdet. Här beskrivs vilka som drabbas och vilka som begår brotten, hur falska eller stulna identiteter kan användas som ett led i bedrägeribrottsligheten samt vilken roll näringslivet har, liksom de utbetalande myndigheterna. Här finns också ett kapitel om rättsväsendets arbete.

Rapportens fjärde, och sista, del består av två avslutande kapitel där vi summerar rapportens innehåll och redovisar förslag till åtgärder.

Tanken är att rapportens olika delar ska kunna läsas mer eller mindre självständigt, vilket också innebär att en och samma fråga på olika sätt kan beröras i flera avsnitt. Exempelvis kan näringslivets roll eller vilka som drabbas av bedrägerier vara teman som löper genom rapportens olika delar eftersom de kan vara viktiga att återkomma till i flera sammanhang.

Det ingår i Brås uppdrag att belysa hur datorer och internet används vid bedrägerier. Då internet används på olika sätt vid majoriteten av de bedrägerityper som belyses i rapporten kommer inget eget avsnitt att ägnas åt frågan, utan den behandlas genomgående i samband med respektive bedrägerityp.

Metod och material

Flera olika datakällor har använts för att besvara studiens frågeställningar. Framför allt har följande fyra huvudmaterial analyserats:

- Nationella trygghetsundersökningen (NTU) och den officiella kriminalstatistiken
- Granskning av polisärenden (urval av anmälningar och förundersökningar)
- Tingsrättsdomar
- Intervjuer med berörda aktörer och gärningspersoner.

Alla dessa empiriska källor har sina styrkor och svagheter, men tillsammans bidrar de till en helhetsbild över bedrägeribrottslighetens omfattning, karaktär och utveckling.

1. NTU och kriminalstatistiken

En övergripande bild av de senaste årens utveckling av bedrägeribrottsligheten kommer att redovisas i kapitlet Bedrägeriutvecklingen enligt befintliga källor. Utgångspunkt är Brås Nationella trygghetsundersökning (NTU) och den officiella kriminalstatistiken.

NTU är en årlig frågeundersökning om allmänhetens utsatthet för brott och kontakter med rättsväsendet. Den genomförs av Brå sedan 2006. Undersökningen bygger på ett nationellt, slumpmässigt urval av befolkningen i åldern 16–79 år.[4] Det bör noteras att bedrägerifrågan i NTU ställs på så sätt att undersökningsdeltagare tillfrågas om sin utsatthet för bedrägerier *i egenskap av privatpersoner*. Utvecklingen enligt NTU avser således endast privatpersoners utsatthet för bedrägerier.

[4] För mer omfattande beskrivningar av undersökningens genomförande hänvisas till tidigare års NTU-rapporter och därtill hörande tekniska rapporter (exempelvis Brå 2016:1).

Kriminalstatistiken ger en bild av de brott som hanteras av rättsväsendet. En sammanställning har gjorts av anmälda bedrägeri- och bidragsbrott, uppklarade brott och lagföringar. Vidare redovisas vissa uppgifter avseende lagförda personer samt de påföljder som beslutats av åklagare respektive domstolar.

2. Granskning av polisärenden

Den löpande officiella kriminalstatistiken över bedrägeribrott skiljer visserligen mellan olika bedrägerityper genom en rad brottskoder, men mycket tyder på att dessa inte beskriver dagens bedrägerier på ett adekvat sätt. Koderna är av äldre datum och det förekommer i dag en stor överlappning mellan exempelvis datorbedrägeri och bedrägeri med hjälp av internet – två bedrägerityper med var sin brottskod.

Ett annat problem är att många anmälda bedrägerier kodas av polisen som ”övrigt bedrägeri”. En kvalitetsstudie av användningen av brottskoder vid upptagning av anmälningar (Brå 2012a) visar att många bedrägerier registreras under fel brottskod och att en stor andel av de ”övriga bedrägerierna” hade kunnat placeras under någon mer specifik brottskod.

För att ta fram en lämplig typologi över olika tillvägagångssätt och för att bättre kunna beskriva bedrägeribrotten har Brå därför samlat in ett urval anmälningar och förundersökningar (härefter kallat ärenden) gällande bedrägerier och bidragsbrott och granskat innehållet i dessa. Granskningens syfte var också att få en mer detaljerad beskrivning av de bedrägeribrott som kommer till polisens kännedom, samt att få insikt i polisens och åklagarnas arbete med att utreda dessa brott.

Urval

Storleken på urvalet av de ärenden som ingår i studien bedömdes utifrån olika kriterier. Dels var det viktigt att granskningen var av sådan omfattning att den kunde hanteras resursmässigt. Ärendenas storlek kan variera väsentligt, och genomläsning och kodning kan vara mycket tidskrävande. Samtidigt måste urvalet vara tillräckligt stort för att fånga upp variationsvidden i den polisanmälda bedrägeribrottsligheten.

Vid bedömningen av urvalsstorleken togs även hänsyn till att relativt många av anmälningarna sannolikt läggs ner relativt tidigt under utredningsprocessen – ett antagande som verkar rimligt med tanke på att personuppklaringsprocenten[5] för bedrägeribrotten är låg. Utifrån dessa kriterier, granskningens syfte samt

[5] Med personuppklaring avses att en brottsanmälan har lett till att åklagaren väckt åtal, utfärdat strafföreläggande eller meddelat åtalsunderlåtelse.

erfarenhet från tidigare studier med liknande metod bedömde Brå att ett urval motsvarande 450 ärenden var av rimlig storlek.

För att kunna belysa både brottsbalksbedrägerier (BrB 9 kap. 1–3 §) och brott mot bidragsbrottslagen gjordes sedan två slumpmässiga delurval bland bedrägerier som anmälts under första halvåret 2013:[6]

- 400 ärenden gällande brottsbalksbedrägerier[7]
- 50 ärenden gällande brott mot bidragsbrottslagen[8]

Valet att vikta huvuddelen av urvalet till fördel för ett större antal ärenden gällande bedrägeri enligt brottsbalken ansågs motiverat då kunskapen om olika modus, men även rättsväsendets hantering av bidragsbrott, är väsentligt bättre än för brottsbalksbedrägerier (Brå 2015:8, ISF och Brå 2011:12, Brå 2008:6, Brå 2007:23, Brå 2005:10).

Genomgången av ärendena

Med utgångspunkt i k-diarienumren i urvalet beställde Brå polisutredningar[9] från respektive polismyndighet.

Ett kodschema utarbetades, dels utifrån befintliga rapporter om bedrägeribrottslighetens karaktär, dels utifrån informationen från en första testgenomgång av ärendena. Varje ärende lästes sedan igenom, och olika omständigheter kring brottet, liksom utredningsmässiga aspekter, kodades in i ett statistikprogram. Nedan följer några exempel på vilken typ av information som kodades

- om anmälaren/målsägaren är privatperson eller ett företag/organisation/myndighet
- målsägarens kön och ålder (om privatperson)
- typ av organisation (om företag/organisation/myndighet)
- tillvägagångssätt vid brotten
- inslag av identitetsstöld

---

6 Beslutet att avgränsa urvalet till första halvåret 2013 gjordes för att så många som möjligt av de anmälda brotten i urvalet skulle hinna handläggas klart före slutet av december 2014. Detta var den sista punkt då projektet skulle få tillgång till information om åtals- respektive nedläggningsbeslut från Brås register (se vidare nedan).

7 Inkluderar brottskoder: 0901, 0902, 0903, 0904, 0905, 0906, 0912, 0913, 0922, 0929, 0932, 0935.

8 Inkluderar brottskoder: 5060, 5061, 5062, 5063, 5064, 5065, 5066, 5067, 5068, 5069, 5070, 5071, 5072, 5073, 5074, 5075.

9 Totalt 31 ärenden har inte skickats till Brå av polismyndigheterna – 29 ärenden avseende brottsbalksbedrägerier, 2 avseende bidragsbrott, vilket motsvarar 7 respektive 4 procent av motsvarande delurval. Dessa har granskats och kodats utifrån Brås så kallade FTK-databas. Databasen innehåller fritextdelen från varje brottsanmälan, det vill säga en kort beskrivning av händelseförloppet vid brottet.

- användning av internet
- vilka typer av utredningsåtgärder som vidtagits.

Det förekommer en stor variation mellan de granskade ärendena i fråga om innehåll. Informationsmängden skiljer sig dessutom åt beroende på vilken typ av bedrägeri ärendet avser. Vissa bedrägerier läggs ner i ett väldigt tidigt skede, och ärendet innehåller därför mycket begränsat med uppgifter. Om förundersökningen pågått under en längre period är informationen mer utförlig.

Granskningen av de 450 anmälda ärendena utgör en stomme i beskrivningen av tillvägagångssätten vid brotten och framtagandet av Brås typologi över de polisanmälda bedrägeribrotten.

Utdrag från Misstankeregistret och Rättsväsendets uppföljningssystem (RUS)

Ytterligare två registerutdrag beställdes i arbetet med ärendegranskningen: från Misstankeregistret respektive Rättsväsendets uppföljningssystem (RUS).

I kombination med den information som framgår av de insamlade polisärendena används dessa utdrag för att beskriva vilka ärenden som gått vidare till åtal samt de grunder som angetts av polis och åklagare vid nedläggning av bedrägeriärenden.

Utdraget från misstankeregistret innehåller samtliga brottsmisstankar som registrerats mot de personer som blivit skäligen misstänkta för bedrägeribrotten i Brås urval av polisärenden. Det innebär att utdraget också ger en överblick över bedrägeriutredningarnas omfattning.

De åtals- respektive nedläggningsbeslut som finns i utdraget avser perioden fram till och med slutet av 2014. I redovisningar av de uppklarade och nedlagda bedrägeribrotten särredovisas därför hur många ärenden som fortfarande var under utredning vid denna tidpunkt.

Granskningens begränsningar: mörkertalet och tidsaspekten

Eftersom Brås granskning av polisärendena är det mest centrala empiriska materialet i studien är det viktigt att vara tydlig om både dess fördelar och begränsningar.

Granskningen ger en fördjupad inblick i de ärenden som hanteras av rättsväsendet, men har sina begränsningar. En av dem är mörkertalet, det vill säga att olika typer av bedrägerier har olika stor tendens att komma till polisens kännedom. Det innebär svårigheter att utifrån anmälda brott mer exakt studera den *faktiska* bedrägeribrottslighetens omfattning och struktur. Det är

dock rimligt att anta att de vanligast förekommande formerna av bedrägerier åtminstone i någon mån blir anmälda till polisen. Tidigare studier baserade på liknande granskningar av polisanmälningar och förundersökningar har visat att de ger en varierande men överlag god information om olika tillvägagångssätt vid brott.

En annan begränsning är urvalets storlek, som innebär att de andelar som redovisas i rapporten avseende fördelningen av olika bedrägerityper bör betraktas som relativt grova skattningar. Detsamma gäller rapportens redovisningar av andelar uppklarade respektive nedlagda bedrägeribrott. Urvalet är dock tillräckligt stort för att belysa tydliga skillnader.

Vidare bör noteras att de granskade ärendena avser brott som anmäldes under våren 2013, och med den dynamiken som bedrägerifältet förändras kan vissa modus redan ha blivit mindre vanliga på bekostnad av nya. De redovisade andelarna av olika bedrägerityper bland anmälda brott kan därmed vara något inaktuella i dag. Samtidigt har de huvudsakliga tillvägagångssätten sannolikt inte förändrats, och de stora brottskategorierna som kunde identifieras i granskningen är troligen desamma i dag liksom under den närmaste framtiden.

Sammantaget kan konstateras att polisärenden utgör en viktig kunskapskälla när det gäller bedrägeribrottslighetens karaktär, även om de behöver kompletteras med annan information.

3. Tingsrättsdomar

Ett av studiens syften är att belysa hur olika typer av bedrägeribrott hanteras i tingsrätterna.[10] För att göra detta har ett särskilt urval av tingsrättsdomar samlats in. Först gjordes ett slumpurval av ärenden avseende bedrägeribrott som hade personuppklarats under första halvåret 2013. För att kunna belysa hanteringen av såväl brottsbalksbedrägerier som bidragsbrott drogs återigen två delurval:

- 140 ärenden gällande personuppklarade brottsbalksbedrägerier
- 25 ärenden gällande personuppklarade brott mot bidragsbrottslagen.

Med utgångspunkt i dessa ärenden beställdes sedan först ett utdrag från misstankeregistret, som gav personnummer på de misstänkta gärningspersonerna. Därefter användes dessa uppgifter för att beställa ett utdrag från lagföringsregistret avseende de

[10] Det har inte varit möjligt inom ramen för uppdraget att samla in och granska domar från överinstanser.

aktuella personerna. Utdraget från lagföringsregistret gicks sedan igenom för att identifiera de aktuella bedrägeridomarna.

En del av ärendena i urvalet (12 st.) hade personuppklarats genom beslut om åtalsunderlåtelse eller strafföreläggande, vilket innebar att ingen tingsrättsdom fanns att tillgå. I ytterligare fem ärenden har det inte varit möjligt att hitta en relevant dom i lagföringsregistret. Bland de 148 ärenden där det varit möjligt att hämta in en tingsrättsdom ingår ibland flera av ärendena i urvalet i samma dom, vilket innebär att antalet domar är mindre än antalet ärenden. Totalt 113 domar har samlats in, av vilka 95 avser brottsbalksbedrägeriärenden och 18 bidragsbrottsärenden.

Domarna har kodats med avseende på bland annat

- antalet tilltalade
- antalet bedrägeritillfällen
- om de tilltalade har fällts eller friats för bedrägeribrotten
- vilka typer av bevisning som åberopats i tingsrätten
- de skäl som anges för att åtalspunkter gällande bedrägeribrott eventuellt ogillats.

4. Intervjuer

För att ge en ökad förståelse för innehållet i polisärendena och för de olika problem som uppstår under arbetet med att utreda och lagföra bedrägerier har Brå intervjuat poliser och åklagare. Då bedrägeribrottsligheten berör många olika samhällssektorer, såväl privata som offentliga, har Brå även intervjuat representanter för näringslivet och myndigheter. Brå har dessutom genomfört intervjuer med gärningspersoner för att ta del av de kunskaper och erfarenheter som finns hos personer med egna erfarenheter av bedrägeribrottslighet. Sammanlagt 61 enskilda och 2 fokusgruppsintervjuer har genomförts. Fokusgruppsintervjuerna kretsade kring it-relaterade bedrägerier respektive identitetsmissbruk som ett led i bedrägeribrottsligheten.

Intervjuerna var semistrukturerade och följde en intervjuguide bestående av frågor som anpassades efter respektive intervjupersons expertområde. Intervjuerna ägde rum löpande under projektet. Parallellt med det övriga arbetet och i takt med att nya relevanta områden identifierades söktes nya intervjupersoner upp i ett kriteriestyrt snöbollsurval. Samtliga intervjuer har varit anonyma.

Representanter för rättsväsendet

Rekryteringen av intervjupersoner från rättsväsendet skedde dels med utgångspunkt i den information som finns i de insamlade

polisärendena om vilka poliser och åklagare som arbetat med fallen, dels utifrån befintliga kontakter inom rättsväsendet, inte minst med polisens Nationella bedrägericenter.

Frågorna kretsade kring eventuella problem med att identifiera gärningspersoner och få fram bevisning samt vilka faktorer som upplevs som centrala i relation till beslut om att lägga ned en förundersökning eller att föra ett fall vidare till åtal. Vidare har frågor ställts kring olika aspekter av hur samordningen av arbetet med den här typen av brottslighet fungerar samt om samverkan mellan polisen, åklagare och andra aktörer. Intervjuer med rättsväsendet gav också inblick i senaste nytt när det gäller bedrägerimodus, vilket var ett viktigt komplement till ärendegranskningen (som bygger på anmälningar från våren 2013).

Sammanlagt har 15 representanter för rättsväsendet intervjuats, varav fem åklagare och tio polisanställda. Bland de polisanställda ingick fyra personer med särskild it-kompetens. Tre av dessa intervjuades i den ovan nämnda fokusgruppsintervjun med inriktning på it-relaterade bedrägerier.

Representanter för andra samhällssektorer

Många bedrägeribrott når aldrig rättsväsendet, och informationen som finns att hämta ur polisens ärenden respektive ur intervjuer med polis och åklagare visar därmed bara en del av den komplexa bilden över samtliga bedrägerier och bedrägeriförsök. Det innebär att intervjuer med rättsväsendets aktörer inte kan ge inblick i alla sätt på vilka bedrägeribrottsligheten kan komma till uttryck. Olika typer av bedragare använder en varierad infrastruktur, och många samhällssektorer kan på olika sätt direkt drabbas eller utnyttjas som brottsverktyg. Det innebär att samhällsfunktioner utanför rättsväsendet måste involveras i det förebyggande arbetet. Därför har en rad berörda aktörer intervjuats – bland annat representanter för bankväsendet, branschorganisationer, fraktföretag, e-handel, säkerhetsföretag, särskilt drabbade sektorer inom handeln och även forskare på området.

Sammanlagt har 32 representanter för olika samhällssektorer intervjuats, därav 9 representanter för finanssektorn, 17 representanter för andra delar av näringslivet och 6 representanter för olika myndigheter. Dessutom har Brå intervjuat en forskare och en fokusgrupp bestående av 8 personer med kunskaper om identitetsmissbruk.

Gärningspersoner

Hur en bedragare vilseleder någon, vilka verktyg som används och vilka luckor i samhällssystemet som utnyttjas kan bäst beskrivas av förstahandskällan – bedragarna själva. Mycket av den

kunskap och de erfarenheter dessa personer besitter kan inte fås på annat sätt. För att nå gärningspersoner kontaktades anstalter och frivilligorganisationer för personer som vill lämna en kriminell miljö. Detta förfarande har resulterat i intervjuer med relevanta personer i många andra studier (exempelvis Brå 2011:7, Brå 2012:12, Brå 2007:4, Brå 2007:7 samt på bedrägeriområdet i Storbritannien, Gill 2005, 2007).

Dessa intervjuer hade en explorativ prägel. Under respektive intervju fick berättelsen växa fram och följdfrågor anpassades därefter. En möjlig brist kan vara att gärningspersoner som är villiga att ställa upp på en intervju inte är representativa för bedragare generellt. Samtidigt är bedrägeribrottsligheten så komplex och heterogen att en ”typisk bedragare” inte existerar. Syftet var heller inte att generalisera, utan att beskriva och ge exempel på den stora mängden tillvägagångssätt.

Att intervjua personer dömda för brott om deras kriminella karriärer kan naturligtvis vara mycket känsligt. Deltagandet var dock frivilligt och anonymt. Inledande frågor som ställdes handlade om generella aspekter kring olika typer av bedrägeribrottslighet och inte om eget deltagande i brottslighet. Det var upp till intervjupersonen själv om denne valde att berätta om sådant som kan uppfattas som känsligt. Erfarenhet från denna och tidigare Brå-studier talar dock för att intervjupersonerna använder sin egen kriminella erfarenhet när frågor av denna typ besvaras.

Brå har intervjuat totalt 16 gärningspersoner med egna erfarenheter av bedrägeribrott.

Bearbetning av intervjuerna

Vid samtycke spelades intervjuerna in och transkriberades. Med hjälp av ett program avsett för analys av kvalitativa data (Atlas) kodades sedan innehållet i de transkriberade intervjuerna utifrån en rad centrala teman, relevanta för studiens syften och frågeställningar. Citat valdes ut för att illustrera analysen och slutsatserna med relevanta exempel.

Övriga informationskällor: litteratursökningar, studiebesök, referensgrupp och samarbete med NBC

Som en del i projektets arbete med att ta tillvara såväl nationell som internationell kunskap har Brå sökt i forskningsdatabaser för att ta del av relevant forskning. Vi har även gjort internetsökningar för att hitta relevanta rapporter och bakgrundsmaterial som inte återfinns i databaserna (så kallad grå litteratur). De

kunskaper som inhämtats från dessa litteratursökningar refereras fortlöpande i rapporten.

Brå har också genomfört flera studiebesök i London, hos National Fraud Intelligence Bureau vid City of London Police, Cifas som tillhandahåller Storbritanniens National Fraud Database, Home Office samt även Counter Fraud Centre vid Cipfa, med ansvar för bland annat forskning och utbildning i syfte att motverka bedrägerier mot den offentliga sektorn. Syftet med besöken var att samla kunskap som kan vara relevant för brottsförebyggande åtgärder i Sverige. Ett fokus var också att ta reda på vilket samarbete olika funktioner har med andra aktörer och vad de ser för utvecklingspotential på området.

Genom hela projekttiden har Brå samarbetat med polisens Nationella bedrägericenter i Stockholm, som etablerades under 2014. Centrets uppdrag är att öka polisens möjligheter att samordna resurser mot bedrägeribrott som sker över hela landet, samt att göra brottsbekämpningen mer effektiv.[11]

Projektet har även knutit till sig en referensgrupp bestående av representanter för såväl rättsväsendet som näringslivet och olika myndigheter. Två seminarier ägde rum, ett vid uppstarten för att inhämta uppslag och ett i slutet av projekttiden, där de preliminära resultaten presenterades med syftet att få återkoppling från seminariedeltagarna.

[11] Rikspolisstyrelsen 2015, se vidare kapitlet om Rättsväsendets arbete.

Bedrägeriutvecklingen enligt befintliga källor

Detta kapitel är en sammanställning av uppgifter om bedrägeribrottsligheten enligt redan tillgängliga datakällor. I kommande kapitel analyseras och beskrivs det empiriska materialet som samlats inom ramen för denna studie.

Fokus för sammanställningen nedan om bedrägeribrottsligheten ligger på perioden sedan 2008. Anledningen är införandet av den tidigare beskrivna bidragsbrottslagen (2007:612), som innebar en förändring i redovisningen av den officiella kriminalstatistiken på bedrägeriområdet. Många typer av bidragsrelaterade bedrägerier, som tidigare hade redovisats i statistiken som brott mot bedrägeribestämmelsen i brottsbalken, har sedan 2008 redovisats separat som brott mot bidragsbrottslagen, vilket innebär att innehållet i vissa kategorier av polisanmälda bedrägerier inte är jämförbart mellan perioden före 2008 och perioden efter.

Nedan redovisas först utvecklingen enligt Nationella trygghetsundersökningen (NTU) och därefter utvecklingen av den polisanmälda bedrägeribrottsligheten samt av personuppklarade brott, bedrägerilagföringar och påföljder. När det gäller NTU, uppklarade brott, lagföringar och påföljder finns tillgänglig statistik för perioden till och med 2014. För de polisanmälda bedrägeribrotten finns även preliminär statistik för 2015.

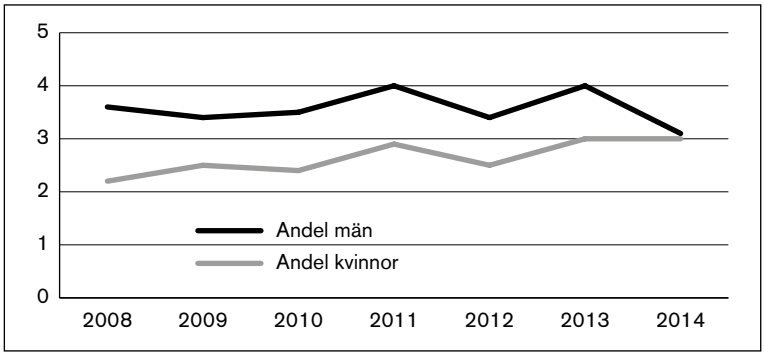
Utvecklingen enligt NTU

Nationella trygghetsundersökningen genomför årliga mätningar om bland annat utsatthet för brott i ett slumpurval av den svenska befolkningen i åldersspannet 16–79 år. Den fråga som ställs i NTU för att fånga upp allmänhetens utsatthet för bedrägeri är: Blev du som privatperson på ett brottsligt sätt lurad på pengar eller andra värdesaker under förra året?[12]

[12] NTU mäter inte utsatthet för bedrägerier som drabbar exempelvis företag och myndigheter utan endast utsattheten hos privatpersoner.

Under perioden 2008–2014 har andelen personer som uppgett sig vara utsatta för bedrägerier enligt NTU varierat och både ökat och minskat från år till år men överlag följer utvecklingen en svagt ökande trend under perioden, åtminstone när det gäller utsatthet bland kvinnor (Brå 2016:1, jfr figur 1). År 2008 uppgav 2,9 procent av undersökningsdeltagarna att de blivit utsatta för bedrägeri, vilket motsvarar 205 000 personer i befolkningen (16–79 år). Motsvarande andel för 2014 är 3,1 procent, motsvarande 230 000 personer i befolkningen. De flesta som uppgett att de blivit utsatta för bedrägerier har uppgett att det rört sig om en enstaka händelse. Under perioden har det skattade antalet bedrägerihändelser i befolkningen enligt NTU varierat mellan som minst 298 000 (år 2008) och som mest 391 000 (år 2013). År 2014 uppgick det skattade antalet bedrägerihändelser i befolkningen till 321 000.

Figur 1. Utsatthet för bedrägeri 2008–2014 enligt NTU. Andel utsatta efter kön. Procent.



Som framgår av figuren har män uppgett sig vara utsatta för bedrägerier i något större utsträckning än kvinnor varje år sedan 2008, med undantag för 2014, då andelarna kvinnor och män som uppgav att de varit utsatta var nästan lika.

Sett till nästan hela perioden 2008–2014 visar NTU att personer i åldersspannet 20–34 år drabbas av bedrägerier i något större utsträckning än andra åldersgrupper samt att den rapporterade utsattheten är minst bland personer i åldersgruppen 65–79 år (se tabell 1). De senaste åren syns en viss förskjutning mot en ökande andel av något äldre utsatta personer; i den senaste mätningen var utsattheten högst i gruppen 45–54 år.

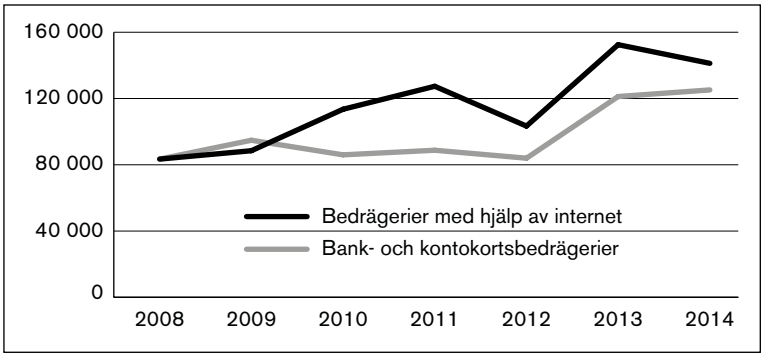
Tabell 1. Andel personer i olika åldersgrupper som uppgett att de blivit utsatta för bedrägeri enligt NTU. 2008–2014. Procent.

Åldersgrupp	2008	2009	2010	2011	2012	2013	2014
16–19	3,1	1,8	2,6	3,0	1,6	2,9	1,6
20–24	4,0	4,0	4,6	6,1	4,3	5,1	3,8
25–34	3,9	4,1	3,6	5,0	4,3	4,2	3,6
35–44	3,8	3,3	3,2	3,6	3,5	5,0	2,9
45–54	2,9	3,2	3,6	3,5	3,5	3,5	4,2
55–64	2,2	2,5	2,5	2,5	2,1	3,0	3,7
65–74	1,3	1,5	1,5	1,8	1,7	1,5	1,6
75–79	0,4	1,7	0,8	1,5	0,9	1,6	1,4

Ökning i både kortbedrägerier och internetbedrägerier enligt NTU

NTU ger inte någon fullständig bild av vilka olika typer av bedrägerier som informanterna blivit utsatta för. Däremot redovisas hur stor andel av de bedrägeribrott som uppges i undersökningen som skett med hjälp av internet respektive genom att någon utnyttjat den utsattes bank- eller kontokort. Figur 2 redovisar en skattning av utvecklingen av antalet bedrägerihändelser som enligt NTU har skett i form bank- eller kontokortsbedrägerier respektive bedrägerier med hjälp av internet.

Figur 2. Utvecklingen enligt NTU av skattat antal bedrägerier mot privatpersoner som skett i form av bank- eller kontokortsbedrägerier respektive bedrägerier med hjälp av internet. 2008–2014. Absoluta tal.[13]



Andelen bedrägerier som enligt NTU har skett med hjälp av internet har ökat markant under perioden 2008–2014 från 28 procent till 44 procent. Andelen bank- eller kontokortsbedrä-

[13] Redovisningen bygger på egna beräkningar dels utifrån NTU:s skattning av det totala antalet bedrägerihändelser i befolkningen för respektive år, dels utifrån de redovisade andelarna bedrägerihändelser för respektive år som skett i form av kontokortsbedrägerier respektive internetbedrägerier.

gerier har också ökat, från 28 procent till 39 procent. Det har således skett en tydlig omfördelning när det gäller vilka typer av bedrägerier som NTU-deltagarna uppgett att de blivit utsatta för under perioden. År 2008 svarade internetbedrägerier och kortbedrägerier för sammanlagt 56 procent av de bedrägerihändelser som NTU-deltagarna hade utsatts för, jämfört med över 80 procent år 2014. Antalet bedrägerier med hjälp av internet har följt en ökande trend under i stort sett hela perioden 2008–2014. För kortbedrägerierna var nivåförändringarna relativt begränsade fram till 2012, men därefter syns en markant ökning under undersökningens två sista år.

Allmänhetens benägenhet att polisanmäla bedrägerier har ökat

Andelen bedrägerihändelser som enligt NTU-deltagarna har blivit anmälda till polisen har ökat under perioden 2008–2014, från 34 procent år 2008 till som mest 44 procent (2013). År 2014 uppgav undersökningsdeltagarna att 40 procent av bedrägerihändelserna som nämnts i undersökningen hade anmälts till polisen.

Den polisanmälda bedrägeribrottsligheten

Totalt sett har de polisanmälda bedrägeribrotten ökat under perioden 2008–2015.[14] Samtidigt har utvecklingen skiljt sig åt inom olika underkategorier av bedrägeribrott. Denna redovisning av de polisanmälda brotten tar först sikte på de polisanmälda händelser som kommer att betecknas som ”brottsbalksbedrägerier”, dvs. brott mot BrB 9 kap. 1–3 § (Bedrägerier inklusive grova brott samt bedrägligt beteende) för att sedan flytta fokus till de polisanmälda brotten mot bidragsbrottslagen.

Stor ökning i antalet polisanmälda brottsbalksbedrägerier

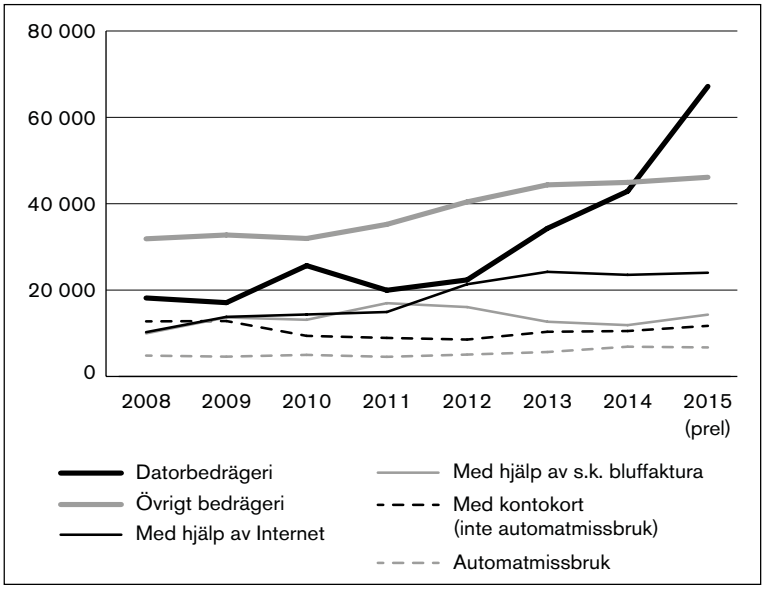
Under perioden 2008–2015 har antalet polisanmälda brottsbalksbedrägerier ökat med 90 procent, från drygt 91 000 anmälda brott år 2008 till över 173 000 år 2015. Jämfört med de anmälda brottsbalksbrotten totalt sett innebär detta en mycket stor ökning, då det sammanlagda antalet anmälda brott mot brottsbalken bara har ökat med 9 procent under samma period. Bedrägeribrottens andel av samtliga anmälda brott mot brottsbalken har ökat från 8 procent år 2008 till 14 procent år 2015.

År 2008 var de till antalet sex största kategorierna av bedrägeribrott enligt anmälningsstatistiken: Övrigt bedrägeri, Datorbedrägeri, Bedrägeri med kontokort, Bedrägeri med hjälp av internet,

[14] I skrivande stund är statistiken för år 2015 fortfarande preliminär.

Bedrägeri med hjälp av så kallad bluffaktura samt Automatmissbruk. Utvecklingen för dessa brottskategorier under perioden 2008–2015 framgår av figur 3.

Figur 3. Utvecklingen av de sex till antalet största kategorierna av anmälda brottsbalksbedrägerier under åren 2008–2015. Absoluta tal.



De största andelsmässiga ökningarna under perioden avser *datorbedrägerier* (ökning med 270 procent) respektive *bedrägerier med hjälp av internet* (ökning med 134 procent). Antalet anmälda *bedrägerier med hjälp av bluffaktura* minskade under några år efter 2011, men ökade igen år 2015 för att ligga 43 procent högre jämfört med 2008, medan antalet *övriga bedrägerier* har ökat med 45 procent under perioden 2008–2015. Under samma period minskade antalet anmälda *kontokortsbedrägerier* med 8 procent, från närmare 12 800 till drygt 11 700; under de senaste tre åren observeras dock en uppgång. Samtidigt har antalet anmälda brott som registrerats som *automatmissbruk*, som framför allt avser att någon olovligen använt en annan persons kort för ett bankomatuttag, ökat med närmare 40 procent, från drygt 4 800 anmälda brott år 2008 till drygt 6 700 anmälda brott år 2015.

I stora drag stämmer bilderna enligt NTU och den polisanmälda brottsligheten överens

Som har nämnts tidigare i rapporten innehåller anmälningsstatistiken en del osäkerheter, beroende på oklarheter avseende hur polisens brottskoder används vid registrering av olika typer av bedrägeribrott. Samtidigt finns det en relativt hög grad av över-

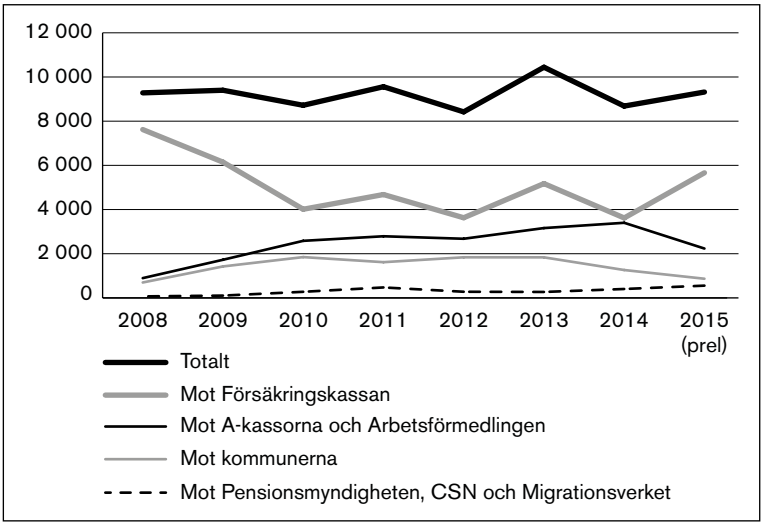
ensstämmelse när man jämför de bilder av bedrägeriutvecklingen som framgår av NTU respektive kriminalstatistiken. Sammantaget tyder resultaten från NTU och kriminalstatistiken på att antalet bedrägerier som faktiskt begås har ökat.

Både NTU och kriminalstatistiken visar en ökning i antalet bedrägerier som begåtts med hjälp av internet. Bedömningen är något svårare när det gäller den stora ökningen som framgår av NTU avseende utsatthet för bank- och kontokortsbedrägerier de senaste åren. Det beror på att kortbedrägerier redovisas i den anmälda brottsstatistiken under flera olika koder. Samtidigt har både antalet anmälda *kontokortsbedrägerier* och antalet anmälningar om *automatmissbruk* ökat under de senaste tre åren, med sammanlagt 35 procent. Det är dessutom sannolikt att en relativt stor del av den stora ökningen i kategorin *datorbedrägerier* som syns i den anmälda brottsstatistiken under perioden 2012–2015 också beror på en ökning i antalet anmälda kortbedrägerier, då dessa utgör en av de bedrägerityper som ryms inom denna brottskategori.[15]

Brott mot bidragsbrottslagen

Utvecklingen 2008–2015 för de anmälda bidragsbrotten framgår av figur 4.

Figur 4. Utvecklingen av de anmälda brotten mot bidragsbrottslagen åren 2008–2015, totalt samt för de anmälande myndigheterna och organisationerna. Absoluta tal.



[15] Som den kommande ärendegranskningen av ärenden från 2013 visar utgjorde bedrägerier med kort nästan hälften av samtliga bedrägerier som polisen kodat som datorbedrägeri (se bilaga 3).

Totalt sett har antalet anmälda bidragsbrott varken ökat eller minskat sett till hela perioden 2008–2015. Antalet anmälda bidragsbrott år 2015 var en halv procent högre än antalet anmälda brott år 2008.

Det har skett en viss omfördelning under perioden när det gäller vilka typer av bidragsbrott som registrerats. Anmälda brott mot Försäkringskassan har minskat med en fjärdedel (men är den största kategorin såväl 2008 som 2015), medan brott mot kommunerna, Arbetslöshetskassorna och Arbetsförmedlingen samt mot Pensionsmyndigheten, CSN och Migrationsverket har ökat i varierande grad.

Bidragsbrott är i huvudsak så kallade spanings- och ingripandebrott, vilket innebär att förändringar i antalet anmälda brott framför allt beror på förändringar i olika myndigheters kontrollarbete och anmälningsbeteende (Brå 2005:10, Brå 2008:6, Riksrevisionen 2011). Det innebär att det inte går att dra slutsatser om den faktiska utvecklingen av bidragsbrotten utifrån den polisanmälda brottsligheten.

Det som utvecklingslinjerna för de olika utbetalande aktörerna visar är framför allt att det skett förändringar när det gäller olika myndigheters fokus på bidragsbrottsligheten – en tillsyn av polismyndigheternas handläggning av bedrägeriärenden har till exempel funnit att det skedde en förändring under senare delen av 00-talet i Försäkringskassans syn på vilka ärenden som skulle föranleda en anmälan om brott (Rikspolisstyrelsen 2012a). Från att ha gjort stora kontrollinsatser av föräldrars tillfälliga vård av barn (vab) har Försäkringskassans resurser flyttats mot att kontrollera svårare ärenden (Brå 2008:6, jfr Riksrevisionen 2011). Det ger färre ärenden, men fall där varje misstänkt bidragsbrott utgör högre belopp.

Personuppklarade brott

Ökning under 2008–2014 i antalet uppklarade brottsbalksbedrägerier

Under perioden 2008–2014 ökade antalet personuppklarade[16] brottsbalksbedrägerier med nästan 20 procent, från närmare 10 000 uppklarade brott år 2008 till närmare 12 000 uppklarade brott år 2014.

Samtidigt varierar personuppklaringsprocenten mellan olika typer av anmälda bedrägeribrott (se tabell 2). År 2014 låg exempelvis personuppklaringsprocenten för bedrägeri med kontokort

[16] Med personuppklaring avses att en brottsanmälan har lett till att åklagaren väckt åtal, utfärdat strafföreläggande eller meddelat åtalsunderlåtelse.

eller med hjälp av internet på 15 respektive 11 procent. Motsvarande siffra för datorbedrägeri låg däremot på 2 procent. Sett till hela perioden 2008–2014 är personuppklaringsprocenten högre år 2014 än år 2008 för tre stora kategorier av anmälda brottsbalksbedrägerier – bedrägerier med hjälp av *bluffaktura, automatmissbruk* och *kontokortsbedrägerier*.

Antalet uppklarade bedrägeribrott har ökat under perioden inom de flesta kategorier av bedrägerier som redovisas i kriminalstatistiken. Den största procentuella ökningen i antalet personuppklarade bedrägeribrott avser *bedrägerier med hjälp av bluffaktura*, som nästan tredubblats, från drygt 300 personuppklarade brott år 2008 till närmare 900 år 2014. Därefter kommer *bedrägerier med hjälp av internet* där antalet personuppklarade brott nästan har fördubblats, från närmare 1 350 år 2008 till närmare 2 700 år 2014. Av de sex stora bedrägerikategorierna som redovisas i tabell 2 är det endast inom kategorin *datorbedrägeri* som antalet uppklarade brott har minskat.

Tabell 2. Personuppklaringsprocent för de sex vanligaste kategorierna av anmälda brottsbalksbedrägerier, respektive för bidragsbrott. Åren 2008–2014.

	Andel personuppklarade brott per år						
	2008	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**
Brottsbalksbedrägerier (totalt)	**11**	**16**	**15**	**14**	**9**	**9**	**8**
Övrigt bedrägeri	15	22	17	14	12	11	11
Datorbedrägeri	7	5	6	8	3	4	2
Med hjälp av internet	13	20	28	28	15	14	11
Bluffaktura	3	6	4	1	2	3	7
Kontokort (ej automatmissbruk)	9	23	20	22	9	11	15
Automatmissbruk	9	12	14	11	10	12	12
Brott mot bidragsbrottslagen (totalt)	**26**	**32**	**41**	**47**	**44**	**54**	**41**
Mot Försäkringskassan	29	39	46	50	46	77	53
Mot kommunerna	10	16	26	39	50	29	38
Mot A-kassorna och Arbetsförmedlingen	7	20	45	49	39	33	31
Mot Pensionsmyndigheten, CSN och Migrationsverket	1	25	13	20	35	32	27

Högre andel personuppklarade bidragsbrott

Antalet personuppklarade brott mot bidragsbrottslagen har ökat under perioden 2008–2014 med närmare 50 procent, från närmare 2 400 till drygt 3 500. Personuppklaringsprocenten för brott mot bidragsbrottslagen har ökat från 26 procent år 2008 till en topp på 54 procent år 2013. År 2014 minskade andelen personuppklarade brott mot bidragsbrottslagen till 41 procent, vilket var samma nivå som år 2010.

Jämfört med andelen personuppklarade brottsbalksbedrägerier är den genomsnittliga personuppklaringsprocenten för bidragsbrotten betydligt högre. En del av förklaringen till detta är att när en misstanke om brott uppkommer är den misstänkta gärningspersonen så gott som alltid känd, i egenskap av mottagare av bidrag eller stöd (Brå 2008:6). Dessutom har Försäkringskassan och många andra utbetalande myndigheter och organisationer särskilda utredare som underlättar polisens och åklagarnas arbete genom att ta fram underlag innan brotten anmäls till rättsväsendet (ISF och Brå 2011:12).

Personuppklaringen bland de polisanmälda bidragsbrotten varierar dels mellan de olika utbetalande myndigheterna, dels från år till år. Sett till hela perioden är andelen personuppklarade bidragsbrott relativt hög för brotten mot Försäkringskassan och jämförelsevis låg för brotten mot Pensionsmyndigheten, CSN och Migrationsverket.

Lagföringsbeslut och påföljder

Lagföringsbeslut redovisas i kriminalstatistiken efter huvudbrottet i lagföringen. Det innebär att när samma lagföring avser två eller flera brott av olika typer, redovisas lagföringen efter den brottstyp som enligt lagstiftningen har den strängaste straffskalan. Ett och samma lagföringsbeslut kan avse alltifrån ett enda brott till ett stort antal brottstillfällen.

Minskat antal lagföringsbeslut gällande brottsbalksbedrägerier

Under perioden 2008–2014 har antalet lagföringsbeslut med bedrägeri enligt BrB 9 kap. som huvudbrott (brottsbalksbedrägerier) minskat med drygt 40 procent (från 2 004 till 1 157). Detta förhållande kan framstå som märklig med tanke på att antalet personuppklarade brott har ökat under samma period. En rimlig förklaring, som också får stöd i Brås intervjuer med aktörer inom rättsväsendet, är att det skett en ökning över tid i andelen lagföringar som avser ett större antal bedrägeritillfällen. Det beror bland annat på en förbättrad samordning av större bedrägeriärenden hos polisen (se kapitlet om Rättsväsendets arbete).

Snabb ökning i antalet lagföringsbeslut avseende bidragsbrott i början av den studerade perioden

Antalet lagföringsbeslut med brott mot bidragsbrottslagen som huvudbrottet i lagföringen visar ett annat utvecklingsmönster (tabell 3). Lagföringsbesluten ökade under perioden 2008–2014, från 27 till 370, genom en snabb ökning under perioden 2008–

2011, som sedan följdes av en gradvis minskning åren 2011–2014. Den snabba ökningen i början av perioden är kopplad till det tidigare nämnda förhållandet att bidragsbrottslagen trädde i kraft först år 2007. Det innebär att brott som begicks innan dess hanterades enligt bedrägeribestämmelsen i brottsbalken, även om de anmäldes till polisen först år 2008 eller senare.

Som nämnts ovan utreds oftast misstankar om bidragsrelaterad brottslighet först av utredare på de utbetalande myndigheterna innan de anmäls till polisen. Det framgår vidare av tidigare granskningar på området att handläggningstiderna för dessa myndighetsutredningar kan bli relativt långa (Riksrevisionen 2011), vilket gäller även för utredningstiderna hos polisen när brotten väl har anmälts (ibid.). Överlag finns det således ofta en betydande eftersläpning mellan brottsdatum och lagföringsdatum vid dessa brott. Det låga antalet uppklarade bidragsbrott år 2008 och den snabba ökningen fram till 2011, är således framför allt ett uttryck för en successiv ökning i antalet brott mot bidragsbrottslagen som hunnit hela vägen genom den rättsliga processen.

Tabell 3. Andelen lagföringar med brottsbalksbedrägerier eller bidragsbrott som huvudbrott som skett i form av strafföreläggande, åtalsunderlåtelser eller domslut efter olika huvudpåföljder, för perioden 2008–2014. Procent.

	2008	2009	2010	2011	2012	2013	2014
Bedrägeri (BrB 9 kap. 1–3 §)	N = 2004	N = 1928	N = 1870	N = 1688	N = 1462	N = 1302	N = 1157
Åtalsunderlåtelse	11	13	14	14	14	12	11
Strafföreläggande	19	16	14	12	11	13	10
Domslut:							
Böter	5	5	7	6	6	4	5
Skyddstillsyn/ villkorlig dom	48	48	45	47	47	47	47
Fängelse	12	13	14	15	15	17	19
Övrigt (ungdomsvård/ ungdomstjänst mm)	5	6	6	6	7	6	7
Brott mot bidragsbrottslagen	N = 27	N = 221	N = 308	N = 472	N = 459	N = 447	N = 370
Åtalsunderlåtelse	11	9	6	3	6	3	5
Strafföreläggande	56	34	29	30	27	24	29
Domslut:							
Böter	7	16	13	15	12	12	6
Skyddstillsyn/ villkorlig dom	22	40	51	50	52	58	54
Fängelse	4	1	1	2	1	1	5
Övrigt (ungdomsvård/ ungdomstjänst mm)	-	-	0	1	2	1	1

Brottsbalksbedrägerier – större andel fängelsedomar över tid

Under perioden 2008–2014 har det skett vissa förändringar när det gäller typ av lagföring och påföljdsbeslut för brottsbalksbedrägerierna. Andelen lagföringar i form av åtalsunderlåtelser och strafföreläggande har minskat, från 30 procent år 2008 till drygt 20 procent år 2014, och andelen lagföringar i form av en fängelsedom har gradvis ökat över tid, från 12 procent år 2008 till 19 procent år 2014.

Under perioden har andelen lagföringar för brottsbalksbedrägerier med *grovt bedrägeri* (BrB 9 kap. 3 §) som huvudbrottet i lagföringen ökat med en tredjedel, från närmare 16 procent år 2008 till närmare 21 procent år 2014, och det har inte skett någon större förändring i hur stor andel av lagföringarna för grovt bedrägeri som resulterat i en fängelsedom (50 procent år 2008, 51 procent år 2014). Det har däremot skett en successiv ökning i andelen lagföringar för bedrägeribrott av normalgraden (BrB 9 kap. 1 §) som resulterat i en fängelsedom (från knappt 6 procent år 2008, till närmare 13 procent år 2014).

Domstolarnas val av ett fängelsestraff i stället för en villkorlig dom eller skyddstillsyn kan påverkas av flera faktorer. Sett mot bakgrund av den tidigare nämnda minskningen i antalet bedrägerilagföringar, samtidigt som antalet personuppklarade bedrägerier har ökat, kan däremot den successiva ökningen i andelen fängelsedomar för bedrägerier av normalgraden också ses som ett tecken på en ökning i andelen så kallade serieuppklaringar bland de personuppklarade brottsbalksbedrägerierna. Allt annat lika skulle en fängelsedom för bedrägeri av normalgraden bli mer sannolik ju fler brott det finns i åtalet. Samtidigt är utvecklingen också sannolikt påverkad av andra förändringar som skett under perioden inom gruppen lagförda för brottsbalksbedrägerier. Dessa diskuteras nedan i anknytning till redovisningen av de personer som blivit lagförda för bedrägeri.

När det gäller den genomsnittliga längden på den utdömda fängelsetiden vid bedrägeribrotten har det inte skett någon större förändring under perioden 2008–2014. För grovt bedrägeri har den genomsnittliga utdömda fängelsetiden varierat mellan 17 månader (år 2008) och 21 månader (år 2014), med ett medianvärde för perioden på 19 månader. För bedrägeribrott av normalgraden har den genomsnittliga fängelsetiden legat mer eller mindre konstant på 4–5 månader.

Brott mot bidragsbrottslagen – minskning över tid i andelen bötesdomar

Om man bortser från år 2008, då det bara registrerades 27 lagföringar med brott mot bidragsbrottslagen som huvudbrottet, finns det inga tydliga mönster i utvecklingen av val av påföljd vid lagföring för dessa brott, med undantag för en successiv minskning i andelen brott som lagförts genom att gärningspersonen blivit dömd att betala böter i domstol. Jämfört med lagföringarna för brottsbalksbedrägerier är det mindre vanligt med lagföringar i form av åtalsunderlåtelser bland brott mot bidragsbrottslagen, och desto vanligare med strafföreläggande. Andelen lagföringar för brott mot bidragsbrottslagen som resulterat i en fängelsedom är mycket lägre, jämfört med lagföringar för brottsbalksbedrägerier. Under den redovisade perioden har andelen lagföringar för bidragsbrott som resulterat i en fängelsedom legat på omkring en procent, med undantag för år 2014, då fem procent av lagföringarna resulterade i ett fängelsestraff.

Sedan år 2009 har antalet lagföringar med grova bidragsbrott (bidragsbrottslagen 3 §) som huvudbrottet i lagföringen varierat mellan 10 (år 2009) och 54 (år 2012). Bland dessa lagföringar har andelen som resulterat i en fängelsedom varierat från år till år, men ligger för hela perioden på närmare 18 procent. Motsvarande andel för lagföringar med *ringa* bidragsbrott eller bidragsbrott av *normalgraden* (bidragsbrottslagen 2 §) som huvudbrott i lagföringen ligger på en dryg halv procent. Det låga antalet fängelsestraff som dömts ut för bidragsbrott gör det mindre meningsfullt att beskriva en utveckling för den genomsnittliga fängelsestrafftiden. Sett till hela perioden 2009–2014 ligger den genomsnittliga strafftiden för lagföringar för grova bidragsbrott på 21 månader. Motsvarande strafftid för de icke grova bidragsbrotten ligger på 2,5 månader.

Lagförda personer

År 2014 misstänktes drygt 3 600 personer för bedrägeri enligt brottsbalken och 967 personer för bidragsbrott. Sammanlagt 1 157 personer lagfördes under samma år för brottsbalksbedrägerier och 370 personer för bidragsbrott.

I tabell 4 redovisas uppgifter om kön och ålder hos personer lagförda för brottsbalksbedrägerier respektive bidragsbrott, sammantaget för hela perioden 2008–2014. En jämförelse görs även av köns- och åldersfördelning bland personer som blivit lagförda för samtliga brott mot brottsbalken. För personer lagförda för brottsbalksbedrägerier respektive brott mot bidragsbrottslagen särredovisas även köns- och åldersfördelningen för de personer som lagförts för grova brott.

Högre ålder och jämnare könsfördelning än vid annan brottslighet – särskilt för bidragsbrott

Som framgår av tabellen är andelen unga personer, 15–20 år, betydligt lägre bland lagförda för brottsbalksbedrägerier (14 procent) jämfört med samtliga brott mot brottsbalken (27 procent). När det gäller grova brott halveras andelen ytterligare. Vid bidragsbrott är det ytterst ovanligt att unga lagförs (1 procent). De flesta lagförda för brottsbalksbedrägerier är mellan 21 och 39 år. Bland de lagförda för bidragsbrott är många även 40–49 år gamla. Genomgående är de lagförda något äldre när brotten är grova.

Tabell 4. Köns- och åldersfördelningar hos personer lagförda för samtliga brott mot brottsbalken, personer lagförda för brott mot BrB 9 kap. 1–3 § (brottsbalksbedrägerier) samt personer lagförda för bidragsbrott, under perioden 2008–2014. Procent.

	Samtliga brott mot brottsbalken	Brottsbalksbedrägerier		Brott mot bidragsbrottslagen	
	Samtliga N = 377 858	Samtliga N = 11 411	Grovt N = 2 118	Samtliga N = 2 304	Grovt* N = 186
Kön					
Kvinna	24	30	20	41	44
Man	76	70	80	59	56
Ålder					
15–20	27	14	7	1	2
21–29	24	32	30	22	18
30–39	18	23	25	29	20
40–49	16	18	21	27	25
50–59	10	9	12	17	22
60–	5	4	6	6	12

* Uppgifter om köns- och åldersfördelningen för lagföringar för grova bidragsbrott avser perioden 2009–2014, då dessa uppgifter inte särredovisas i statistiken för år 2008.

Det finns en något större andel kvinnor bland de lagförda för samtliga brottsbalksbedrägerier (30 procent) än bland de lagförda för samtliga brottsbalksbrott (24 procent). Bland de lagförda för grovt bedrägeri (BrB 9 kap. 3 §) är däremot andelen kvinnor mindre (20 procent).

Bland de lagförda för samtliga bidragsbrott är könsfördelningen jämnare (41 procent kvinnor, 59 procent män). Könsfördelningen är ännu jämnare bland de lagförda för grova bidragsbrott (44 respektive 56 procent).

När man ser till utvecklingen över tid (redovisas ej i tabell) i könsfördelningen inom de olika grupperna av lagförda personer har det skett vissa förändringar under perioden 2008–2014. Bland de lagförda för samtliga brott mot brottsbalken har köns-

fördelningen varit stabil. Detsamma gäller för könsfördelningen bland de lagförda för bidragsbrott (med undantag för året 2014, då andelen kvinnor ökade). Andelen kvinnor bland de lagförda för brottsbalksbedrägerier har däremot minskat successivt under perioden, från 35 procent år 2008 till 26 procent år 2014.

Denna utveckling hänger sannolikt ihop med den tidigare nämnda eftersläpningen i bidragsmyndigheternas och rättsväsendets hantering av bedrägeribrott mot bidragsmyndigheterna. Andelen lagförda kvinnor är högre när det gäller bidragsbrott; minskningen i andelen kvinnor lagförda för brottsbalksbedrägeri förklaras då sannolikt av en överflyttning till lagföringar för bidragsbrott efter 2007.

Tidigare belastning: lagförda för bidragsbrott relativt sällan tidigare straffade

I tabell 5 redovisas de tidigare brottsbelastningsnivåerna hos personer lagförda för brottsbalksbedrägerier respektive brott mot bidragsbrottslagen under perioden 2008–2014. På samma sätt som vid redovisningarna av köns- och åldersfördelningarna ovan redovisas även brottsbelastningsnivån för de lagförda för samtliga brott mot brottsbalken under samma period som en jämförelse.

Tabell 5. Tidigare belastning (andelar personer med olika antal tidigare lagföringar för brott) bland personer lagförda för samtliga brott mot brottsbalken, brottsbalksbedrägerier respektive bidragsbrott under perioden 2008–2014. Procent.

	Lagförda för …		
Antal tidigare lagföringar	… samtliga brott mot brottsbalken N = 377 858	… brottsbalks-bedrägerier N = 11 411	… brott mot bidragsbrottslagen N = 2 304
0	47	41	60
1–2	23	28	28
3–4	9	12	6
5+	21	19	6

Sett till hela perioden 2008–2014 är andelen brottsbelastade personer något större i gruppen lagförda för brottsbalksbedrägerier jämfört med motsvarande andel bland de lagförda för samtliga brott mot brottsbalken.

Det är endast små skillnader mellan grupperna när det gäller andelen personer med tre eller fler tidigare lagföringar för brott. Andelen personer med inga tidigare lagföringar för brott är däremot större bland de lagförda för brott mot brottsbalken (47 procent) än bland de lagförda för brottsbalksbedrägerier (41 procent). Just den här typen av skillnad är däremot förväntad

på grund av att andelen ungdomar är mycket mindre bland de lagförda för brottsbalksbedrägerier. Ungdomar är en grupp som av naturliga skäl – de har sällan hunnit samla på sig särskilt många lagföringar jämfört med äldre personer – i regel är mindre brottsbelastade än andra grupper av lagförda personer.

Jämfört med både gruppen lagförda för samtliga brottsbalksbrott och gruppen lagförda för brottbalksbedrägerier är gruppen lagförda för bidragsbrott betydligt mindre brottsbelastad.

Av de lagförda för bidragsbrott är det 60 procent som inte har någon tidigare lagföring för brott, vilket är en betydligt högre siffra jämfört med motsvarande andelar bland de lagförda för samtliga brott mot brottsbalken respektive de lagförda för brottsbalksbedrägerier. Samtidigt är det en mycket mindre andel av de lagförda för bidragsbrott, jämfört med de andra två grupperna av lagförda personer, som har fem eller fler tidigare lagföringar.

Utveckling mot en högre brottsbelastning bland lagförda för brottsbalksbedrägerier

Inom gruppen lagförda för brottsbalksbedrägerier har det under perioden 2008–2014 skett en minskning över tid i andelen personer med inga tidigare lagföringar, från 48 procent år 2008 till 38 procent år 2014. Det har samtidigt skett en successiv ökning i andelen personer med fem eller fler tidigare lagföringar, från 15 procent år 2008 till 23 procent år 2014. Den tidigare belastningsnivån inom gruppen lagförda för brottsbalksbedrägerier har således ökat något över tid.

En viss minskning i andelen personer med inga tidigare lagföringar för brott syns under perioden även bland de lagförda för samtliga brottsbalksbrott (från 50 procent år 2008 till 45 procent år 2014) samt även en viss ökning i andelen personer med fem eller fler lagföringar (18 procent år 2008, 22 procent år 2014). Förskjutningen mot en ökning i andelen tidigare belastade personer bland de lagförda är däremot något mer uttalad bland de lagförda för brottsbalksbedrägerier.

På samma sätt som vid minskningen över tid av andelen kvinnor bland de lagförda för brottsbalksbedrägerier, hänger denna utveckling också sannolikt till stor del ihop med en förflyttning över tid av mindre belastade personer från gruppen lagförda för brottsbalksbedrägerier till gruppen lagförda för brott mot bidragsbrottslagen.

När man ser till utvecklingen i den genomsnittliga brottsbelastningen inom den kombinerade gruppen lagförda för både brottsbalksbedrägerier och bidragsbrott, ser man fortfarande en viss förskjutning mot en högre brottsbelastning över tid, men

skillnaderna jämfört med utvecklingen inom gruppen lagförda för samtliga brott mot brottsbalken är relativt små.

Sammanfattning

Sammanfattningsvis har det under de senaste åren skett en ökning i bedrägeribrottsligheten, både i termer av självrapporterad utsatthet och i antalet ärenden som hanteras av rättsväsendet. Beträffande de utsatta har en viss utjämning ägt rum beträffade ålder och kön. Från det att män tidigare uppgav sig vara betydligt mer utsatta för bedrägerier än kvinnor kunde ingen skillnad observeras i den senaste NTU-mätningen – efter att utsattheten bland kvinnor tycks ha ökat. Enligt denna senaste mätning har även koncentrationen av utsatta 20–24-åringar minskat och andelen var då högst bland 45–54 år gamla. Enligt NTU har det samtidigt skett en markant ökning i bedrägerier med hjälp av internet och med kontokort.

Bilden motsvarar utvecklingen enligt kriminalstatistiken, där en ökning observeras främst i bedrägerianmälningar gällande de brottskoder som motsvarar kortbedrägerier och internetrelaterade bedrägerier. Personuppklaringsprocenten för brottsbalksbedrägerier var 8 procent år 2014 men varierar mellan olika typer av anmälda bedrägeribrott. Andelen personuppklarade brott är betydligt högre beträffande bidragsbrott – 41 procent år 2014.

Antalet brottsbalksbedrägerier som lett till åtal har ökat sedan 2008, samtidigt som antalet lagföringsbeslut har minskat. Det tyder på en ökning i andelen lagföringar som avser ett större antal bedrägeribrott. Andelen fängelsedomar har blivit större bland lagföringar för brottsbalksbedrägerier, motsvarande cirka en femtedel år 2014. Antalet lagföringar för bidragsbrott ökade snabbt i början av perioden allteftersom brott mot det nya lagrummet hann utredas klart. Fängelse döms sällan ut för bidragsbrott.

Personer lagförda för brottsbalksbedrägerier, men ännu mer de som lagförts för bidragsbrott, uppvisar en jämnare köns- och åldersfördelning jämfört med lagförda för samtliga brottsbalksbrott. Det är vidare betydligt mindre vanligt att lagförda för bidragsbrott är tidigare straffade – i jämförelse med lagförda för brottsbalksbedrägerier och personer lagförda för samtliga brottsbalksbrott.

Del 2. De polisanmälda bedrägerierna – en fördjupande analys

Bedrägeribrottsligheten omfattar allt från enkla upplägg med ensamma gärningspersoner till stora härvor där flera företag medverkar för att systematiskt utnyttja välfärdssystemet. Samtidigt innehåller de officiella statistiska källorna i form av NTU och kriminalstatistiken endast begränsat med information om vad det är för olika tillvägagångssätt som används vid bedrägeribrottsligheten i Sverige. Med vissa undantag, exempelvis fakturabedrägerier, vet vi ganska lite om vilka typer av bedrägerimodus som ligger bakom siffrorna i den officiella statistiken.

Huvudsyftet med denna del av rapporten är att beskriva de olika typerna av bedrägeribrott som anmäls till polisen och deras omfattning, samt eventuella variationer i rättsväsendets hantering av dessa olika typer av bedrägeribrott. För att kunna beskriva den polisanmälda bedrägeribrottsligheten har ett första steg varit att, med utgångspunkt i Brås urval av anmälda bedrägeriärenden, utveckla en tydlig struktur, en så kallad typologi, i form av ett antal kategorier under vilka de granskade fallen kan placeras.

En typologisk beskrivning av polisanmälda bedrägerier

Arbetet med typologin

Typologin över bedrägeribrott som redovisas i detta kapitel utgår från skillnader i *tillvägagångssättet* vid polisanmälda bedrägerier mot BrB 9 kap. 1–3 § (brottsbalksbedrägerier), då det framför allt är för dessa brott som en fungerande och aktuell kategorisering saknas. Brott mot bidragsbrottslagen utgör däremot en i hög grad homogen och tydligt avgränsad kategori, och kommer därför att behandlas i ett särskilt avsnitt.

Ett första steg har varit att i möjligaste mån skapa enhetliga och ömsesidigt uteslutande kategorier av brottsbalksbedrägerier, även om en viss överlappning kan förekomma.[17] För att kartlägga olika tillvägagångssätt till innehållet har de insamlade ärendena gällande brottsbalksbedrägerier samt även domarna använts. Fördelningen mellan de olika kategorierna redovisas däremot enbart utifrån de 400 anmälda ärendena, för att ge en representativ bild.

Hela arbetet med den nya typologin genomsyrades av en växelverkan mellan information utifrån andras erfarenheter och befintliga publikationer respektive innehållet i det egna materialet bestående av anmälningar, förundersökningsdokument och domar. På så sätt växte ett slutgiltigt kodschema fram som sedan använts vid kategoriseringen av materialet.

Det bör understrykas att eftersom mörkertalet, det vill säga brott som aldrig anmäls till polisen (se kapitlet om Metod och material) sannolikt varierar beroende på bedrägerityp, och eftersom

[17] Som ett exempel kan nämnas att det som här refereras till som annonsbedrägerier handlar om bedräglig *försäljning* genom internetannonser. Samtidigt kan också en del bedrägliga *köp* äga rum via liknande annonser, även om detta tycks vara betydligt mer ovanligt.

tillvägagångssätten förändras över tid, är den här presenterade typologin inte på något sätt definitiv, och fördelningen är inte enkelt generaliserbar till bedrägeribrottsligheten i stort. Den ger dock en fullgod övergripande bild av vilka typer av bedrägerier som drabbar både individer och olika delar av samhället och ger även en bra grund för att beskriva hur olika bedrägeriärenden hanteras av rättsväsendet.

Nedan ges en översikt av de olika kategorierna för att i kommande kapitel mer djupgående analysera dels de huvudkategorier bland brottsbalksbedrägerierna som kunnat identifieras i granskningen, dels bidragsbrotten.

Brottsbalksbedrägerier är oftast kopplade till en köp- eller säljprocess

Vid granskning av ärendena kunde, som väntat, en stor mängd av olika typer av bedrägerier enligt BrB 9 kap. identifieras, se tabell 6. På den mest övergripande planen kunde de flesta, cirka tre fjärdedelar, av de granskade brottsbalksbedrägerierna (BrB 9 kap. 1–3 §) rymmas under två huvudkategorier – *bedräglig försäljning* respektive *bedrägliga köp m.m.* med en tredje kategori av övriga brottsbalksbedrägerier. Majoriteten av brottsbalksbedrägerierna, men inte alla, kan alltså sägas vara kopplade till någon form av köp- eller säljprocess. Var och en av dessa tre typer av bedrägerier består sedan av ett antal underkategorier.

Bedräglig försäljning

Bedräglig försäljning motsvarar en tredjedel av samtliga bedrägerier mot BrB 9 kap. och består främst av två stora underkategorier – *annonsbedrägerier* och *fakturabedrägerier* samt en kategori av *annan bedräglig försäljning*. Den underliggande logiken är att gärningspersonen/-personerna använder försäljningsprocessen för att vilseleda en annan för egen vinning.

Vid *annonsbedrägerier* (16 procent av samtliga anmälda bedrägerier mot BrB 9 kap.) är den vanliga metoden att någon, via en internetannons, låtsas avse sälja en vara eller en tjänst som dock, trots betalning, aldrig levereras. Det kan även handla om att den köpta varan är falsk (exempelvis en falsk konsertbiljett eller en kopia av ett märkesplagg) eller på något sätt inte motsvarar vad som stod i annonsen. *Fakturabedrägerier* (12 procent) kan ha flera olika och ibland mer komplicerade upplägg. De präglas av att gärningspersoner, antingen enskilda individer eller företag, genom faktura kräver målsägaren på betalning för en vara eller tjänst som denne aldrig beställt. I vissa fall hänvisar gärningspersonen till ett befintligt avtal som dock målsägaren har en annan

uppfattning om eller inte alls känner till. Ett annat exempel är att målsägaren erhåller en faktura med högre summa än vad som fanns i överenskommelsen.[18]

I kategorin *övrig bedräglig försäljning* (5 procent) finns bl.a. internetförsäljning från bedrägliga företagssidor samt händelser då mycket tyder på att det rör sig om annonsförsäljning men det beskrivs otydligt i dokumentationen. Här finns även några fall då pengar fortsätter att dras från målsägares kort efter ett avslutat internetköp eller test av varuprov. Ett annat exempel är bedrägerier av mer traditionell karaktär i form av försäljning av falska varor (i ett fall falska mattor) genom dörrknackning.

Bedrägligt köp, lån eller uttag

Bedrägliga köp, lån eller uttag motsvarar så mycket som 43 procent av alla anmälda brottsbalksbedrägerier. Även i detta fall domineras bilden av två stora underkategorier – *kortbedrägerier* respektive *kreditbedrägerier* – samt *övriga bedrägliga köp, lån eller uttag*. Det grundläggande tillvägagångssättet här är att gärningspersonen köper sig en vara eller tjänst på någon annans bekostnad. I samband med *kortbedrägerier* (22 procent) kan elektroniska kortuppgifter användas för att handla, vanligen via internet, (så kallat *card not present*, CNP) eller så kan fysiska kort användas (*card present*, CP). I det sistnämnda fallet kan det exempelvis handla om stulna kort eller om manipulerade kort som har försetts med stulna kortuppgifter (exempelvis genom skimning). *Kreditbedrägerier* (17 procent) innebär att gärningspersonen köper en vara eller tjänst i någon annans namn. Det förutsätter alltså i regel en identitetsstöld (se särskilt kapitel om Identitetsmissbruk). Tecknande av mobilabonnemang och köp av varor på kredit är de vanligaste exemplen, men det förekommer även direkta banklån eller sms-lån i annans namn.

Bland *övriga bedrägliga köp, lån eller uttag* (5 procent) finns exempelvis snyltning (8 ärenden) – samtliga utom en mot taxibolag, eller bedrägerier med falska checkar. Här finns även tre fall av annonsbedrägerier då gärningspersonen utger sig för att vara en potentiell köpare. I ett fall betalas en deposition mot utprovning

[18] Att man fått en faktura för en tjänst eller vara man inte beställt, vilket ofta är all information i ärendet, behöver inte utgöra ett fakturabedrägeri. Det kan exempelvis också handla om att bedragaren har använt anmälarens personuppgifter vid ett kreditköp, så att denne fick fakturan medan själva varan skickades till bedragaren. Den här typen av bedrägeribrottslighet beskrivs närmare under ***kreditbedrägerier***. Vid ett kreditbedrägeri kommer fakturan i regel från ett seriöst, etablerat företag. Vid fakturabedrägeri är det däremot snarare frågan om bedräglig företagsverksamhet. En närmare granskning av de företag som nämns i fakturabedrägeriärenden visade att dessa ofta fanns med på nätbaserade varningslistor som publiceras av Svensk Handel och Förenade Bolag. På så sätt kunde alltså fakturabedrägerier skiljas från kreditbedrägerier i det granskade materialet.

av vara, men resten av pengarna förs aldrig över. I ett annat fall ber köparen att få varan skickad till England mot uppvisande av ett falskt betalningskvitto. I det tredje fallet lovar bedragaren att förmedla försäljning av en husvagn åt målsägaren, skriver på ett uppdragskontrakt och försvinner sedan spårlöst.

Övriga brottsbalksbedrägerier

Bland övriga bedrägerier mot BrB 9 kap. (23 procent) ingår händelser som vare sig präglas av försäljning eller köp, lån och uttag. Kategorin domineras av vad Brå valt att kalla *övriga telefon- och internetbedrägerier* (15,5 procent). Det rör sig om bland annat så kallat nätfiske eller bedrägerier som kan genomföras med hjälp av diverse former av skadlig kod. Hit hör också de så kallade romansbedrägerierna och även mejlbedrägerier, till exempel där gärningspersonen låtsas vara en vän till den utsatte som är i en utsatt situation och i behov av pengar.

En annan kategori präglad av simpla upplägg och fysisk kontakt mellan bedragaren och den utsatte valde vi att kalla för *butiksbedrägerier* (2 %). Den gemensamma nämnaren är att gärningspersonen är närvarande i en butik och exempelvis försöker få igenom ett falskt återköp, luras med växel eller falska sedlar eller använder falsk pant. Det förekom även i två fall att gärningspersonen bröt upp förpackningar och omplacerade varan för att få den till ett billigare pris.

Den sista kategorin av *annat bedrägeri enligt BrB 9 kap*. (6 %) består av enstaka bedrägeribrott som inte ryms under den övergripande typologin. Dels har det med udda upplägg, dels med ett lågt antal att göra. Här finns exempelvis enbart ett ärende gällande ett *försäkringsbedrägeri*, något som visserligen utifrån sitt innehåll kan förtjäna en egen kategori och utrymme i analysen. Det låter sig dock inte göras på grund av det låga antalet.[19] Den som vill veta mer om försäkringsbedrägerier hänvisas till Brås rapport 2015:19, där dessa bedrägerier behandlas särskilt.

I kategorin ”annat bedrägeri” finns även två fall av bruk av falska registreringsskyltar och feladresserade p-böter, två fall av uteblivna löner samt två fall av pengaöverföring där de inblandade kände till varandra och gärningspersonen kom över målsägarens kontouppgifter och bankdosa. Vidare finns här två fall av bidragsbrott under felaktig brottskod samt ett antal ärenden

[19] Då typologin bygger på ett urval av polisanmälda ärenden, kan vissa mer sällsynta typer av bedrägerier inte alls vara representerade (även om de i vissa fall motsvaras av en specifik brottskod). Ett exempel är de så kallade investeringsbedrägerierna. Den framtagna typologin är dock avsedd att utgöra ett verktyg för att mer övergripande beskriva det stora antalet olika slags modus som är aktuella när det gäller bedrägeribrottsligheten.

som egentligen inte är brott utan missförstånd som tidigt reds ut alternativt snarare motsvarar civilrättsliga tvister, eller är ett annat brott än bedrägeri (vanligtvis stöld, skattebrott, avtalsbrott/uteblivna löner m.m. – dock initialt i utredningen rubricerat som bedrägeri). I kategorin annat bedrägeri ingår även ett fall av lån av bekant utan återbetalning. Det rör sig alltså om lån mellan två privatpersoner, varför brottet inte har kategoriserats som bedrägligt köp, lån eller uttag (som avser främst köp- och säljrelaterade händelser).

Tabell 6. Typer av brottsbalksbedrägerier i Brås ärendegranskning (anmälda brott). Antal och procent.

	Antal	Procent
Bedräglig försäljning		
Annonsbedrägeri	62	15,5
Fakturabedrägeri	49	12,3
Annan bedräglig försäljning	20	5,0
Bedrägliga köp, lån eller uttag		
Kortbedrägeri	87	21,8
Kreditbedrägeri	68	17,0
Annat bedrägligt köp/lån/uttag	18	4,5
Övriga brottsbalksbedrägerier		
Övriga telefon- och internetbedrägerier	62	15,5
Butiksbedrägeri	9	2,3
Annat bedrägeri enligt BrB 9 kap.	25	6,3
Totalt	**400**	**100,0**

Bidragsbrott och andra välfärdsbedrägerier

Som nämnts i metoddelen drogs också ett särskilt urval bland anmälda ärenden om brott mot bidragsbrottslagen. Det är främst Försäkringskassan, arbetslöshetskassorna och kommunerna som anmäler sådana brott. Den gemensamma nämnaren är att en sökande lämnat felaktig information för att få ett för högt bidrag eller annan utbetalning från välfärdssystemen. I vissa fall har det handlat om att den sökande inte underrättat den utbetalande myndigheten eller organisationen om ändrade förhållanden, vilket fått samma konsekvens – för mycket utbetalt.

I denna typ av bedrägerier ingår också för enkelhetens skull de brottsbalksbedrägerier som riktar sig mot samma utbetalande myndigheter. Några av dessa är för ovanliga för att ha dykt upp i Brås begränsade urval av anmälda brottsbalksbedrägerier – men beskrivs i avsnittet om bidragsbrotten på basis av intervjumaterial och tidigare studier. Det handlar framför allt om bedrägerier som företag begår mot exempelvis Arbetsförmedlingen.

Fördjupning i sex huvudkategorier av bedrägeribrott

Efter den övergripande beskrivningen ovan ägnas resten av den här delen av rapporten åt en fördjupad redovisning som börjar med de fem kategorier av brottsbalksbedrägerier som är någorlunda homogena till sitt innehåll och som var och en utgör en relativt stor andel. Tillsammans motsvarar dessa fem kategorier 82 procent av de ärenden som ingår i Brås urval av brottsbalksbedrägerier.

I ett sjätte avsnitt redovisas en mer fördjupad bild av de ärenden som ingår i Brås särskilda urval av brott mot bidragsbrottslagen från första halvåret 2013.

1. Annonsbedrägerier
2. Fakturabedrägerier
3. Kortbedrägerier
4. Kreditbedrägerier
5. Övriga telefon- och internetbedrägerier
6. Bidragsbrott och andra välfärdsbedrägerier

De olika avsnitten disponeras på så sätt att varje del inleds med en beskrivning av typiska tillvägagångssätt – så som de gestaltar sig i Brås samlade empiriska material samt i litteraturen. Därefter redovisas vilka de inblandade är – oftast i termer av anmälare (dvs. oftast den utsatte[20]), medan det inte alltid framkommer vilka som pekats ut eller misstänks för brottet vid tiden för anmälan. Sedan beskrivs hur rättsväsendet hanterar bedrägeriärendena av respektive typ – hur många som klaras upp, vilka utredningssvårigheter som finns och hur eventuella nedläggningar motiveras. Slutligen redogörs för vad som händer efter åtalet. Här granskas de insamlade domarna för att ge en bild av hur respektive bedrägerityp hanteras i rätten, bland annat vilken bevisning som åberopas och vilka motiveringar som anges när åtal för bedrägeribrott ogillas.

[20] Anmälare är i de flesta fall även målsägare i ärendena, men det finns undantag då en annan än den utsatte har anmält.

Annonsbedrägerier

Gärningspersonen vilseleder en intresserad köpare genom att på en annonssida på internet erbjuda en önskad vara/tjänst till försäljning/uthyrning. Varan/tjänsten betalas, men leveransen uteblir.

Sammanlagt 16 procent av anmälningarna i ärendegranskningen av brottsbalksbedrägerier är annonsbedrägerier (62 anmälningar).[21]

Typiska tillvägagångssätt: ofta simpla upplägg

Annonsbedrägerier följer i regel ett mycket enkelt upplägg som inte kräver någon mer omfattande förberedelse av bedragaren. Gärningspersonen lägger ut en vara eller tjänst till försäljning på en annonssajt på internet[22] där det finns många andra liknande annonser. Det karaktäristiska är att den bedragne blir vilseledd att betala i tron att den utannonserade varan eller tjänsten sedan kommer att levereras av annonsören. I själva verket har bedragaren ingen avsikt att leverera det som utlovats. När den bedragne har fört över pengar till annonsören upphör oftast kontakten och den förväntade leveransen uteblir.

Ett alternativt tillvägagångssätt är att bedragaren söker upp och svarar på så kallade köpesannonser, där potentiella köpare efter-

[21] Majoriteten av annonsbedrägerier i urvalet har polisen kodat som bedrägeri med hjälp av internet (42 ärenden). Vidare har 14 ärenden kodats som övrigt bedrägeri, 5 ärenden som datorbedrägeri och ett som fakturabedrägeri (se tabell 1B i bilaga 3).

[22] Bedräglig annonsförsäljning kan naturligtvis äga rum även utanför internet. Sannolikt är dock detta i dag relativt ovanligt. De granskade ärendena innehåller en del upplägg där annonser (på internet eller ej) kan ha använts som verktyg vid bedräglig försäljning utan att det tydligt framkommer i anmälan. Dessa kategoriserades som ”övrig bedräglig försäljning”. Det som här menas med annonsbedrägerier motsvarar en underkategori av vad som i internationell litteratur refereras till som *internet auction fraud* (Chua m.fl. 2007, Youngblood 2015). I dessa fall är alltså internet ett centralt brottsverktyg.

Det förekommer även, som nämnts i ett föregående kapitel, bedrägliga *köp* via annons. Detta är dock ett mindre vanligt upplägg och har kategoriserats som ”annat bedrägligt köp, lån eller uttag”.

lyser specifika varor eller tjänster. I dessa fall hävdar bedragaren att han eller hon har en sådan vara eller tjänst till försäljning. Därefter är tillvägagångssättet detsamma – köparen uppmanas att betala i förskott, bedragaren tar emot pengarna och varan eller tjänsten levereras inte.

Enskilda brott rör låga värden – men ofta upprepad brottslighet

Enligt de granskade ärendena har annonsbedrägerierna skett både via generella köp och sälj-sidor som E-bay, Blocket eller Tradera och via mer nischade sidor, som bland annat inriktar sig på uthyrning av andrahandslägenheter eller semesterhem.

Den enskilt vanligaste kategorin av varor är mobiltelefoner (cirka en femtedel) och annan elektronik (6 ärenden), se tabell 7. Den näst största kategorin avser försäljning av kläder, skor och diverse accessoarer (10 ärenden). I övrigt finns det en stor spridning avseende varorna eller tjänsterna – det gäller allt från konsertbiljetter till möbler, böcker och verktyg. Sju av anmälningarna avser annonser om lägenhetsuthyrning och en anmälan avser en annons för uthyrning av ett semesterhus.

Tabell 7. Typ av varor och tjänster vid annonsbedrägerier. Polisanmälda ärenden första halvåret 2013.

	Antal	Procent
Mobiltelefoner	13	21
Annan elektronik	6	10
Kläder, skor eller liknande	10	16
Lägenhetsuthyrning	7	11
Annat (biljetter, böcker, möbler, verktyg m.m.)	26	42
Totalt	**62**	**100**

Det är sällan några större summor som bedragarna lurat till sig genom de enskilda brotten. I en tredjedel av ärendena är beloppet lägre än 1 000 kronor, och medianvärdet motsvarar drygt 1 700 kronor. Beloppen är vanligtvis lite högre när det gäller anmälningarna som avser lägenhetsuthyrning, där medianbeloppet på förskottsbetalningarna ligger på närmare 6 000 kronor. Det finns enbart fem ärenden bland de anmälda annonsbedrägerierna där summan är högre än 10 000 kronor, och i dessa fall avser annonserna försäljning av ett fordon eller någon form av industrivara.

Även om de enskilda anmälningarna om annonsbedrägeri oftast avser relativt små belopp, visar det insamlade förundersökningsmaterialet att anmälningarna ofta har samordnats i utredningar som kan avse en längre serie av annonsbedrägerier som begåtts

av samma gärningsperson. Det innebär att den totala brottsvinsten för bedragaren kan bli relativt stor över tid, i vissa fall motsvarande miljonbelopp – enligt de granskade domarna.

Vilka är de inblandade?

Oförsiktiga gärningspersoner använder sitt eget bankkonto

I en del ärenden framgår att köparen har ombetts att föra över förskottsbetalningen med hjälp av en viss betaltjänst (t.ex. Paypal, Payson eller Internetgiro). I de flesta ärenden har köparen däremot ombetts föra över förskottsbetalningen direkt till ett visst bankkonto, oftast gärningspersonens. I vissa ärenden framgår däremot att bedragaren har förmått andra personer, så kallade målvakter, att upplåta sina bankkonton för inbetalningarna, så att pengarna inte går direkt till gärningspersonen.

I många av de polisanmälda annonsbedrägerierna har gärningspersonen även använt sitt eget namn vid annonseringen. I cirka en tredjedel av ärendena har gärningspersonen däremot använt sig av en annan persons namn och adressuppgifter vid själva annonseringen. Ibland har gärningspersonen även använt sig av en helt påhittad identitet. I vissa fall motsvarar dessa uppgifter en riktig persons namn och adress, som gärningspersonen till exempel tagit del av via någon form av söktjänst på internet. I enstaka ärenden framgår att gärningspersonen har gjort intrång i anmälarens e-postkonto och använt det för att lägga upp annonser.

I sju ärenden gällande annonsbedrägerier framkom tydligt att gärningspersonen hade problem med missbruk eller psykisk ohälsa, alternativt befann sig i en i övrigt kaotisk livssituation. Det är en större andel än vid andra bedrägerityper. På det hela taget kan det konstateras att bedragare som använder sig av annonsförsäljning ofta är personer i akut behov av snabba pengar; de bryr sig sällan om konsekvenserna som brottet kan medföra. Det skapar relativt goda förutsättningar för uppklaring.

Anmäls av privatpersoner när brotten fullbordas

Det är i regel de utsatta som själva anmält brotten till polisen. Givet vad som framgår av ärendena har de anmält brotten i egenskap av privatpersoner snarare än som exempelvis representanter för ett företag eller någon annan form av organisation. Könsfördelningen bland dem som anmält brotten till polisen är mycket jämn. I 80 procent av ärendena framgår en uppgift om anmälarens ålder, som varierar mellan 16 och över 90 år. Närmare åtta av tio anmälare är under 50, och medianåldern är 35 år.

Närmare 90 procent av de anmälda annonsbedrägerierna avser brott som har fullbordats genom att den utsatte har fört över pengar till annonsören. I de allra flesta av dessa ärenden har anmälan gjorts på grund av att den utannonserade varan eller tjänsten inte har levererats efter att betalningen gjorts. I vissa ärenden framgår dock att en vara faktiskt har skickats och tagits emot av anmälaren. I dessa fall kan anmälningarna bero på att den levererade varan inte ansågs motsvara den som beskrivits i annonsen. Till exempel har annonsören skickat en mobil av fel modell eller kläder som var trasiga. I vissa ärenden finns en misstanke om att annonsören har sålt och levererat en vara som egentligen inte tillhört honom eller henne. Anmälan kan till exempel handla om att annonsören har gjort sig oanträffbar efter att ha levererat en bil till anmälaren, dock utan att ha lämnat över ett ägarbevis.

I de ärenden där inga pengar har överförts kan polisanmälan bland annat handla om att anmälaren har fått ett brev från en annonssida om att någon har öppnat ett konto i hans eller hennes namn.

Även annonsörer är oftast privatpersoner, enligt informationen i ärendena. Samtidigt finns enstaka anmälningar där annonsören har beskrivit sig som ett företag som säljer via olika annonssidor på nätet.

När rättsväsendet tar vid

Drygt ett av fyra har klarats upp

Sammanlagt 27 procent av de anmälda annonsbedrägerier som granskats här har lett till ett personuppklaringsbeslut.[23] Det innebär en hög personuppklaring, om man jämför med samtliga anmälda brottsbalksbedrägerier i samma urval, som motsvarar 8 procent. De flesta av annonsbedrägerierna hade personuppklarats genom ett beslut om att väcka åtal (se tabell 8).

Utöver de anmälningar om annonsbedrägeri som blivit personuppklarade var 8 procent fortfarande under utredning i slutet av 2014. Av misstankeregistret framgår att de öppna ärendena, med ett undantag, ingår i utredningar där det finns ett flertal öppna brottsmisstankar, och det framstår som sannolikt att åtminstone de flesta av dessa utredningar så småningom också kommer att leda till åtal.

Drygt en av tio anmälningar om annonsbedrägeri har lagts ner genom ett beslut om så kallad förundersökningsbegränsning. Här

[23] Studieperioden sträcker sig fram till slutet av 2014 (den sista punkt där det funnits information tillgänglig om eventuella uppklarings- eller nedläggningsbeslut från Brås statistikregister).

har den misstänkte gärningspersonen antingen redan tidigare blivit dömd för brott eller kommer att åtalas för annan brottslighet. I båda situationerna innebär beslutet att den misstänkte gärningspersonen antingen redan fått eller kommer att få en påföljd som anses tillräcklig för att omfatta även det aktuella brottet.

Tabell 8. Personuppklaringsbeslut, ärenden fortfarande under utredning och nedlagda ärenden efter nedläggningsorsak. Annonsbedrägerier. (n = 62)

	Antal	Procent
Personuppklarade ärenden	**17**	**27**
Åtal	16	26
Åtalsunderlåtelse	1	2
Fortfarande under utredning 2014-12-31	**5**	**8**
Nedlagda ärenden*	**40**	**65**
Ej brott/Anmälan inte längre aktuell	10	16
Ej utredningsbart	10	16
Spanings-/bevisproblem (ingen misstänkt identifierad)	6	10
Bevisproblem (misstänkt identifierad)	4	6
Misstänkt lämnat landet	1	2
Förundersökningsbegränsning	8	13
Oklart	1	2
Totalt	**62**	**100**

* För en beskrivning av hur nedläggningsbesluten har kodats, se bilaga 2.

Bankkonton ger ett säkert spår att följa

Bilden av att annonsbedrägerier kännetecknas av jämförelsevisa goda uppklaringsmöjligheter får ytterligare bekräftelse i intervjuer med poliser och åklagare. Bland annat framgick att man i dessa ärenden oftast har ett säkert spår att följa i form av ett kontonummer dit anmälaren har fört över pengar till annonsören. Genom att begära ut kontoutdrag kan man också styrka att de belopp som målsägaren har betalat har förts över till annonsörens konto vid aktuella datum, vilket gör det möjligt att knyta gärningspersonen till enskilda brottstillfällen i en längre brottsserie.

Då annonsbedrägerier ofta sker just i form av brottsserier, ger kontonumret också goda möjligheter att samordna anmälningar som avser olika annonsbedrägerier från samma brottsserie. Intervjuade poliser har berättat att man i vissa fall också använder kontoutdrag från gärningspersonens bankkonto för att identifiera ytterligare brottsoffer som valt att inte göra en polisanmälan.

Nedläggning beror ofta på att konflikten mellan annonsör och anmälare är löst

En vanlig anledning för att annonsbedrägerier läggs ner är att den anmälda händelsen inte anses vara ett brott eller att anmälan inte längre är aktuell. I flera av ärendena har exempelvis de köpta varorna, som vid anmälningstillfället inte hade levererats, dykt upp efter ett tag, eller så har annonsören gått med på att lämna tillbaka köparens pengar.

Lika vanligt är att polisen har lagt ner ärendet med motiveringen att brottet inte går att utreda. Det handlar till exempel om ärenden där målsägare köpt varor som inte levererats från annonsörer utomlands och där betalningen skett till ett utländskt konto. Här finns också några ärenden där tillgängliga spaningsuppslag har ansetts vara otillräckliga.

I kategorierna spanings- och bevissvårigheter ingår anmälningar som lagts ner antingen med motiveringen att man inte lyckats identifiera gärningspersonen trots att försök har gjorts eller med en hänvisning till bevisproblem, till exempel att det inte går att styrka att gärningspersonen haft brottsligt uppsåt.

Svårt att styrka brott vid en enskild anmälan

Enligt intervjupersoner inom rättsväsendet kan det vara svårt att styrka enskilda annonsbedrägeribrott om anmälaren hävdar att hon eller han har betalt annonsören för en vara som sedan inte levererats, medan annonsören hävdar att varan faktiskt har skickats. När det handlar om brottsserier där ett flertal liknande ärenden har samordnats framstår däremot annonsörens påståenden som mindre trovärdiga; det kan anses orimligt att varorna skulle ha försvunnit under postens hantering i ett flertal liknande fall.

Penningtvättsbrott används som alternativ brottsrubricering

Ytterligare en utredningssvårighet kan uppstå om misstänkta gärningspersoner hävdar att de inte har lagt ut de aktuella annonserna och att de inte heller vet var de pengar som överförts till deras bankkonton kommit ifrån. Enligt intervjupersoner inom rättsväsendet är det ibland inte möjligt att knyta en misstänkt person till själva annonserna. Det kan exempelvis visa sig att annonserna har lagts upp från en IP-adress som inte går att spåra till en fysisk adress.

Även om det saknas andra uppgifter i utredningen som knyter gärningspersonen till själva annonserna, menar intervjuade poliser att det i många fall ändå går att väcka åtal genom penning-

tvättsbrott (tidigare penninghäleri).[24] Enligt intervjuade poliser och åklagare beror det på att gärningspersonen rimligen borde ha insett att de pengar som hamnat på hans eller hennes bankkonto härrör från brottslig verksamhet. Straffskalorna för de två brotten är likvärdiga. Mot bakgrund av detta har flera intervjupersoner också förklarat att om det finns bra bevisning i form av kontoutdrag och vittnesmål från målsägare är det ofta mer rimligt ur ett utredningsekonomiskt perspektiv att i stället väcka åtal för penningtvättsbrottet, eller att använda penningtvättsbrottet som en alternativ brottsrubricering vid ett åtal för bedrägeri än att lägga ner ytterligare resurser på att knyta gärningspersonen till annonserna.

När åtal väckts

Stor variation i antalet brottstillfällen i domarna

Brås särskilda urval av bedrägeridomar innehåller 49 domar som avser annonsbedrägerier. De flesta domar avser en enda tilltalad gärningsperson, och endast ett mål avser fler än tre tilltalade personer. Totalt sett avser domarna 60 gärningspersoner som åtalats för annonsbedrägerier, av vilka 70 procent var män, 30 procent kvinnor.

Den bevisning som åberopats i domstolen är oftast relativt okomplicerad. Vanligtvis handlar det om ett förhör med den tilltalade (som ofta erkänner), förhör med målsägare samt kontoutdrag som styrker att pengarna har förts över från målsägarna till den tilltalades bankkonto.

I hälften av de insamlade annonsbedrägeridomarna avser åtalet mellan 1 och 15 bedrägeritillfällen och i ytterligare en fjärdedel avser åtalet mellan 16 och 30 brottstillfällen. Samtidigt avser drygt en av tio domar över 100 bedrägeribrott.

Det finns även stor variation i värdet på den bedrägeribrottslighet som åtalen avser, delvis beroende på antalet brottstillfällen, delvis beroende på vad det är för typ av varor eller tjänster som annonserna avsett. Summorna vid de fullbordade brotten i annonsbedrägeridomarna varierar mellan som minst 400 kronor och som mest över en miljon. I trettio procent av domarna avser åtalet fullbordade bedrägerier till ett värde av över 100 000 kronor, och medianbeloppet för samtliga 49 domar ligger på ca 40 000 kronor.

[24] Fram till den 30 juni 2014 dömdes bland annat den som otillbörligen främjar möjligheterna för annan att tillgodogöra sig egendom som härrör från brottsligt förvärv för penninghäleri. Bestämmelsen om penninghäleri utmönstrades ur brottsbalken den 1 juli 2014, då den nya lagen (2014:307) om straff för penningtvättsbrott trädde i kraft.

Enstaka mål av mer organiserade bedrägerier

Det finns några exempel på domar som visar tecken på betydligt högre grad av organisering än de övriga annonsbedrägerimålen. Ett exempel är ett mål där åtal väckts mot ett flertal personer som sålde förfalskade konsertbiljetter via flera olika annonssidor. Gärningspersonerna hade också använt sig av ett företag, där en av de tilltalade satt i styrelsen för att köpa den utrustning som användes vid tillverkningen av de förfalskade biljetterna.

I ett annat mål hade den tilltalade anlitat ett större antal personer som så kallade försäljningsombud och fått dem att upplåta sina bankkonton för inbetalningar från annonsbedrägerier. Brotten hade pågått i flera år. Dessa ombud hade sedan skickat pengarna vidare till huvudgärningspersonen, som befann sig utomlands. Det framgår också av domen att en del av de anlitade försäljningsombuden hade blivit åtalade och dömda i separata rättegångar.

I ett tredje mål hade gärningspersonen blivit åtalad både för annonsbedrägerier och för delaktighet i fakturabedrägerier som bedrivits av ett företag där gärningspersonen ingick i styrelsen.

En tiondel frias

Av de 60 personer som åtalats för annonsbedrägerier i de insamlade domarna har en tiondel friats i tingsrätten. I enstaka fall har domstolen menat att det funnits visst tvivel om huruvida den tilltalade ändå inte haft för avsikt att leverera varorna. I andra ärenden har det inte funnits någon bevisning som knutit den tilltalade till annonserna, och det har av olika anledningar inte ansetts styrkt att den tilltalade ska ha insett att de aktuella kontoinbetalningarna härrörde från annonsbedrägerierna.

De övriga tilltalade har i de flesta fall blivit dömda för bedrägeri eller i vissa fall för grovt bedrägeri. I några av domarna har de tilltalade i stället dömts för penninghäleri, och i enstaka fall för medhjälp till bedrägeri. I flera av målen har en del åtalspunkter inte vunnit bifall, även om gärningspersonen i fråga har dömts enligt andra av åtalspunkterna. I mål med mer än en tilltalad kan det exempelvis handla om att den ene av de tilltalade menar att det finns vissa bedrägeritillfällen i serien där hon eller han inte deltagit i annonseringen eller i kontakterna med köparna. Eftersom pengarna i dessa fall inte har förts över till just den tilltalades konto har domstolen menat att den tilltalades delaktighet i dessa brott inte kan anses vara styrkt.

Fakturabedrägerier

Målsägaren vilseleds att betala en faktura för en vara eller en tjänst som han eller hon inte har beställt. Alternativt vilseleds målsägaren att betala en faktura gällande en annan summa eller utifrån andra villkor än vad som tidigare avtalats.

I det granskade urvalet av anmälda brottsbalksbedrägerier fanns sammanlagt 49 anmälningar som har kategoriserats som fakturabedrägerier (12 procent av urvalet).[25]

Typiska tillvägagångssätt: två huvudmodus

Grunden i ett fakturabedrägeri är att bedragaren vilseleder den utsatte att betala en faktura som inte motsvarar någon faktisk skuld.[26] Det kan till exempel handla om fakturor som avser varor eller tjänster som mottagaren aldrig beställt eller som inte levererats, eller där det fakturerade beloppet inte står i rimlig proportion till den levererade varan eller tjänsten. Jämfört med flera av de andra bedrägerityperna har fakturabedrägerier varit föremål för relativt mycket uppmärksamhet från politiskt håll under senare år. Ett tydligt exempel på det är inte minst regeringens tillsättning av Fakturabedrägeriutredningen (SOU 2015:77, se även bilaga 1).

Både enligt utredningen och Brås ärendegranskning följer fakturabedrägerier oftast ett av två grundläggande upplägg: *bluffakturor* och *fakturabedrägerier efter kontakt*.

1. Bluffakturor: ofta upplägg med kapad faktura

Bluffakturor är en beteckning för flera olika typer av bedrägliga fakturor, som skickas till mottagare utan att dessa tidigare haft

[25] De flesta granskade fakturabedrägerier (41 ärenden) har av polisen kodats som just fakturabedrägeri, men 6 ärenden kodades som övrigt bedrägeri och 2 ärenden som automatmissbruk (se tabell 1B i bilaga 3).

[26] Jfr SOU 2015:77, s. 41.

någon kontakt med avsändaren. Sammanlagt 15 granskade ärenden var av denna typ.

Fakturabedrägeriutredningen särskiljer tre typer av bluffakturor: bluffakturor från okända leverantörer, kapade fakturor och erbjudandefakturor. Med *bluffakturor* från okända leverantörer avses framför allt fall där bedragaren skickar en faktura i hopp om att mottagaren helt enkelt ska betala den utan att lägga märke till att fakturan kommer från någon som mottagaren inte har något avtal med. Tillvägagångssättet vid *kapade fakturor* är att bedragaren skickar ut fakturor som framställts så att de liknar en faktura från en känd leverantör, alternativt bokstavligen kapar en riktig faktura och ändrar kontot dit pengarna ska betalas. *Erbjudandefakturor* avser erbjudanden som är utformade som fakturor och där det kan vara svårt att upptäcka att det egentligen bara är fråga om ett erbjudande, och därmed inget som behöver betalas.

Bland de granskade ärendena gällande bluffakturorna finns ett flertal exempel på så kallade kapade fakturor (8 ärenden), se tabell 9. De flesta av dessa anmälningar hör till en enda utredning, där gärningspersonerna, sannolikt genom dataintrång, har kommit över uppgifter om kunder och faktureringsbelopp tillhörande ett seriöst företag. Gärningspersonerna har sedan med hjälp av denna information skickat ut till synes riktiga fakturor till en stor grupp av företagets kunder. En av anmälningarna avser en betydligt mindre avancerad typ av kapad faktura. Anmälaren hade i detta fall fått hem en faktura efter en sjukhusvistelse. Det ursprungliga bankgironumret hade täckts över med tipp-ex och ett nytt kontonummer skrivits in för hand.

Tabell 9. Olika typer av fakturabedrägerier. Polisanmälda ärenden första halvåret 2013.

	Antal	Procent
Bluffaktura	**15**	**31**
Kapad	(8)	(16)
Annat/oklart (okända leverantörer, erbjudandefakturor m.m.)	(7)	(14)
Efter kontakt	**34**	**69**
Telefonförsäljning	(25)	(51)
Annat	(9)	(18)
Totalt	**49**	**100**

Vid de övriga bluffakturorna i ärendegranskningen är det svårt att göra en distinktion mellan det som fakturabedrägeriutredningen betecknar som erbjudandefakturor respektive fakturor från okända leverantörer. Fakturorna har oftast skickats till företag eller andra organisationer och avser någon form av internet-

tjänst. Det handlar till exempel om fakturor för internetannonser eller ett domännamn som fakturamottagaren inte har beställt.

Bluffakturorna har oftast skickats i form av pappersfakturor eller i enstaka fall via e-post, de flesta från avsändare i Sverige. I enstaka fall har avsändaradressen varit till ett företag i ett annat land i Europa.

2. Fakturabedrägerier efter kontakt: ofta telefonförsäljning

Fakturabedrägerier efter kontakt avser bedrägliga fakturor som skickas efter att det skett, eller där bedragaren påstår att det skett, en tidigare kontakt mellan fakturans avsändare och mottagare. Kontakten ska enligt avsändaren ha resulterat i ett avtal dem emellan.[27]

Totalt 34 av de granskade ärendena avsåg ett fakturabedrägeri efter kontakt. Fakturan avsåg i många fall någon form av påstådd internettjänst som fakturaavsändaren ska ha utfört åt mottagaren. Tjänsten ska ha gått ut på att göra mottagarföretaget mer synligt på nätet. Det handlar oftast om tjänster som påstås innebära en fördelaktig positionering för företaget när potentiella kunder gör google-sökningar eller någon annan form av annonsering på internet.

I de flesta fall (25 ärenden) har fakturan skickats ut efter det att mottagaren först blivit kontaktad av en telefonförsäljare som arbetar åt gärningspersonernas företag. Det vanligaste upplägget som framgår i ärendegranskningen är att telefonförsäljaren ringer målsägaren och hävdar att det under en tid funnits ett avtal mellan gärningspersonernas företag och målsägaren och att det nu har blivit dags att antingen förnya tjänsten eller avsluta avtalet. Målsägaren har dessutom inte sällan informerats om att de båda alternativen – förlängning eller uppsägning – innebär en avgift som denne måste betala. Därefter skickas en faktura. I ärenden framgår oftast att det i själva verket aldrig funnits ett avtal. I vissa ärenden finns uppgifter om att en inspelning av samtalet mellan telefonförsäljaren och målsägaren först har manipulerats för att få det att låta som att målsägaren har tackat ja till förlängning. I en del av ärendena har anmälarna beskrivit att gärningspersonerna har hotat dem med Kronofogden om de inte betalar.

En del av fakturabedrägerierna efter kontakt avser ärenden där företag eller företagare har kontaktats via post eller e-post med

[27] Enligt Fakturabedrägeriutredningens betänkande kan det handla både om fall där påståendet om ett ingånget avtal är helt grundlöst och fall där fakturamottagaren blivit vilseledd eller pressad till att ingå ett avtal med avsändaren. I de fall där det funnits en kontakt mellan fakturans avsändare och mottagare innan fakturan skickas kan det till exempel ske via telefonförsäljare, e-post eller pappersbrev.

ett erbjudande om att ingå i en nätbaserad branschkatalog eller om att lägga till ytterligare information om sig själva på en nätbaserad nummerupplysningstjänst. Ibland skickas e-post där mottagaren ombes att svara OK med vändande post om erbjudandet avböjs. Den ursprungliga e-posten innehåller emellertid en bifogad fil som utgör en offert och efter att mottagaren svarat OK faktureras denne för den påstådda tjänsten.

Kontakterna via papperspost följer ett liknande upplägg. Mottagarna får exempelvis en blankett där de uppmanas att fylla i och komplettera uppgifterna om sitt företag till en nummerupplysningstjänst och skicka tillbaka. På blanketten kan det stå att det handlar om ett erbjudande samt att det är gratis att lägga till ytterligare information i framtiden, men i det finstilta på exempelvis blankettens baksida står att om man skickar tillbaka den ifyllda blanketten så innebär det en kostnad för inskickaren. Därefter kommer en faktura.

Bedräglig försäljning av telefonabonnemang till äldre

I de ärenden som avser fakturabedrägerier efter kontakt där anmälaren är en privatperson snarare än ett företag avser anmälan oftast en faktura om någon form av telefonabonnemang. I dessa ärenden är målsägarna framför allt äldre personer, och även här har fakturan skickats efter att målsägaren först blivit uppringd av en telefonförsäljare. I vissa ärenden har telefonförsäljaren hävdat att hon eller han jobbar åt en välkänd teleoperatör och därefter lurat målsägaren att ingå ett nytt avtal, som sedan visat sig vara ett avtal med ett helt annat företag, som telefonförsäljaren egentligen representerar. Det förekommer att försäljaren förhandlar om kostnaden för abonnemanget efter det att målsägaren först tackat nej. När fakturan sedan kommer, gäller den en högre summa än vad som avtalats via telefon. De villkor som anmälaren gått med på under telefonsamtalet kan ha ändrats även på andra sätt när fakturan skickas ut, till exempel avseende abonnemangets bindningstid.

Tre av anmälningarna i urvalet, som också drabbat privatpersoner, avser ett särskilt upplägg där gärningspersonerna har skickat hotfulla brev med krav på att mottagaren ska betala skadestånd för ett upphovsrättsintrång. I dessa brev hävdar avsändaren att brevmottagarna har laddat ner upphovsrättsskyddat filmmaterial från en internetsajt i strid med ett påstått avtal, som de utsatta ansetts ha godkänt då de tryckt på en OK-knapp för att komma in på sidan.[28]

[28] Liksom vid bluffakturor har även dessa fakturor som föregicks av en slags kontakt oftast skickats inom Sverige av företag med svensk hemvist. I vissa fall framgår dock att företaget har sin hemvist i ett annat europeiskt land.

Fakturabedrägerier efter kontakt anmäls oftare än bluffakturor

Fakturabedrägeriutredningen (SOU 2015:77) gjorde en kartläggning av utsattheten för fakturabedrägerier i form av stora frågeundersökningar bland privatpersoner, företag samt statliga och kommunala myndigheter. I denna kartläggning var storleksordningen den motsatta när det gäller andelen bluffakturor respektive fakturabedrägerier efter kontakt; enligt enkätresultaten utsattes både privatpersoner, företag och förvaltningsmyndigheter oftare för bluffakturor än fakturabedrägerier efter kontakt. Mot bakgrund av Brås kartläggning av polisanmälda ärenden innebär det rimligtvis att fakturabedrägerier efter kontakt polisanmäls i en större utsträckning. En förklaring kan vara att bluffakturor, enligt ett av utredningens resultat, oftare slutar med ett försök; mottagaren betalar ej och ser heller ingen vinst i att anmäla händelsen till polisen. Det kan även tänkas att graden av kränkning blir större när den drabbade blivit vilseledd eller utsatt för försök till det, genom en direkt personlig kontakt – något som också kan bidra till benägenheten att anmäla.

Totalt sett är det ändå relativt många av de fakturabedrägerier som anmälts till polisen som har stannat vid ett försöksbrott.[29] I 65 procent av de granskade ärendena framgår att anmälaren inte har betalat fakturan (32 anmälningar). I närmare 30 procent av de anmälda fakturabedrägeriärendena (14 anmälningar) framgår att fakturan hade betalats, medan det i de övriga tre ärendena är oklart om någon betalning ägt rum.

Vilka är de inblandade?

Gärningspersonerna använder oftast företag

Enligt intervjupersonerna begås fakturabedrägerier oftast med hjälp av företag. Det beror bland annat på att storskaliga fakturabedrägerier kräver ett företagskonto för inbetalning av pengarna. Enligt intervjuade experter finns det kända konstellationer av gärningspersoner som flyttar sina fakturabedrägeriverksamheter mellan olika företag. Samtidigt som det ena företaget sätts i konkurs registreras ett nytt, med samma eller nya målvakter i styrelsen. Bedrägerimoduset i det nya företaget kan bli i stort sett likadant, eller kan utvecklas lite, och så småningom sätts även detta bolag i konkurs för att ett nytt återigen ska startas.

[29] Samtidigt är försök till fakturabedrägeri sannolikt fortfarande kraftigt underrepresenterade bland polisanmälningar. Andelen fullbordade brott är överlag högre här än i Fakturabedrägeriutredningens frågeundersökning om utsatthet.

Enligt både poliser och andra experter finns vidare tydliga tecken på att en del av de gärningspersoner som legat bakom fakturabedrägerier i Sverige numera har börjat rikta sitt fokus utåt, framför allt mot företag och företagare i andra länder.

Anmäls ofta av drabbade företagare

I en fjärdedel (12 ärenden) av de granskade fakturabedrägeriärendena framgår att den brottsdrabbade är en privatperson. Drygt 40 procent av fakturabedrägerianmälningarna (20 anmälningar) har gjorts av företagare eller av företagsanställda. I enstaka fall har anmälan gjorts av någon annan form av organisation, exempelvis en kommun eller bostadsrättsförening. Övriga anmälningar (närmare tre av tio) har upprättats av polisen under pågående fakturabedrägeriutredningar. I flera av de anmälningar som upprättats av polisen är det oklart huruvida den utsatte har drabbats i egenskap av privatperson eller som representant för ett företag.

Informationen om de utsattas ålder har ofta saknats i det insamlade materialet. I 10 av de 12 ärenden där det framgår att den brottsdrabbade är en privatperson är denne en man. Information om ålder saknas i två ärenden, men i de övriga är den drabbade över 50 år i åtta av de tio fallen. Medianåldern på utsatta privatpersoner är hög, 68 år.

De fakturerade beloppen varierar, med ett medianvärde på cirka 4 400 kronor. I 90 procent av de granskade ärendena avsåg fakturan en summa under 10 000 kronor. I fyra ärenden avsåg fakturan ett belopp på mellan 20 000 och 40 000 kronor.

När rättsväsendet tar vid

Totalt 14 procent av fakturabedrägerierna i urvalet av anmälda brott hade lett till ett personuppklaringsbeslut fram till slutet av 2014, samtliga i form av ett beslut att väcka åtal. Ytterligare 16 procent av anmälningarna var fortfarande under utredning i slutet av 2014. Nedläggningsorsakerna för de övriga anmälningarna om fakturabedrägeri redovisas i tabell 10.

De två vanligaste nedläggningsorsakerna är att man anser att det anmälda brottet inte går att utreda eller att ärendet har lagts ner med ett beslut om förundersökningsbegränsning.

Tabell 10. Personuppklaringsbeslut, ärenden fortfarande under utredning och nedlagda ärenden efter nedläggningsorsak. Fakturabedrägerier. (n = 49)

	Antal	Procent
Personuppklarade ärenden	**7**	**14**
Åtal	7	14
Fortfarande under utredning 2014-12-31	**8**	**16**
Nedlagda ärenden*	**34**	**69**
Ej brott	3	16
Ej utredningsbart	10	16
Spanings-/bevisproblem (ingen misstänkt identifierad)	6	10
Bevisproblem (misstänkt identifierad)	5	6
Förundersökningsbegränsning	9	13
Oklart	1	2
Totalt	**49**	**100**

*För en beskrivning av hur nedläggningsbesluten har kodats, se bilaga 2.

”Ej utredningsbara” ärenden med hänvisningar till civilrätt

I de ärenden som lagts ner med hänvisning till att brottet inte går att utreda har anmälaren oftast inte betalat fakturan. Några av dessa ärenden avser fakturor som har skickats till en svensk mottagare från utlandet och har lagts ner med en hänvisning till att brottet har begåtts utomlands och att det inte går att utreda av den anledningen.

I de andra ärendena med samma nedläggningsmotiv (dvs. ej utredningsbart) har polisen skrivit en anteckning om att det inte finns förutsättningar för att styrka brott eller att en förundersökning ej kan förväntas leda till åtal. Dessa ärenden handlar ofta om fakturor som skickats efter det att mottagaren kontaktats av en telefonförsäljare, och avsändaren hävdar att ett avtal har ingåtts. I flera fall har polisen skrivit en anteckning om att den anmälda händelsen anses vara av civil- eller konsumenträttslig karaktär samt att fakturan ska bestridas av anmälaren.

En del intervjuade åklagare, som får ta ställning till överklaganden av polisens nedläggningsbeslut, har menat att poliser ibland kan vara för snabba att lägga ner bedrägeriutredningar med hänvisningar till att den anmälda händelsen avser en civilrättslig tvist. Det intressanta, menar åklagarna, är i första hand inte huruvida ett avtal har ingåtts utan snarare huruvida det skett ett vilseledande i syfte att få anmälaren att föra över pengar till fakturaavsändaren. För att reda ut huruvida det skett ett bedrägeri krävs således utredningsåtgärder från polisens sida för att klargöra bakgrunden till det påstådda avtalet.

Nedlagda anmälningar ingår ofta i stora utredningar som lett till åtal

En majoritet av de ärenden som lagts ner genom beslut om förundersökningsbegränsning eller på grund av bevisproblem när en misstänkt person har identifierats har samordnats med stora utredningar om fakturabedrägeri, där det registrerats ett mycket stort antal (ibland flera tusen) brottsmisstankar i misstankeregistret. De flesta av dessa brottsmisstankar var fortfarande under utredning i slutet av 2014. Utdrag från misstankeregistret visar vidare att flera av de misstänkta gärningspersonerna i dessa ärenden också har varit under utredning av Ekobrottsmyndigheten för bokföringsbrott och skattebrott.

Överlag visar de anmälda fakturabedrägerierna att en okritisk tolkning av andelen nedlagda ärenden kan ge en missvisande bild av rättsväsendets utredningsprestation i dessa mål. Enligt uppgifter från misstankeregistret och intervjuer med poliser och åklagare avsåg drygt hälften av de granskade 42 anmälningarna som lagts ned eller som fortfarande var under utredning brott som begåtts inom stora fakturabedrägerihärvor. Dessa utredningar hade vid slutet av 2015 antingen redan lett till åtal eller ingick i mål där åtal så småningom sannolikt kommer att väckas.

Utredningar om fakturabedrägeri kräver mycket tid och resurser

Bland de största svårigheterna med fakturabedrägeriutredningar är deras stora omfattning i termer av dels det stora antalet brottstillfällen och målsägare, dels hur mycket bevisning som måste samlas in och sorteras upp för att kunna styrka de enskilda brottstillfällena i domstol. Detta är en av Egendomsskyddsutredningens slutsatser (SOU 2013:85) och har även tydligt framkommit i Brås intervjuer med polis och åklagare.

För att ta ett exempel måste man bevisa att det skett ett vilseledande i förhållande till varje målsägare som blivit vilseledd. Det innebär att varje målsägare måste förhöras om varje enskild faktura, och i förekommande fall om skälet till att hon eller han har betalat fakturan. Det kan handla om tusentals målsägare som är utspridda över hela landet. Detta kräver både ett stort samordningsarbete och resurser som kan göras tillgängliga för arbetet hos polisen på lokal nivå.

En annan stor utmaning för fakturabedrägeriutredningar enligt intervjupersonerna är att de rent juridiskt är mycket komplexa. Det beror bland annat på att svåra gränsdragningar aktualiseras avseende förhållandet mellan straffrättsliga bestämmelser och andra rättsliga områden. Denna komplexitet belyses åtminstone till viss del i de domar som samlats in och beskrivs nedan.

När åtal väckts

Endast en dom i Brås urval av bedrägeridomar avser fakturabedrägeribrott. Brå har därför kompletterat materialet genom att särskilt ha begärt in ytterligare tre domar som är kopplade till ärenden i urvalet av anmälda brott.[30] Syftet var att kunna ge en bättre bild av tingsrätternas hantering av olika typer av fakturabedrägerimål.

Ett ovanligt upplägg med kapad faktura

En av de fyra domar som granskats avser en ovanlig variant av det tidigare nämnda upplägget med kapad faktura. I det här fallet hade gärningspersonen genom datorintrång lyckats ta kontroll över pågående mejlkommunikationer avseende köp- och säljtransaktioner mellan företag i olika länder, och på så sätt fått information om de pågående transaktionerna. Därefter hade gärningspersonen skickat fakturamejl till flera olika köpare från en adress som skapades för att efterlikna säljbolagets. På detta sätt hade gärningspersonen lyckats styra över betalningen till ett bankkonto som gärningspersonen själv disponerade. Åtalet avsåg fullbordade fakturabedrägerier till ett värde av över en miljon kronor.

Enligt rätten fanns det ingen bevisning som direkt visade att det var den tilltalade som hade utfört själva bedrägerierna, då man inte hade hittat något spår av den aktuella mejltrafiken i dennes beslagtagna dator. Däremot var det utrett att den tilltalade hade upplåtit ett konto som använts för överföring av pengar från bedrägeribrotten, och den tilltalade dömdes för bland annat grovt penninghäleri.

Tingsrätternas hantering av andra typer av fakturabedrägerimål

De övriga tre domarna som Brå har begärt in avser ett massutskick avseende medlemskap i en nätbaserad branschkatalog, ett successivt utskick av kravbrev avseende skadestånd för upphovsrättsintrång och ett fakturabedrägeri avseende telefonförsäljning av en påstådd tjänst i form av en företagspresentation på nätet. Domarna avser mellan 400 och över 3 000 målsägare.

I massutskicksmålet var det relativt få fullbordade brott, då gärningspersonerna hade anlitat ett seriöst inkassobolag för att skicka ut fakturorna och utskicket hade avbrutits direkt när

[30] Dessa hade alltså hunnit igenom hela rättssystemet fram till andra halvåret 2015. Kontroller med aktuella tingsrätter har visat att det finns flera fakturabedrägeriutredningar i Brås material där åtalsbeslut har fattats under 2015, men där huvudförhandlingen i tingsrätten inte hade påbörjats vid årets slut.

inkassobolaget började få in klagomål från fakturamottagarna. Enligt tingsrätten var det klarlagt att fakturamottagarna inte hade ingått något avtal att betala för medlemskap i den aktuella branschkatalogen och de båda gärningspersonerna dömdes för bedrägeri och försök till grovt bedrägeri.

I de övriga två målen uppgick summorna vid de fullbordade brotten till drygt 2 miljoner respektive över 4 miljoner kronor. Bevisningsunderlaget i de båda målen var stort med bland annat resultat från omfattande it-forensiska analyser och i det ena fallet inspelade ljudfiler från telefonförsäljning och avlyssnade telefonsamtal mellan gärningspersonerna. Enligt domarna uppgick tingsrätternas handläggningstid i målen till mellan 3 och 6 månader. Detta kan jämföras med handläggningstiden i tingsrätten i de granskade annonsbedrägerimålen, där huvudförhandlingarna typiskt sett har pågått i mellan en och fyra timmar.

Åtal för utpressning i stället för bedrägeri

I målet som avsåg kravbreven efter ett påstått upphovsrättsintrång åtalades ett flertal personer, men för utpressning i stället för bedrägeri. Domen innehåller komplexa juridiska resonemang kring förhållandet mellan olika civilrättsliga, marknadsrättsliga och straffrättsliga aspekter av de åtalade gärningarna. En central fråga var i vilken mån innehållet i kravbreven kunde anses uppfylla rekvisitet om olaga tvång i utpressningsbestämmelsen. Enligt rätten kunde olika bedömningar göras i denna fråga, bland annat beroende på om de enskilda målsägarna själva ansåg att de hade ingått ett avtal. Eftersom många målsägare inte hördes under huvudförhandlingen menade rätten att det inte kunde uteslutas att dessa hade betalat kraven för att de ansåg sig vara bundna av ett avtal. Det resulterade i att delar av åtalet lämnades utan bifall. Enligt rättens bedömning var andra delar av åtalet däremot styrkta och samtliga tilltalade dömdes, bland annat för antingen utpressning eller försök eller medhjälp till utpressning.

Åtal mot både företrädare för bolaget och telefonförsäljare

Även i det sista målet, som avsåg ett upplägg med bedrägliga fakturor efter telefonkontakter, lämnade rätten delar av åtalet för fullbordade bedrägeribrott utan bifall. Det berodde bland annat på att en del målsägare hade betalat fakturorna trots att de insett att de aldrig ingått ett avtal med bolaget. Det innebar att det inte var styrkt att dessa målsägare betalat på grund av att de blivit vilseledda, vilket är en förutsättning för ett fullbordat bedrägeri. Samtidigt ansåg tingsrätten att det var styrkt att många andra målsägare hade blivit utsatta för antingen bedrägeri eller försök till bedrägeri.

En central fråga i tingsrättens bedömning var även huruvida huvudgärningspersonerna, som varit företrädare för bolaget, respektive telefonförsäljarna, kunde hållas ansvariga för brottsligheten. När det gäller huvudgärningspersonerna gjorde rätten bedömningen att dessa hade ett gemensamt ansvar för de brott som begåtts inom ramen för verksamheten. I fråga om telefonförsäljarna gjorde tingsrätten en individuell bedömning i uppsåtsfrågan för var och en av de tilltalade. En viktig faktor var att många av säljarna var unga och saknade tidigare arbetslivserfarenhet. Tingsrätten ansåg att de därmed kunde sakna förutsättningar att bedöma om bolagets verksamhet var seriös. I den mån en del av telefonförsäljarna dömdes till ansvar för bedrägerierna menade rätten att det var utrett att dessa personer, åtminstone efter en tid som anställda på bolaget, måste ha förstått att verksamhetens upplägg var brottsligt.

Kortbedrägerier

Vid kortbedrägerier använder gärningspersonen någon annans kontokort eller elektroniska kortuppgifter för att olovligen genomföra köp eller uttag.

Bedrägerier med hjälp av kontokort, kreditkort eller kortuppgifter utgör den största av de fem huvudkategorierna i urvalet av brottsbalksbedrägerier, motsvarande närmare 22 procent (87 ärenden).[31]

Typiska tillvägagångssätt: med eller utan ett fysiskt kort

Det centrala i ett kortbedrägeri är att gärningspersonen olovligen använder någon annans kontokort eller kortuppgifter för att genomföra ett köp eller uttag. För att kunna begå ett kortbedrägeri måste gärningspersonen först komma över ett fysiskt kort eller de kortuppgifter som behövs för att antingen framställa ett falskt kort eller för att exempelvis köpa varor via internet.

I kartläggningar från både rättsväsendet och näringslivet görs en åtskillnad mellan två huvudtyper av kortbedrägerier: *card present* (CP) respektive *card not present* (CNP). Polisens Nationella bedrägericenter använder följande definitioner (jfr Montague 2011, Bhargav 2015):

Card present (CP)
Transaktion med kort genomförd i direkt interaktion med säljare där köpare/kortinnehavare är fysiskt närvarande och där kort är synligt och används vid köp av tjänst eller vara.

Card not present (CNP)
Transaktion med kort genomförd via internet eller telefonsamtal med säljare där köpare/kortinnehavare inte är fysiskt närvarande och där något kort inte är synligt men kortdata används vid köp av tjänst eller vara.

[31] Majoriteten av kortbedrägerier i det granskade urvalet kodades av polisen som datorbedrägeri (36 ärenden), men många även som bedrägeri med kontokort (26 ärenden). Ytterligare 12 ärenden kodades som automatmissbruk och 11 ärenden som övrigt bedrägeri. Två ärenden kodades som bedrägeri med hjälp av internet (se tabell 1B i bilaga 3).

För att begå ett CP-bedrägeri krävs alltså att gärningspersonen har tillgång till ett fysiskt kort. Det kan antingen vara ett riktigt kort som kan ha blivit upphittat eller stulet, eller ett förfalskat kort där information från ett riktigt kort som man kommit åt (t.ex. med hjälp av skimning) har lagts in på magnetremsan. Trots att handeln på många håll har gått över till ett säkrare så kallat chip-och-pin förfarande vid exempelvis kortköp i fysiska butiker[32] menar Brås intervjupersoner att det finns företag som tillåter att magnetremsan används som ett reservalternativ. Det innebär att det fortfarande finns butiker och restauranger där kort med manipulerad magnetremsa kan användas. En form av CP-bedrägerier är också kontantuttag med stulna, borttappade eller skimmade kort.

Vid ett CNP-bedrägeri är det inte nödvändigt att ha ett fysiskt kort. Det kan räcka med den information som finns synligt på kortet för att genomföra ett köp, vanligtvis via internet. Vilka uppgifter som behövs kan variera, bland annat eftersom aktörer inom distanshandeln i olika länder kräver, enligt de intervjuade, olika mycket information för att godkänna en transaktion.

Knapphändig information i akterna försvårar gränsdragningen

De ovan beskrivna definitionerna av CP- respektive CNP-bedrägerier har varit vägledande i ärendegranskningen av kortbedrägerier. Det är dock viktigt att påpeka att omständigheterna kring kortbedrägerierna i många fall är ganska otydligt beskrivna i anmälningarna. Ytterst få ärenden av denna typ leder till uppklaring (se nedan) och informationen i det insamlade materialet är då ofta begränsad till anmälans fritextdel. Där beskrivs inte sällan med en enda mening att en viss summa pengar har dragits, ofta utomlands, från anmälarens konto.

Med dessa reservationer har 28 av ärendena (32 procent) kategoriserats som CP-bedrägerier, se tabell 11. Många av dessa anmälningar (11 ärenden) avser automatuttag som gjorts med stulna kort. I ett fall hade en metallist fästs i en bankomat som fångar upp sedlar vid uttag (så kallat ”cash trap”, jfr Ahola 2013). De övriga CP-ärendena är relativt jämnt fördelade över anmälningar som avser kortköp i fysisk butik, på restaurang eller på nattklubb, respektive anmälningar om att gärningspersonen använt ett borttappat eller stulet kort för att tanka bensin.

I totalt 26 kortbedrägerianmälningar (30 procent) har det funnits tillräckligt med information för att kunna kategorisera de anmäl-

[32] För mindre köp har dock utvecklingen varit det motsatta genom introducerandet av s.k. kontaktlösa kort (se kapitlet om Näringslivets roller).

da brotten som CNP-bedrägerier. En majoritet av dessa anmälningar avser att någon olovligen har genomfört köp via internet med hjälp av anmälarens kortuppgifter. Ofta är det oklart vad det är för varor eller tjänster som har köpts, men i vissa ärenden framgår att det handlar om exempelvis köp på Itunes eller köp av flyg- eller tågbiljetter. Fem av de ärenden som kategoriserats som CNP-bedrägerier avser att någon har använt anmälarens kortuppgifter för att föra över pengar till en spelsajt på internet.

I sammanlagt 33 (närmare 40 procent) av de anmälda kortbedrägeriärendena har det inte varit möjligt att avgöra vilken av dessa två typer av kortbedrägeri som det varit frågan om.

Tabell 11. Olika typer av kortbedrägerier. Polisanmälda ärenden första halvåret 2013.

	Antal	Procent
Card present (CP)	**28**	**32**
Automatuttag (stulna kort, shoulder-surfing)	(11)	(13)
Köp i fysisk butik (skimmade/stulna kort)	(8)	(9)
Bensintankning	(5)	(6)
Annat	(4)	(5)
Card not present (CNP)	**26**	**30**
Köp av varor/tjänster på internet	(17)	(20)
Spelsajter	(5)	(6)
Annat	(4)	(5)
Oklart om CP/CNP	**33**	**38**
Totalt	**87**	**100**

CNP ökar mest

Bland de granskade anmälningarna utgör alltså CP- respektive CNP-bedrägerierna ungefär lika stora kategorier. Det är dock tveksamt om denna fördelning motsvarar den faktiska brottsligheten. Enligt intervjuade poliser och näringslivsrepresentanter är CNP den snabbast ökande bedrägeritypen. Flera härvor där stora mängder kortuppgifter från diverse dataintrång har använts för bedrägliga köp avslöjades bara under 2014, enligt uppgifter från polisen och bankerna. Samtidigt anmäls dessa troligen i lägre utsträckning än bedrägerier med fysiska kort. Dels ersätter banken ofta kunden snabbt, dels har det framkommit i intervjuer med representanter för finansbranschen att det från bankernas sida sker omfattande monitorering av alla transaktioner och en stor mängd bedrägeriförsök avbryts *innan* kunden drabbas. Banken spärrar då kortet och kontaktar kunden. Kortbedrägerierna i det granskade urvalet av polisanmälda ärenden har dock oftast upp-

täckts först när kortinnehavaren sett att ett eller flera belopp har dragits från dennes bankkonto eller kreditkort.[33] De flesta polisanmälningar avser således brott som har fullbordats (över 90 procent), medan den stora mängden försök sannolikt inte fångas av ärendegranskningen. Trots denna troligen lägre anmälningsbenägenhet av CNP-bedrägerier (jämfört med CP) observeras en särskilt stor ökning av anmälningar under brottskoden datorbedrägeri (se figur 3), som omfattar CNP-bedrägerier.

Den strikta kodningen som Brå tillämpat, i kombination med bristande information i anmälningarna, innebär dessutom att många CNP-bedrägerier sannolikt finns med i den stora kategorin av ”oklart om CP eller CNP”. Sammanfattningsvis kan alltså antas att andelen CNP-bedrägerier är betydligt större än vad som framgår i granskningen.

Egentligen inte många likheter

De intervjuade representanterna för näringslivet understryker att även om det i bägge fallen rör sig om bedrägerier med kontokort, är det egentligen frågan om två väsensskilda typer av bedrägeribrottslighet. Jämfört med CNP ligger CP-bedrägerier till sin karaktär mycket närmare den traditionella tillgreppsbrottsligheten. CP-bedrägerier föregås inte sällan av rena stölder eller inbrott, och det mer fysiska tillvägagångssättet (i kontrast till det kontaktlösa förfarandet vid CNP-upplägg) gör dels att det kan finnas fler (enklare) spår att följa, dels att den som utsatts troligen är mer benägen att kontakta polisen.

Samtidigt bör beaktas att trots den stora, och ökande, volymen av e-handel är det fortfarande så att de flesta av dagens köp görs med hjälp av fysiska kort, det vill säga i CP-form. Å andra sidan skapar den nya tekniska utvecklingen och internetanvändandet nya möjligheter för bedragare att begå stora mängder brott med enbart några knapptryckningar, dessutom utan de risker som fysisk kontakt innebär. Det är därför i dessa brott, det vill säga CNP-bedrägerier, där det förebyggande arbetet har sin största utmaning.

Många sätt att skaffa kort eller kortuppgifter

Skimning – inte bara bankomater

Typiskt sett innebär skimning att gärningspersonerna fäster en avläsare på exempelvis en bankomat eller bensinautomat; avläsaren fångar sedan informationen på kortens magnetremsa. Skimningsutrustningen kan sitta kvar i något dygn och registrera kortuppgifter vid samtliga uttag och köp. Ofta finns även någon

[33] Det har inte varit möjligt med utgångspunkt i anmälningar och förundersökningar att göra någon säker uppdelning av om de kort som använts vid kortbedrägerierna varit kontokort eller kreditkort.

form av utrustning som används för att filma när kortinnehavaren trycker in sin pinkod. De uppgifter som sparas med hjälp av avläsaren kan sedan användas för att tillverka falska kort med den olovligen åtkomna kortinformationen på magnetremsan (t.ex. Kronqvist 2013).

Enligt Brås intervjupersoner tycks skimning vid bankomater ha blivit mindre vanligt förekommande i Sverige de senaste åren, vilket bland annat kan bero på att det i dag finns flera bankomater som är utrustade med olika former av elektroniskt skydd som ska försvåra skimning. Bankomater av nyare modeller avläser exempelvis bara kortets datachip (t.ex. Ahola 2013, Kronqvist 2013).

Skimning kan dock också ske vid exempelvis betalning av en taxiresa eller i samband med ett restaurangbesök. Ett sätt att komma åt kortuppgifter i liknande sammanhang är att kortets båda sidor fotograferas i samband med en betalning. Litteraturen beskriver också hur gärningspersoner, företrädesvis genom inbrott i butiker, kan manipulera butikernas kortbetalningsterminaler så att de registrerar både kortets kod och kundens pinkod. Koderna kan sedan till exempel skickas från utrustningen till gärningspersonerna via det vanliga mobiltelefonnätet (Kronqvist 2013).

Intervjuade poliser har också beskrivit organiserade ligor där någon först ställer sig i närheten av en person som genomför ett bankomatuttag eller en kortbetalning i en fysisk butik och avläser kortinnehavarens pinkod (så kallad shoulder-surfing). Därefter kommer gärningspersonerna åt kortet genom exempelvis en fickstöld och använder kortet för att göra bankomatuttag. Det finns enstaka exempel på sådana tillvägagångssätt bland ärendena som Brå granskat.

En etablerad svart marknad för stulna kortuppgifter på nätet

Med utgångspunkt i den information som finns i polisanmälda ärenden är det oftast oklart hur gärningspersonen har kommit över anmälarens kortuppgifter. Det framgår dock både av forskningen och av Brås intervjuer att gärningspersoner kan köpa kortuppgifter via olika forum på internet (jfr Kirwan och Power 2013). Enligt forskningen har det funnits en någorlunda organiserad svart marknad för stulna kortuppgifter på nätet sedan åtminstone 2002. Sedan dess har denna svarta marknad successivt blivit mer sofistikerad, först med garantier om att köpta kortuppgifter skulle fungera och så småningom med garantier att uppgifterna skulle fungera upp till ett specificerat belopp (Ablan m.fl. 2014).

Enligt intervjupersonerna stjäls de kortuppgifter som säljs på den svarta marknaden på flera olika sätt, till exempel med hjälp av så kallade keyloggers (en form av skadlig kod som avläser tangent-

tryckningar) eller genom olika typer av nätfiske. Ett exempel på nätfiske är att en förfrågan om verifiering av uppgifter kommer från en mejladress som är nästan identisk med bankens (eller ett annat företags), men den är falsk, och när kunden fyller i sina uppgifter hamnar dessa i fel händer. Ett annat sätt som används för att stjäla stora mängder kortuppgifter är genom datorintrång på företagsservrar (Ablan m.fl. 2014). En forskningsrapport från bekämpningen av den organiserade brottsligheten i USA (RO-CIC 2014) hänvisar till flera fall där datorintrång i stora företags datorsystem har inneburit stölder av kunders kortuppgifter och annan känslig information. Samma rapport beskriver hur man år 2013 lyckades stjäla uppgifter från miljontals kort genom att installera skadlig kod i en stor amerikansk butikskedjas kortterminalsystem. Enligt rapporten fördes de stulna kortuppgifterna vidare till Ryssland för att sedan göras tillgängliga till försäljning på internet.

Vilka är de inblandade?

Privatpersoner anmäler

Anmälaren är oftast en privatperson (närmare 90 procent) och det är nästan dubbelt så vanligt att anmälaren är en man än en kvinna. Anmälarnas ålder (framkommer i nio av tio ärenden) varierar mellan 20 och 82 år, och åldersfördelningen däremellan är mycket jämn. Medianåldern är 41 år.

I en tiondel av kortbedrägerianmälningarna är det ett företag eller en förening som anmält brottet, och i dessa ärenden handlar det framför allt om att olovliga köp har gjorts på ett företags- eller föreningskort. I ett ärende är det en bankanställd som gjort anmälan. Det är således sällan som kortutgivare eller banker anmäler dessa brott till polisen, även om det ibland framgår av anmälan att banken har kontaktat anmälaren och gjort denne uppmärksam på att det skett misstänkta transaktioner på hans eller hennes konto samt att kortet har spärrats. En intervjuad bankperson betonar att de i sådana lägen uppmanar den drabbade att polisanmäla.

Det insamlade materialet visar att det också är ovanligt att företag som sålt varor eller tjänster som köpts med stulna kortuppgifter gör en polisanmälan om detta. Det rör sig om enbart två sådana ärenden, och båda avser försöksbrott.

Enligt vad som framgår av de enskilda anmälningarna om kortbedrägeri, varierar summorna mellan 100 kronor och närmare 90 000. Medianbeloppet är cirka 3 500 kronor.

De bedrägliga summorna är dock betydligt större när den samlade brottsligheten med samma gärningspersoner studeras utifrån

domarna. De sammanlagda summorna vid de fullbordade bedrägeribrotten i domarna gällande CP-bedrägerier varierar mellan mindre än 2 000 kronor och närmare 250 000 kronor, med ett medianbelopp på ca 50 000 kronor. Gällande CNP-domarna uppgår motsvarande summor till mellan cirka 100 000 kronor och över 2,5 miljoner, med ett medianvärde på över en miljon kronor.

När rättsväsendet tar vid

Ytterst få kortbedrägerier klaras upp

Jämfört med annonsbedrägerier och fakturabedrägerier är andelen anmälningar som resulterat i ett personuppklaringsbeslut betydligt lägre gällande kortbedrägerierna. Enbart två ärenden (drygt två procent) av de anmälda kortbedrägerierna hade lett till ett personuppklaringsbeslut i slutet av 2014. I båda fallen handlar det om CP-bedrägerier; det ena avser uttag med ett kort som stulits under ett inbrott, det andra avser ett kortköp i fysisk butik efter skimning vid taxiresa. Ett ärende har lagts ner genom ett beslut om förundersökningsbegränsning, då den åtalade skulle åtalas för annan brottslighet. Vid slutet av 2014 var ingen av de granskade anmälda kortbedrägerierna fortfarande under utredning (tabell 12).

Tabell 12. Personuppklaringsbeslut, ärenden fortfarande under utredning och nedlagda ärenden efter nedläggningsorsak. Kortbedrägerier. (n = 87).

	Antal	Procent
Personuppklarade ärenden	**2**	**2**
Åtal	2	2
Fortfarande under utredning 2014-12-31	**-**	**-**
Nedlagda ärenden*	**85**	**98**
Dubbelanmält	1	1
Ej utredningsbart	56	64
Spanings-/bevisproblem (ingen misstänkt identifierad)	21	24
Bevisproblem (misstänkt identifierad)	5	6
Förundersökningsbegränsning	1	1
Oklart	1	1
Totalt	**87**	**100**

Vanligaste nedläggningsorsak: brottet går inte att utreda

Den enskilt vanligaste orsaken som registrerats i samband med nedläggningen av anmälningar om kortbedrägeri är att brottet

inte går att utreda. Nedläggningsbesluten i dessa ärenden har i regel fattats mer eller mindre direkt efter att anmälan registrerats. Den vanligaste anledningen som anges till att dessa anmälningar inte går att utreda är att pengarna har dragits från den utsattes konto utomlands, ofta med en skriftlig motivering att bevisningen därför inte är tillgänglig i Sverige. Ibland har polisen också lagt till att brottet inte är av sådan art att det föreligger förutsättningar att begära internationell rättslig hjälp. I övriga ärenden som lagts ner som icke utredningsbara hänvisas oftast till att det inte finns några bearbetningsbara spår som skulle ge möjlighet att identifiera en misstänkt gärningsperson.

Det är endast några få av utredningarna i urvalet som har lagts ner med en hänvisning till bevisproblem efter att man identifierat en misstänkt person. I dessa fall beror nedläggningen framför allt på svårigheter med att knyta den misstänkta gärningspersonen till det aktuella brottstillfället. Det handlar till exempel om ärenden där utredningen visat att den misstänkte har eller haft tillgång till ett kort som använts vid ett bedrägligt köp eller uttag, men där det saknats vittnesuppgifter eller bildbevisning som kan styrka att det var den misstänkte som faktiskt genomförde det aktuella köpet eller uttaget.

Åtgärder vidtas, men spaningsproblem vanligt vid CP-bedrägerier

Vid de anmälningar som kategoriserats som CP-bedrägerier är det relativt vanligt att polisen vidtagit vissa åtgärder för att försöka identifiera en misstänkt person innan ärendet har lagts ner. Som tidigare nämnts handlar dessa brott framför allt om bankomatuttag, tankning av bensin eller kortköp i fysiska butiker.

De spaningsåtgärder, som vidtagits i ärendena, och som Brås intervjupersoner har beskrivit som vanligast i dessa fall, handlar om att begära in övervakningsbilder från den aktuella automaten eller butiken. Även om bilderna i sig sällan räcker för att hitta en gärningsperson kan de utgöra en viktig stödbevisning. Intervjuade poliser beskriver dock en del problem med hantering av bilderna. Ett av dem är att kameraövervakningsbilder ofta inte sparas särskilt länge. En del butiker sparar inte övervakningsbilder i mer än några dagar, vilket innebär att polisen inte hinner komma tillräckligt långt i handläggningen av en anmälan innan eventuell bildbevisning har förstörts. Bilderna vid bankomater sparas längre, men även här kan det finnas problem. I vissa ärenden har man exempelvis fått in övervakningsbilder från en bankomat där gärningsmannen gjort sig oigenkännlig med neddragen mössa eller liknande. Det är heller inte alltid så att den tekniska utrustningen för bildövervakning fungerar vid brottstillfället.

Fokus på leveransadresser och utlämningsställen vid utredning av CNP-bedrägerier

Vid CNP-bedrägerier finns betydligt mer sällan några utredningsbara spår. Enligt Brås intervjupersoner kan man dock ibland identifiera gärningspersoner genom att följa upp en leveransadress för varor som har köpts med stulna kortuppgifter. Det framgår till exempel av ärendegranskningen att polisen har tagit kontakt med kortutgivare för att få information om på vilka webbplatser som kortköp har genomförts. Man har sedan också tagit kontakt med internetförsäljare för att få information om vart de aktuella beställningarna har skickats. Gärningspersoner begär ofta en sms-avisering, i regel till ett oregistrerat kontantkort, när varorna ska hämtas från postens utlämningsställen. Även om leveransadressen därför inte behöver vara till den person som faktiskt hämtar ut varorna, kan man ändå begära in övervakningsbilder från utlämningsstället. Som tidigare nämnts sparas dock inte dessa särskilt länge, och polisen har i de flesta fall fått besked om att bilderna inte längre finns kvar när de väl tagit kontakt med de aktuella butikerna.

När åtal väckts

Brås urval av bedrägeridomar innehåller 15 domar som avser kortbedrägerier. Av dessa handlar 9 domar om CP-bedrägerier och 6 om CNP-bedrägerier.

Tre huvudtyper av CP-domar

Domarna gällande CP-bedrägerier avser tre huvudsakliga typer av ärenden. Den ena handlar om uttag som gjorts med kort stulna från t.ex. en förälder eller släkting, där den misstänktes identitet redan var känd vid tidpunkten för anmälan. Den andra avser köp med stulna eller förfalskade kort i fysiska butiker. Här har de misstänkta personerna bland annat kunnat identifieras genom att butiksbiträden har fattat misstanke och lyckats hålla gärningspersonen på plats tills polisen kommit. Den tredje typen av CP-bedrägerier i domarna avser uttag med stulna kort som begåtts av mindre kriminella grupperingar som systematiskt arbetat med shoulder-surfing och fickstölder, framför allt riktade mot äldre personer. Domarna avser sammanlagt 18 tilltalade, därav 8 kvinnor och 10 män. Antalet bedrägeritillfällen som behandlats i dessa domar varierar mellan ett och ett femtiotal.

Stora mängder stulna kortuppgifter i CNP-domarna

Totalt 21 personer har blivit åtalade för bedrägeribrott i de sex CNP-domar som ingår i Brås material, samtliga män. Antalet

bedrägeritillfällen i respektive dom varierar från 21 till över 200. I två av domarna finns ingen information om hur gärningspersonerna har kommit över de stulna kortuppgifterna, medan det i de övriga fyra målen framgår att gärningspersonerna antingen har köpt eller på annat sätt kommit över kortuppgifterna på olika webbplatser på internet. I dessa fall har ett stort antal stulna kortuppgifter påträffats på en dator tillhörande åtminstone en av de tilltalade gärningspersonerna, och de kortuppgifter som användes vid bedrägeribrotten har kunnat kopplas till banker och kortutgivare i flera olika länder, inklusive Sverige.

Kortuppgifterna har främst använts för köp via internet, ibland från internetsidor i Sverige, ibland utomlands. Uppgifterna har även använts för att ladda pengar på presentkort som sedan sålts vidare via annonssidor, eller för att föra över pengar till konton på onlinespelsajter.

Medhjälpare av olika slag bland de tilltalade

I några av CNP-målen har vissa tilltalade på olika sätt arbetat åt huvudgärningspersonerna. De användes till att hämta ut varor som köpts via internet, eller till att upplåta sina konton för överföringar från exempelvis spelsajter. I ett av målen har även några personer åtalats för häleri, då de hjälpt till med vidareförsäljningen av varor som köpts med hjälp av stulna kortuppgifter.

Omfattande och komplex bevisning

Polisens utredningar i målen gällande CNP-bedrägerier har varit omfattande. Man kan ha fått börja med att utreda en enda misstänkt person som till exempel identifierats genom sitt kontonummer eller vid hämtning av varor på ett utlämningsställe. Därefter har man fått lägga ett komplext pussel för att leta sig fram till andra gärningspersoner, bland annat med hjälp av uppgifter från it-forensiska analyser av beslagtagna telefoner och datorer. Utöver förhör med målsägare, tilltalade och olika expertvittnen samt bevisningen från it-forensiska analyser redovisas ofta även orderuppgifter avseende kortköp på internet, IP-spårningar som visar varifrån kortköp har genomförts samt omfattande transaktionsanalyser som visar hur pengar har förts över mellan olika spel- eller bankkonton.

Nästan alla tilltalade döms

Med ett undantag har samtliga personer som blivit åtalade för kortbedrägerier blivit dömda för grovt bedrägeri, bedrägeri (inklusive försök), medhjälp till bedrägeri eller penninghäleri. I de mål där polisen har upptäckt listor med stulna kortnummer på gärningspersoners datorer har dessa personer även åtalats och blivit dömda för förberedelse till grovt bedrägeri.

En del av åtalspunkterna för bedrägeri i särskilt de större CNP-målen har inte vunnit bifall i tingsrätten. Här handlar det framför allt om att domstolen har ansett att bevisningen på vissa punkter inte har varit tillräcklig för att knyta vissa gärningspersoner till en del av bedrägeritillfällena i en längre brottsserie. I vissa fall handlar det exempelvis om att den enda stödbevisning som kunde knyta en gärningsperson till ett visst brottstillfälle var en medgärningspersons vittnesmål, vilket inte har ansetts tillräckligt tillförlitligt. I andra mål har medhjälpare som haft i uppdrag att hämta ut varor beställda med stulna kortuppgifter friats från ansvar vid vissa åtalspunkter avseende försöksbrott. Detta då varorna inte har skickats (bedrägeriet upptäcktes innan) och man inte har kunnat utesluta att den tilltalades inblandning i de aktuella brottstillfällena därmed inte blivit aktuell. Vissa åtalspunkter har inte vunnit bifall då leverantören brast i att utföra en identitetskontroll vid en leverans av varor. I dessa fall har det inte ansetts styrkt att det var den aktuella gärningspersonen som tog emot varorna.

Kreditbedrägerier

Kreditbedrägerier innebär att gärningspersonen genomför ett köp av en vara/tjänst, alternativt tar ett lån, i någon annans namn. I regel inleds brottet med en identitetsstöld. Kreditvärdiga bolag används inte sällan som verktyg.

Kreditbedrägerier utgör totalt 17 procent av urvalet av anmälda brottsbalksbedrägerier (68 ärenden).[34]

Typiska tillvägagångssätt: köp och lån i annans namn

Kreditbedrägerier går oftast ut på att man tar ett lån eller köper varor eller tjänster på exempelvis avbetalning eller mot fakturering, ofta i någon annans namn, utan att det finns någon avsikt hos låntagaren eller köparen att betala. Skillnaden mellan kort- och kreditbedrägerier är att vid de förstnämnda betalas varan vid köptillfället, även om det ibland är ett (falskt) kreditkort som används. Vid kreditbedrägerier separeras dessa två moment. Att bedragaren vid köp- eller lånetillfället låtsas vara någon annan än den hon eller han egentligen är utgör en central del i kreditbedrägerier. Det underlättas också av att betalning sker vid en annan tidpunkt än köptillfället. Det kan ske genom att bedragaren genomför den aktuella transaktionen i en annan privatpersons identitet eller genom att man vilseleder motparten att tro att man representerar ett företag och att beställningen görs och så småningom ska betalas av företaget.

Den internationella forskningen på området hänvisar även i detta sammanhang till kriminella individer eller grupper som genom dataintrång på företagsservrar kommit åt stora mängder med information rörande personer som varit kunder hos olika företag.

[34] Två tredjedelar (43 ärenden) av kreditbedrägerierna kodades av polisen som övrigt bedrägeri, men en del också som bedrägeri med hjälp av internet (13 ärenden) och datorbedrägeri (6 ärenden). Tre ärenden kodades som bedrägeri med kontokort och två som fakturabedrägeri (se tabell 1B i bilaga 3).

I dessa personers namn kunde sedan bedrägliga köp äga rum. För Sveriges del menar dock Brås intervjupersoner att de personuppgifter som krävs för att genomföra köp eller lån i någon annans namn är mycket lättillgängliga (se kapitlet om Identitetsmissbruk). Ett annat problem är även de många godkända typer av identitetshandlingar, med varierande säkerhetsstandard, som gör det svårare att kontrollera identiteter.

Kräver oftast identitetshandlingar

Vid tecknandet av ett låneavtal eller vid köp på kredit som sker i ett fysiskt möte (i butiker, på banker m.m.) krävs att man legitimerar sig, vilket innebär att den här typen av brottslighet ofta kräver en stulen, falsk eller manipulerad identitetshandling. Kreditbedrägerier kan också genomföras med hjälp av att helt falska, påhittade identiteter skrivs in i Bolagsverkets register eller folkbokföringen på basis av felaktiga identitetshandlingar. Genom exempelvis påhittade anställningar skapas en kreditvärdighet hos ett företag som sedan används som brottsverktyg (se vidare kapitlet Näringslivets roller).

Vid distansköp på kredit, det vill säga oftast via internet, förskjuts den fysiska identitetskontrollen[35] ofta till den punkt där varan lämnas ut vid ett utlämningsställe, eller vid leverans till beställarens hem- eller företagsadress. På utlämningsställen krävs en identitetshandling, vilket återigen ställer krav på gärningspersonen att skaffa en stulen, falsk eller manipulerad identitetshandling. Vid leveranser till en hem- eller företagsadress är det enligt Brås intervjupersoner oklart hur ofta någon form av identitetskontroll genomförs, och det kan ibland räcka med att mottagaren skriver under ett papper om att varan har mottagits från leverantören.[36]

I kapitlet om identitetsmissbruk beskrivs mer ingående olika sätt att använda osanna (stulna eller helt falska) identiteter i ett bedrägligt syfte. Det kan vara aktuellt även vid andra typer av bedrägerier, men bara vid kreditbedrägerier är det oftast ett centralt moment.

Det finns dock enligt Brås intervjupersoner även kreditbedrägeriupplägg där gärningspersonen inte nödvändigtvis försöker dölja sin identitet bakom någon annans. Ett exempel är att bedragaren köper en bil på avbetalning och betalar de första månaderna för att förhindra misstankar om bedrägligt uppsåt, för att sedan försvinna med bilen utomlands.

[35] Vissa sidor med internetförsäljning (liksom banker i samband med lån) kräver e-legitimering vid köptillfället. För mer detaljer, läs kapitlet om Identitetsmissbruk.

[36] Vissa företag har avtal med fraktfirmorna om dessa förenklade rutiner.

Mindre kreditbedrägerier: köp av varor i annans namn

Det finns en stor variation i omfattningen och komplexiteten bland kreditbedrägeribrotten. Tre av fyra av de anmälda ärendena om kreditbedrägeri avser situationer där gärningspersonen har köpt eller försökt köpa en vara eller en tjänst i någon annans namn på kredit eller mot faktura. Det är framför allt privatpersoners identiteter som används, men ibland framgår att gärningspersonen har utgett sig för att vara representant för ett företag. I dessa fall har gärningspersonen ibland tecknat, eller försökt teckna, ett nytt kreditavtal i företagets namn, medan gärningspersonen i enstaka ärenden tycks ha utnyttjat ett redan befintligt kreditavtal mellan säljföretaget och det företag som gärningspersonen säger sig representera.

Tabell 13. Olika typer av kreditbedrägerier. Polisanmälda ärenden första halvåret 2013.

	Antal	Procent
Bedrägliga kreditköp	**56**	**82**
Mobil och/eller abonnemang i annans namn	(19)	(28)
Köp av annan tjänst/vara i annans namn (på kredit/faktura)	(37)*	(54)
Bedrägliga lån	**9**	**13**
Bank- eller kreditlån i annans namn	(7)	(10)
Sms-lån i annans namn	(2)	(3)
Annat kreditbedrägeri	**3**	**4**
Totalt	**68**	**100**

* 5 av dessa anmäldes av företag.

Ofta mobilabonnemang och elektronik

Det absolut vanligaste tillvägagångssättet bland de polisanmälda ärendena är att gärningspersonen har skaffat sig ett mobilabonnemang – ofta där en ny mobiltelefon ingår i abonnemangspaketet – med hjälp av någon annans, ofta anmälarens, identitet (tabell 13). Av materialet framgår ofta inte explicit huruvida abonnemangen har tecknats i fysisk butik, men många av de anmälda brotten har troligen skett via internet, då det framgår att en försändelse innehållande telefonen har skickats med post. I omkring hälften av dessa ärenden har gärningspersonen lyckats få krediten godkänd och dessutom kunnat hämta ut försändelsen med falska identitetshandlingar. I de övriga fallen stannade det vid ett försök, antingen genom att gärningspersonen nekats den sökta krediten eller genom att gärningspersonen inte lyckats med att omdirigera försändelsen.

Övriga varor som enligt anmälningarna handlas i annans namn är datorer och annan elektronik, möbler, kläder och byggmaterial. Enligt de granskade ärendena använder bedragarna oftast andra privatpersoners identiteter, men det händer att de handlar i ett företags namn (exempelvis byggmaterial).

Få bedrägliga kreditköp av tjänster

Jämfört med kreditköp av telefoner med tillhörande abonnemang och andra typer av varor är det mindre vanligt med anmälda kreditbedrägerier som avser köp av tjänster. I några ärenden rör det sig om SL:s sms-biljettjänst. Andra ärenden handlar om köp av evenemangsbiljetter eller medlemskap på olika kontaktsidor på internet. I två ärenden har personer utgett sig för att vara representanter för företag och i det ena fallet bott på hotell, i det andra fallet hyrt byggmaskiner och kläder i det aktuella företagets namn utan att återlämna dem.

Enligt Brås intervjupersoner har kreditbedrägerier gällande flygresor varit relativt frekventa under en period. Enbart ett sådant ärende förekommer dock i det granskade materialet. Anmälaren har fått en faktura för flygbiljetter som någon köpt i dennes namn.

Lån i annans namn: tidigare relation vanligt

Sammanlagt sju anmälda ärenden avser att gärningspersonen försökt ta eller tagit ett banklån i någon annans namn. I fyra av dessa ärenden framgår att den utpekade gärningspersonen tidigare varit i ett förhållande med anmälaren, och brotten har ofta upptäckts först i samband med eller efter en separation. Vanligtvis är urkundsförfalskning ett led i brottet, då gärningspersonen förfalskat anmälarens namn på lånehandlingarna. Ytterligare två av anmälningarna avser snabba sms-lån som gärningspersonen tagit respektive försökt ta i någon annans namn (läs mer om snabba sms-lån i kapitlet Näringslivets roller).

Mer avancerade kreditbedrägerier genom företag

Brås intervjupersoner beskriver även en annan, mer komplex, form av kreditbedrägeri som utnyttjar företagsformen. Det påbörjas exempelvis genom att gärningspersoner först köper upp befintliga företag. Därefter nyttjas företagets krediter för att beställa varor utan avsikt att betala, varpå gärningspersonerna driver företaget i konkurs och säljer de beställda varorna vidare. Att företag används på dessa sätt har även konstaterats i annan svensk forskning (Rönnblom, Skinnari och Korsell 2015, se vidare kapitlet Näringslivets roller i denna rapport).

Ett mindre vanligt, men mer komplicerat, bedrägeriupplägg som enligt de intervjuade används vid storskaliga kreditbedrägerier mot företag (inte bara i Sverige, se Savona och Berlusconi 2015) involverar en avancerad kapning av kända företags namn och varumärken (s.k. domänkapning). Det görs först en mer eller mindre exakt kopia av ett känt företags hemsida på nätet. Den enda skillnaden är att vissa kontaktuppgifter byts ut och internetadressen skiljer sig enbart med en knappt märkbart förändrad stavning. Denna förfalskade hemsida kopplas till en mejlserver, som sedan används för att skicka ut beställningar på varor till andra företag med det riktiga företagets logga på. För mottagaren ser beställningarna, med länken till den förfalskade webbsidan, riktiga ut. Varorna skickas, betalning uteblir och webbsidan försvinner.

Dessa mer komplicerade kreditbedrägerihärvor med inblandning av företag är samtidigt svåra att studera utifrån anmälda brott, där enbart fragment, i bästa fall, fångas i form av information om brotten vid respektive anmälan. Bland de granskade ärendena finns bara ett där det framgår att gärningspersonerna har begått kreditbedrägerier med hjälp av att först ha köpt ett kreditvärdigt företag och sedan utnyttjat företagets kredit. Både intervjuade gärningspersoner och representanter för näringslivet bedömer att många drabbade företag tar de förluster som orsakas av den här typen av bedrägerier utan att anmäla brotten (se vidare kapitlet Näringslivets roller).

Fyra av tio är anmälda försöksbrott

I närmare fyra av tio av de anmälda ärendena om kreditbedrägeri framgår att gärningspersonen inte har lyckats få någon vinning av gärningen. I dessa ärenden kan anmälan ha föranletts av att anmälaren har kontaktats av ett kreditupplysningsföretag som berättat att någon försökt teckna kredit i dennes namn. Det kan också handla om att anmälaren har fått hem ett låneavtal för påskrift. Ett annat exempel är att gärningspersonen har beställt varor på kredit i anmälarens namn, men inte lyckats omdirigera postens avisering, vilket har inneburit att anmälaren själv har tagit emot de beställda varorna och fått skicka tillbaka dem.

De anmälningar där brottet har fullbordats har i många fall upptäckts först när anmälaren, vars identitet har använts vid exempelvis ett kreditköp, har fått hem en faktura eller inbetalningsavi. I dessa fall framgår ofta att anmälaren först har tagit kontakt med det bolag som skickat fakturan eller inbetalningsavin och att detta bolag har uppmanat den utsatte att anmäla brottet till polisen för att bolaget självt sedan ska utreda ärendet och eventuellt befria anmälaren från betalningsskyldighet.

Summorna vid fullbordade kreditbedrägerier varierar mellan 180 och 200 000 kronor i enskilda anmälda ärenden. Medianbeloppet är cirka 2 800 kronor.

Vilka är de inblandade?

Anmälaren oftast en (bekant) privatperson

I de allra flesta fall är anmälaren en privatperson (närmare 90 procent av ärendena), och på samma sätt som vid de anmälda kortbedrägerierna är det något vanligare att anmälaren är en man än en kvinna. Kreditbedrägerierna tycks inte vara riktade mot någon specifik åldersgrupp, utan anmälarens ålder (framgår i 55 ärenden) sträcker sig mellan 20 och 88 år och fördelningen däremellan är mycket jämn. Medianåldern är 35 år.

Jämfört med de övriga bedrägerityper som beskrivs i rapporten, där bedragaren i de allra flesta fall är en okänd person, är det något vanligare vid kreditbedrägerier att anmälaren misstänker (eller vet) att gärningspersonen är en bekant person. Det är rimligt att den här typen av bedrägeri som involverar identitetsstöld oftare begås av gärningspersoner som är bekanta med den vars identitet används; närheten gör det lättare att komma över identitetsuppgifterna. Det framgår oftast vid anmälningar som avser att gärningspersonen tagit ett lån i anmälarens namn, men bekantskap mellan de inblandade förekommer också vid andra typer av kreditbedrägerier. Totalt sett framgår av anmälningarna att det finns sådana misstankar i omkring ett av fyra anmälda kreditbedrägeriärenden. Det rör sig inte alltid om en nära relation, men i 7 ärenden riktades anmälarens misstankar mot någon som stod henne eller honom relativt nära, som före detta partner, släkt eller vänner.

Få anmälningar av företag

Fem av anmälningarna om kreditbedrägerier har gjorts av företag. I två fall handlar det om att någon olovligen har köpt varor på kredit i det aktuella företagets namn. Enbart i de övriga tre anmälningarna framgår att anmälaren är det företag som sålt eller lämnat ut varor eller tjänster på kredit till en bedragare. På samma sätt som med kortbedrägerierna är det således sällan som kreditbedrägerier anmäls till polisen av de delar av näringslivet som drabbas av den här typen av brottslighet.

Ytterligare två av anmälningarna har upprättats av polisen, då de aktuella kreditbedrägerierna har upptäckts under en pågående utredning.

När rättsväsendet tar vid

Relativt låg personuppklaring

På samma sätt som vid kortbedrägerierna är andelen anmälningar som resulterat i ett personuppklaringsbeslut låg vid kreditbedrägeribrotten. Knappt sex procent av de anmälda kreditbedrägerierna hade lett till ett personuppklaringsbeslut i slutet av 2014. Ett av brotten var fortfarande under utredning vid denna tidpunkt (tabell 14).

Tabell 14. Personuppklaringsbeslut, ärenden fortfarande under utredning och nedlagda ärenden efter nedläggningsorsak. Kreditbedrägerier. (n = 68).

	Antal	Procent
Personuppklarade ärenden	**4**	**6**
Åtal	4	6
Fortfarande under utredning 2014-12-31	**1**	**1**
Nedlagda ärenden*	**63**	**93**
Dubbelanmält	1	1
Ej brott/Preskriberat/Anmälan inte längre aktuell	7	10
Ej utredningsbart	25	37
Spanings-/bevisproblem (ingen misstänkt identifierad)	24	35
Bevisproblem (misstänkt identifierad)	2	3
Förundersökningsbegränsning	3	4
Oklart	1	1
Totalt	**68**	**100**

* För en beskrivning av hur nedläggningsbesluten har kodats, se bilaga 2.

Att det finns enstaka anmälningar i materialet som lagts ner med hänvisning till att brottet är preskriberat beror på att bedrägerier, som skett inom en parrelation, kan upptäckas först när relationen tar slut, ibland många år efter brottstillfället. De motiveringar som angetts för nedläggningen i kategorin *anmälan inte längre aktuell* är bland annat att det så småningom har visat sig att en faktura har skickats till anmälaren av misstag, på grund av någon form av förväxling. Dessutom finns ett fall där anmälaren dragit tillbaka anmälan då det kommit fram att en misstänkt transaktion handlade om att ett barn hade använt förälderns mobilabonnemang för att genomföra köp på en internetsida.

Längre tid mellan brotts- och anmälningstillfället påverkar möjligheter att säkra bildbevisning

En dryg tredjedel av anmälningarna om kreditbedrägerier har lagts ner med motiveringen att brottet inte går att utreda. Här hänvisar man framför allt till att det inte finns tillräckligt med

bearbetningsbara spaningsuppslag. I fall där anmälaren har misstankar mot en viss person kan polisens motivering till att brottet inte går att utreda vara att en utredning sannolikt inte kommer att leda till åtal, eller att det saknas förutsättning för att styrka att den utpekade (eller någon annan) har begått brottet.

Det är nästan lika många anmälningar om kreditbedrägeri som lagts ner med en hänvisning till att de spaningsåtgärder som vidtagits inte har gett något resultat. Huvudfokus för polisens spaningsåtgärder har, på samma sätt som vid kortbedrägeribrotten, varit att säkra eventuella kameraövervakningsbilder av gärningspersonen när hon eller han genomfört ett kreditköp i en butik eller hämtat ut varor på ett utlämningsställe.

Det framgår av ärendegranskningen att polisen med hjälp av anmälarens uppgifter och olika utredningsåtgärder har kunnat identifiera vilken butik eller vilket utlämningsställe som är intressant. Som vid utredningar av kortbedrägerier är det dock i regel så att butiker inte sparar övervakningsbilder särskilt länge, och förutom i undantagsfall har eventuell bildbevisning redan raderats när polisen väl har tagit kontakt med de aktuella butikerna.

Ärendegranskningen visar vidare att polisens möjligheter att genom bildbevisning identifiera okända gärningspersoner ofta är förenade med ännu mer påtagliga problem vid kreditbedrägerier än vid kortköp. Det beror på att den vars identitet har använts vid ett fullbordat kreditköp ofta reagerar och gör en polisanmälan först när hon eller han får hem en faktura eller inbetalningsavi. Det finns flera ärenden i det insamlade materialet där köp har gjorts med kreditavtal som kräver en första avbetalning först en relativt lång tid efter köptillfället. Det framgår också av materialet att en del anmälare har väntat med att anmäla tills de fått hem en påminnelse eller till och med ett inkassokrav. I dessa ärenden kan det ha gått flera månader mellan brottstillfället och polisanmälan, vilket i princip omöjliggör inhämtning av eventuell bildbevisning.

En del misstänkta personer identifierade

I de ärenden där det finns en identifierad misstänkt person har denne kunnat identifieras på olika sätt. I vissa ärenden har anmälaren, som nämnts, haft en misstanke om gärningspersonens identitet redan vid anmälningstillfället, då den misstänkte exempelvis varit en tidigare partner eller en bekant till anmälaren. Det finns även enstaka ärenden där man identifierat den misstänkte genom att följa pengarna, när ett lån har tagits i någon annans namn, eller där polisen kunnat identifiera den misstänkte genom att denne använt egna identitetshandlingar vid tecknandet av ett kreditavtal. Här handlar det till exempel om en gärningsperson

som använt sitt eget namn i kreditavtalet som representant för ett företag, då denne råkade ha samma namn som en person i företagets ledning. I det tidigare nämnda ärendet där ett kreditvärdigt bolag hade köpts och sedan använts för att göra kreditköp, har kreditbedrägeribrotten upptäckts då en av gärningspersonerna utreddes av Ekobrottsmyndigheten för bland annat bokföringsbrott och skattebrott.

När åtal väckts

Sammanlagt 17 domar i Brås urval avser kreditbedrägerier. De flesta avser en enda gärningsperson men i enstaka domar åtalas två eller tre gärningspersoner som har begått brotten tillsammans. Sammanlagt avser domarna 22 gärningspersoner, av vilka sju är kvinnor.

Tre domar där en bekants identitet använts

I tre av domarna är gärningspersonen någon som har en relation till den vars identitet har använts vid bedrägeribrotten – dennes förälder, syskon eller personliga assistent. Det är naturligt att förutsättningarna för brottets uppklaring är bättre när gärningspersonen finns i målsägarens nära omgivning. Den tilltalade i var och en av dessa tre domar var kvinna och domarna avser mellan 13 och 33 bedrägeritillfällen (inklusive försök), framför allt i form internetköp av varor eller tecknande av mobilabonnemang. I två av domarna finns uppgift om att den tilltalade också hade begått bedrägerier med hjälp av en eller flera ytterligare identiteter eller genom olovliga kontoöverföringar med hjälp av annans bankdosa. Alla tre tilltalade har dömts för brotten, och summorna vid de fullbordade brotten motsvarar 19 000, 55 000 respektive över 200 000 kronor.

Oftast har existerande personers identiteter använts

I de övriga 14 målen är gärningspersonerna oftast män. Knappt hälften av domarna avser ett eller endast ett fåtal (högst fem) bedrägeritillfällen, medan de övriga avser mellan tio och tjugofem brottstillfällen. Summorna vid de fullbordade bedrägeribrotten i domarna varierar mellan ca 4 000 och över tre miljoner kronor (medianvärdet var ca 80 000 kronor).

Dessa domar avser ofta köp av varor eller tecknande av abonnemang i annans namn, antingen i butik eller på internet; i vissa mål har gärningspersonen eller -personerna använt flera olika modus. När de fått tillgång till falska identitetshandlingar har de både genomfört köp i butik och via internet samt även tecknat lån i andras namn. I de domar som avser något längre brotts-

serier framgår att gärningspersoner använt flera olika identiteter, och flera av de tilltalade har till slut tagits på bar gärning, då butiksanställda fattat misstanke om de identitetshandlingar som uppvisats. I de flesta fall är det en existerande persons identitet som har använts, vilket bland annat framgår av att dessa personer ofta nämns som målsägare i åklagarens stämningsansökan.

I enstaka fall har den tilltalade i stället begått de åtalade kreditbedrägerierna med hjälp av ett uppköpt företag eller med helt falska identiteter (dvs. utan koppling till en existerande person). I det senare fallet handlar det exempelvis om en gärningsperson som använde förfalskade passhandlingar och gjorde ansökningar om EU-invandring till Skatteverket i olika identiteter, som sedan tilldelades svenska personnummer. Förfalskade inkomstdeklarationer hade också skickats till Skatteverket. De falska identiteterna användes sedan bland annat för att genomföra köp och lån för stora belopp.

Medhjälpare mindre synliga i kreditbedrägeridomar

Jämfört med de mer komplexa kortbedrägerimålen, där det finns tilltalade som haft olika roller i bedrägerierna, är det sällan en sådan rollfördelning syns i domarna avseende kreditbedrägerierna. Ett undantag är ett mål där den tilltalade är en person som mot betalning systematiskt hämtade ut paket som hade köpts på kredit via internet. Den tilltalade hade försetts med en förfalskad legitimationshandling i det namn som användes vid beställningen av varorna. Han hade också fått använda sin egen legitimation, då han varit tvungen att hämta ut varorna som ”bud” för den person vars namn fanns på beställningarna. Detta gjorde det möjligt för polisen att spåra den tilltalade, men enligt domen har man i detta fall inte lyckats identifiera huvudgärningspersonerna. Det finns även ett mål där en person blivit dömd för penninghäleri kopplat till en del av de åtalade kreditbedrägerierna. Till skillnad från en del av kortbedrägeridomarna tycks man däremot i utredningarna inte ha kopplat de identifierade gärningspersonerna till en större grupp, där det funnits andra personer inblandade i till exempel en relaterad häleriverksamhet. Det innebär att det saknas den typen av bevisning som använts för att koppla gärningspersoner till varandra i vissa av kortbedrägeridomarna.

Samtidigt innehåller många kreditbedrägeridomar ändå ett omfattande bevisningsunderlag. Det handlar om alltifrån kameraövervakningsbilder, vittnesmål av butikspersonal, kvitton och abonnemangsavtal till de ovan nämnda ansökningar om EU-invandring och inkomstdeklarationer som skickats till Skatteverket. Bevisningen innehåller ofta kopior av förfalskade identitetshandlingar och dokumentutlåtanden som styrker att identitetshandlingarna är falska.

Samtliga åtalade dömda, men inte på alla åtalspunkter

Samtliga gärningspersoner har dömts antingen för bedrägeri eller grovt bedrägeri eller penninghäleri, förutom i två av målen, som båda avsåg ett enskilt brottstillfälle där de tilltalade inte hade lyckats fullborda brotten. Dessa två personer har båda dömts för försök till bedrägeri. Flera av de tilltalade har också dömts för brukande av falsk urkund samt urkundsförfalskning.

På samma sätt som för de övriga bedrägerityperna har en del av åtalspunkterna avseende kreditbedrägerierna inte vunnit bifall i tingsrätten. I ett fall har den tilltalade friats på en del åtalspunkter, då resultaten från en skriftanalys från dåvarande SKL[37] av de namnteckningar som fanns på vissa skuldebrev inte kunde binda gärningspersonen till de aktuella lånen på ett tillräckligt säkert sätt. Andra åtalspunkter har ogillats därför att det som främst kunde knyta gärningspersonerna till de aktuella brotten var identifieringsuppgifter från butiksanställda, som inte ansågs som tillräckligt säkra – bland annat på grund av den tid som hade förflutit mellan brotten och domstolsförhandlingen.

[37] Numera NFC – Nationellt forensiskt centrum.

Övriga telefon- och internetbedrägerier

Bland övriga telefon- och internetbedrägerier finns flera olika typer av upplägg där gärningspersoner använder skadlig kod eller kontaktar den utsatte via telefon eller internet. Upplägen tillhör inte någon av de tidigare beskrivna kategorierna av bedrägeribrott men kan ibland utgöra ett försteg.

Kategorin av övriga telefon- och internetbedrägerier motsvarar 16 procent av det granskade urvalet av anmälda brottsbalksbedrägerier (62 ärenden).[38]

Ett brett spektrum av olika tillvägagångssätt

Den gemensamma nämnaren bland många olika slags händelser som tillhör denna kategori är att gärningspersonerna använder antingen internet eller telefonkontakter, eller en kombination av dessa, för att på olika sätt vilseleda de utsatta personerna till att föra över pengar eller lämna ut känsliga uppgifter. Till skillnad från de övriga bedrägerierna handlar dessa brott om vare sig bedrägliga köp eller försäljning, även om de upplägg som används i vissa fall kan utgöra ett försteg till andra typer av bedrägeribrott – till exempel om den utsatte luras till att lämna ifrån sig sina kortuppgifter.

Litteraturen på området beskriver ett brett spektrum av olika typer av tillvägagångssätt som har använts av bedragare i ovan nämnda syften, bland annat bedrägerier som sker med hjälp av skadlig kod (t.ex. Goldberg och Larsson 2013), bedrägerier

[38] Brotten är spridda över ett antal olika brottskoder, men majoriteten av övriga telefon- och internetbedrägerier har av polisen registrerats som bedrägeri med hjälp av internet (25 ärenden) respektive datorbedrägeri (21 ärenden). En del har även kodats som övrigt bedrägeri (15 ärenden) och ett ärende som bedrägeri med kontokort (se tabell 1B i bilaga 3).

genom så kallat nätfiske (t.ex. Maras 2015), förskottsbedrägerier (t.ex. Kirwan och Power 2013), romansbedrägerier (t.ex. Gillespie 2016) och bedrägerier med hjälp av datorintrång i mejlkonton eller konton på sociala media (t.ex. Turban m.fl. 2015). Många av dessa bedrägerimodus har också beskrivits i litteraturen som delar i en bredare kategori av bedrägliga tillvägagångssätt som ingår under paraplybegreppet *social engineering* (Watson m.fl. 2014, El-Din m.fl. 2015). Enligt Turban m.fl. (2015) handlar det om modus där kriminella personer utnyttjar mer eller mindre universella psykologiska sårbarheter för att manipulera människor att lämna ifrån sig känslig information, som sedan kan användas i syfte att begå brott.

Exempel på alla de ovan nämnda tillvägagångssätten finns i varierande grad i urvalet av anmälda brottsbalksbedrägerier (se tabell 15), och de olika typerna av modus beskrivs därför kortfattat nedan tillsammans med aktuella exempel som förekommer i materialet.

Tabell 15. Olika typer av övriga telefon- och internetbedrägerier. Polisanmälda ärenden första halvåret 2013.

	Antal	Procent
Skadlig kod (Ransomware m.m.)	25	40
Nätfiske (Phishing m.m.)	19	31
Teknisk-support bedrägerier	5	8
”Vän i nöd” – bedrägerier via mejl eller sociala media	10	16
Förskotts- och romansbedrägerier	3	5
Totalt	**62**	**100**

Bedrägerier med hjälp av skadlig kod

Man brukar ofta tala om tre huvudtyper av så kallad skadlig kod (”malware”) – virus, maskar och trojaner (t.ex. Kronqvist 2013, Goldberg och Larsson 2013) – och det är framför allt trojaner som beskrivs i litteraturen om bedrägerier. Enligt Brås intervjupersoner blir datorer, smartphones eller surfplattor[39] oftast smittade med trojaner genom att användaren öppnar en infekterad bilaga som skickats i ett mejlutskick, klickar på en länk i ett mejl eller besöker en webbsida som har infekterats av gärningspersoner med avsikt att sprida den skadliga koden.

Trojaner: Ransomware, spyware och banktrojaner

Det finns flera olika typer av funktioner som trojaner kan vara programmerade att utföra. Bland annat kan trojaner ge gärnings-

[39] För enkelhetens skull används ”dator” som ett samlingsnamn i resten av detta avsnitt.

personer möjligheten att fjärrkontrollera den infekterade datorn (Goldberg och Larsson 2013). Enligt Brås intervjupersoner kan olika varianter av så kallad *spyware* ge gärningspersonen tillgång till datorns filsystem, vilket innebär att den får läsa känslig information som sparats på datorn. Andra former av spyware kan läsa av användarens tangentavtryckningar (så kallade keyloggers som tidigare nämnts i avsnittet om kortbedrägerier) och spara ner information för att sedan skicka den vidare till gärningspersonen (jfr Goldberg och Larsson 2013, Youngblood 2015).

När en dator blir smittad av så kallade *ransomware-trojaner,* kan de aktuella trojanerna exempelvis kryptera antingen hela filsystemet eller vissa typer av filer på datorn, till exempel foton, musikfiler eller dokument, så att användaren inte längre kan få tillgång till innehållet. Alternativt kan trojanen låsa datorn så att den blir helt oanvändbar (Kharraz m.fl. 2015). Samtidigt visar trojanen oftast upp ett meddelande som kräver en lösensumma för att återställa datorn (ibid.). Ett alternativt sätt att kräva lösensumma på är, enligt Brås intervjupersoner, att gärningspersonen i stället skickar ett mejl till den utsatte.

Enligt Brås intervjupersoner har det skett en utveckling under de senaste åren, där fokus för ransomwareangrepp har förskjutits, från att framför allt ha riktats mot privatpersoner till ett större fokus på företag. Det har också skett en utveckling i angreppen från att nästan uteslutande ha drabbat datorer som använder Windows, till att allt oftare även drabba enheter med andra typer av operativsystem.

Vidare finns det även *banktrojaner*. Enligt litteraturen finns det olika varianter men de har gemensamt att de kommer emellan och tar kontroll över det elektroniska kommunikationsflödet mellan bankkunden och bankens servrar när kunden loggar in på sin internetbank. Det möjliggör för gärningspersonen att manipulera de transaktioner som den utsatte själv genomför på kontot, till exempel genom att ändra i det angivna beloppet vid en kontoöverföring samt omdirigera överföringar till andra mottagarkonton (se t.ex. Buescher m.fl. 2011, Goldberg och Larssson 2013).

Det framgår av Brås intervjuer med experter på området att när en dator väl har blivit smittad kan den skadliga koden också ”ropa till sig” andra trojaner, så att samma dator blir angripen av skadlig kod som utför flera olika typer av funktioner. Datorer som smittats med trojaner som ger gärningspersonen möjligheten att fjärrkontrollera dem kan sedan också ingå i så kallade botnets (se t.ex. Kaushik 2013). Dessa är stora nätverk av infekterade datorer som används i flera olika kriminella sammanhang, till exempel för att skicka spammejl, som kan användas både för

nätfiske eller för att sprida annan skadlig kod, eller för att utföra så kallade överbelastningsattacker mot specifika webbplatser (Goldberg och Larsson 2013).

Ransomware klart vanligast i Brås ärendegranskning

Det finns totalt 25 ärenden i urvalet av anmälda brottsbalksbedrägerier där det framgår, eller finns en misstanke om, att skadlig kod har använts. Ett av dessa ärenden avser en person vars dator blivit smittad av en banktrojan, vilket lett till att en stor summa pengar tagits från den utsattes bankkonto. Ytterligare ett ärende avser en anmälan där man misstänker att anmälarens dator har smittats med någon form av spyware, vilket också resulterat i att pengar dragits från anmälarens bankkonto.

De övriga 23 ärendena avser ransomware. I samtliga ärenden har anmälarens dator låsts och det har kommit upp ett meddelande som ser ut att komma från polisen. Meddelandet kräver att den utsatte betalar en viss summa pengar, i form av ”böter”, med motiveringen att den utsatte har besökt otillåtna internetsidor. Den utsatte får också en instruktion om hur betalningen ska gå till. I enbart två av de studerade fallen hade den utsatte fört över summan. I ett av dessa ärenden framgår att datorn hade låsts upp – dock bara i några dagar. Därefter begärdes en ny summa pengar och det blev klart för den utsatte att det rörde sig om ett bedrägeri.

Att inslaget av ransomware är så slående i Brås material behöver inte betyda att andra typer av trojaner inte förekommer i någon större utsträckning. Enligt Brås intervjupersoner är en rimlig tolkning att utsatta personer inte inser att datorn blivit smittad med skadlig kod, till exempel i form av spyware.

Phishing, vishing och smishing

En nästan lika stor grupp av bedrägerier (19 ärenden) handlar om olika former av så kallad phishing (ofta kallat nätfiske på svenska), vishing, från engelskans voice-phishing (Maras 2015), eller smishing, från engelskans sms-phishing (Kang m.fl. 2013).

Vid *phishing* skickar gärningspersonerna mejl till de utsatta med syftet att få dem att frivilligt lämna ifrån sig känslig information, till exempel i form av användarnamn och lösenord eller kortuppgifter (Maras 2015). Typiskt sett framstår mejlen som om de kommer från en bank eller ett väletablerat företag, och mottagaren uppmanas att klicka på en länk som leder till en webbsida för att exempelvis bekräfta olika typer av uppgifter (Watson m.fl. 2014). Andra exempel är att de utsatta istället får ett mejl om att de vunnit på lotteri och att deras uppgifter behövs för att de ska kunna få ut vinsten (Tak och Ojha 2012).

Vid *vishing* är gärningspersonens syfte detsamma som vid phishing via mejl men med skillnaden att den utsatte i det här fallet antingen får ett mejl som uppmanar mottagaren att ringa upp ett visst nummer, eller så kontaktas den utsatte direkt via ett telefonsamtal (Dunham m.fl. 2009). Enligt litteraturen använder gärningspersonerna ofta IP-telefoni, vilket ger möjligheten att dessutom manipulera samtalsdata så att nummerpresentatören på mottagarens telefon visar att samtalet kommer från en till synes tillförlitlig källa, exempelvis en bank eller kundtjänsten hos ett känt företag (Grant och Shaw 2014).

Uppläggen vid så kallad *smishing* följer samma mönster. Man får exempelvis ett sms om att man ska få en återbetalning med en länk till en webbsida där man ska lämna olika typer av känslig information (Grant and Shaw 2014, Kang m.fl. 2013). I litteraturen beskrivs även phishing-upplägg som sker genom reklam i sociala medier, som Facebook, med någon form av erbjudande. När användare klickar på reklamen, blir de dirigerade till förfalskade webbsidor, där de ombes att uppge olika typer av information för att kunna ta del av erbjudandet (Clough 2015). Både phishing och smishing används också i upplägg som samtidigt utnyttjas för att sprida trojaner, som sedan också ger gärningspersonerna tillgång till den utsattes dator eller mobiltelefon (Kang m.fl. 2013).

Nätfiske via mejl vanligare än andra kontaktsätt

Det vanligaste av dessa modus bland de granskade ärendena avser nätfiske via mejl. Mejlen har i de flesta fall utgett sig för att vara från Skatteverket, en bank eller ett välkänt företag och har uppmanat mottagaren att via en länk eller i en bifogad fil antingen bekräfta sina kontouppgifter eller fylla i sina kortuppgifter. De skäl som anges i mejlen för att anmälaren ska lämna uppgifterna är exempelvis för att kunna få en skatteåterbäring eller för att få en återbetalning efter ett misstag som inneburit att mottagaren betalat för mycket för en tjänst. Ett undantag är ett mejl där man bett om mottagarens kortuppgifter för att denne skulle få delta i ett lotteri. Materialet innehåller även två ärenden som avser smishing. Det ena av dessa ber mottagaren att lämna ifrån sig uppgifter för att få en återbetalning, det andra för att få ut en stor lotterivinst.

Det är relativt få av anmälningarna avseende de här uppläggen som har resulterat i någon förlust för de utsatta personerna. Enligt flera av anmälningarna i materialet har anmälaren tagit kontakt med det aktuella företaget och fått en bekräftelse på att det inte är de som har skickat mejlet. I några fall har dock anmälaren lämnat ifrån sig sina kortuppgifter, och en summa pengar har därefter dragits från anmälarens bankkonto.

Det är ovanligt med rena vishinganmälningar i Brås urval, men det finns enstaka anmälningar där det framgår att en okänd person har ringt till anmälaren och försökt få fram olika typer av uppgifter. I ett ärende har anmälaren till exempel blivit kontaktad av en person som hävdat att denne ringer från anmälarens telefonoperatör. Anmälaren har därefter kontaktat operatören och fått besked om att det sannolikt handlade om ett försök att kapa anmälarens telefonabonnemang. Enligt ytterligare två anmälningar i materialet har anmälaren blivit utsatt för telefonkontakter, som sannolikt har handlat om någon form av vishing, men i dessa fall saknas vidare information om de typer av uppgifter som har efterfrågats.

Teknisk support-bedrägerier

Ytterligare fem av anmälningarna i urvalet avser ett upplägg som kan sägas ligga i en gråzon mellan vishing och bedräglig försäljning. Bedrägeriet börjar med att någon ringer till den utsatte och på bruten engelska hävdar att hon eller han ringer från en teknisk supportavdelning, företrädesvis på Microsoft. Av denna anledning har dessa bedrägerier också blivit kända som ”Microsoftbedrägerier”.

Syftet med samtalet är att först övertyga den utsatte om att hans eller hennes dator har drabbats av ett virus eller annat problem. Därefter försöker ”teknikern” att få den utsatta personen att ladda ner en programvara som tillåter ”teknikern” att fjärrstyra datorn för att sedan låtsas hjälpa den utsatte genom att rätta till de påstådda (men egentligen obefintliga) problemen. Bedragaren vill sedan få betalt och kan också erbjuda någon form av programvara eller försäkring som ska skydda datorn från liknande angrepp i framtiden. Betalningen kan exempelvis ske via den utsattes internetbank, eller så kan bedragaren, genom fjärrstyrning av datorn, guida den utsatte till en internetsida, till exempel Paypal eller liknande, för att genomföra överföringen.

Ett av ärendena i Brås material avser ett fullbordat brott, det vill säga den utsatte hade fört över pengar till bedragaren. I detta fall hade bedragaren därefter även ringt tillbaka och fått den utsatte att ange sina kortuppgifter via ett webbformulär, under förespegling att den utsatte skulle få en återbetalning, varpå ytterligare en olovlig överföring hade gjorts från bankkontot.

”Vän i nöd”: bedrägeri via intrång i mejl- eller sociala media-konton

Sammanlagt 10 av de ärenden som ingår i kategorin övriga telefon- och internetbedrägerier handlar om bedrägerier som skett efter att bedragaren först har gjort intrång i och tagit kon-

troll över en persons mejl- eller Facebook-konto. Nio av dessa ärenden avser ett upplägg som har kallats för ”den strandsatta resenären” (t.ex. Anderson m.fl. 2013). Efter att ha tagit kontroll över ett webbmejl-konto skickar bedragaren ut ett mejl till kontoinnehavarens kontakter. Det innebär att mottagarna får mejlet från någon de känner, vilket genast ökar trovärdigheten i innehållet. Meddelandet beskriver hur avsändaren befinner sig i en svår situation utomlands och exempelvis har blivit rånad på sin plånbok. I regel blir mejlmottagarna ombedda att skicka pengar, ofta genom en alternativ betalningsförmedlare som Western Union. I tre av dessa nio ärenden hade bedrägeriet fullbordats genom att den utsatte hade skickat de efterfrågade pengarna.

Det finns bara ett ärende i Brås material där det framgår att händelsen har föregåtts av att gärningspersonen gjort intrång i någons Facebook-konto. Anmälaren i detta ärende var en Facebookvän till den person vars konto hade kapats av gärningspersonen. Gärningspersonen hade lurat anmälaren att lämna ifrån sig koderna från sin bankdosa för att därefter tömma anmälarens konto på pengar. Enligt Brås intervjupersoner har den här typen av bedrägeri varit relativt vanligt under en tid. Enligt samma intervjupersoner har även en ny typ av Facebook-relaterat bedrägeriupplägg nyligen börjat synas, som också går ut på att övertala de utsatta att lämna ifrån sig information som kan användas till att logga in på deras internetbankkonton. Upplägget går ut på att gärningspersonen först startar en Facebookgrupp i namnet av en banksäkerhetsavdelning eller liknande. Därefter tar man kontakt med folk och får dem att lämna ifrån sig koder till sina bankdosor eller BankID.

Förskotts- och romansbedrägerier

Ett förskottsbedrägeri går ut på att bedragaren lurar den utsatte att skicka pengar i förväntan om att så småningom få en mycket större summa tillbaka. Det klassiska exemplet är det så kallade nigeriabrevet, där mottagaren får ett mejl om att avsändaren behöver hjälp med att föra ut en stor summa pengar ur landet. Mottagaren erbjuds en del av dessa pengar för att hjälpa till. Ett typiskt upplägg enligt litteraturen är att avsändaren ska ärva en stor summa pengar. Så småningom visar det sig däremot att det finns vissa kostnader, till exempel i form av advokatarvoden eller liknande, som den utsatta personen övertalas att hjälpa till med. Nya former av kostnader tillkommer till dess att den utsatte inser att hon eller han blivit lurad, eller tills pengarna tar slut (Brenner 2012, Simha 2013).

Romansbedrägerier via internet delar ofta flera gemensamma drag med förskottsbedrägerier (Whitty och Buchanan 2016). I detta fall är bedragarens syfte att först utveckla en kärleksrela-

tion med den utsatte på distans för att sedan börja lura denne på pengar på olika sätt. Enligt forskningen och Brås intervjupersoner kan det exempelvis handla om pengar som ska användas för en resa för att träffa den utsatta personen eller för att hjälpa till med gamla skulder (jfr Gillespie 2016). Jämfört med många andra typer av bedrägerier kan romansbedrägerier enligt forskningen förorsaka särskilt allvarliga känslomässiga skador hos de utsatta personerna (Buchanan och Whitty 2014).

Tre av anmälningarna i Brås urval av anmälda brott avser förskotts- eller romansbedrägerier. I ett ärende hade anmälaren kontaktats av en person, som utgav sig för att vara advokat, med besked om att han skulle få en stor summa pengar i arv efter en släkting. I ett annat hade anmälaren varit i kontakt med en kvinna i Asien och skickat pengar för att hjälpa henne med att få ut ett arv. I detta ärende framgår inte om anmälaren själv, en man, skulle ta del av pengarna, eller om det i stället handlade om en del i ett romansbedrägeri. I det tredje ärendet hade anmälaren utvecklat en relation med en person utomlands, som sedan skulle besöka anmälaren i Sverige. Anmälaren hade bland annat skickat pengar för att betala flygresan men besöket uteblev.

Vilka är de inblandade?

I samtliga granskade ärenden gällande övriga telefon- och internetbedrägerier – utom ett – framgår att anmälaren är en privatperson. Könsfördelningen bland de utsatta personerna är relativt jämn (55 procent män, 45 procent kvinnor). Det finns en stor åldersspridning bland anmälarna, från 11 år till närmare 90 år, men medianåldern (54 år) är relativt hög jämfört med exempelvis annons-, kort- och kreditbedrägerierna. I drygt tre av fyra ärenden framgår att anmälan har gjorts utan att det skett någon form av överföring från den utsatte till gärningspersonen. I de ärenden där det skett en överföring handlar det om belopp på mellan närmare 400 kronor och drygt 90 000, (medianbeloppet ca 4 000).

Kriminella nätverk och tekniska verktyg

Enligt både litteraturen (t.ex. Luiijf 2012) och Brås intervjupersoner är någon form av bakomliggande organisation mer eller mindre ett krav vid dessa typer av bedrägeriupplägg. Samtidigt är organisationen i regel mindre strukturerad och hierarkisk jämfört med mer traditionella former av organiserad brottslighet (t.ex. Europol 2014). Brotten sker ofta i projektform med hjälp av nätverkskontakter, där flera aktörer kan bidra med olika kriminella tjänster. Det handlar om aktörer som kan tillhandahålla olika tekniska verktyg som används vid brotten, nätverk för att tvätta pengar, översättningstjänster eller så kallade ”skottsäkra” hostingtjänster i olika delar av världen, som ger kriminella en till-

gång till internet och samtidigt vägrar att samarbeta med brottsbekämpande myndigheter (Bradbury 2014, Levi m.fl. 2015a, b). Enligt litteraturen sker dessa nätverkskontakter via kriminella marknader på nätet (Europol 2014, Levi m.fl. 2015a, b).

När rättsväsendet tar vid

Svåra förutsättningar för personuppklaring

Det framgår av både litteraturen och Brås intervjuer att de ovan beskrivna bedrägerityperna är mycket svåra att utreda och klara upp. Det beror bland annat på att brotten antingen begås från utlandet eller via utländska servrar, till exempel med hjälp av de nyss nämnda skottsäkra hostingtjänsterna. Det avspeglas i att ingen av de anmälningar som ingår i den här kategorin av brottsbalksbedrägerier hade resulterat i ett personuppklaringsbeslut vid slutet av 2014 (tabell 16).

Tabell 16. Personuppklaringsbeslut, ärenden fortfarande under utredning och nedlagda ärenden efter nedläggningsorsak. Övriga telefon- och internetbedrägerier. (n = 62).

	Antal	Procent
Personuppklarade ärenden	**-**	**-**
Fortfarande under utredning 2014-12-31	**2**	**3**
Nedlagda ärenden*	**60**	**97**
Ej brott	1	2
Ej utredningsbart	50	81
Spanings-/bevisproblem (ingen misstänkt identifierad)	9	15
Totalt	**62**	**100**

* För en beskrivning av hur nedläggningsbesluten har kodats, se bilaga 2.

Över 80 procent av anmälningarna har lagts ner som icke-utredningsbara utan att man inlett en förundersökning. De motiveringar för nedläggningen som framgår av materialet i dessa ärenden är framför allt att brottet har begåtts utomlands, att det inte finns tillräckligt med bearbetningsbara spaningsuppslag eller att en utredning inte förväntas leda till att brott kan styrkas.

I de ärenden som ingår i kategorin *spaningsproblem* har man inlett en förundersökning. I dessa fall har polisen oftast lagt ner ärendena efter några dagar med motiveringen att det saknas förutsättningar för att styrka brott mot viss person. I två ärenden har en misstänkt person identifierats, i båda fallen genom att följa pengar som förts över från den utsatta personens bankkonto. Enligt misstankeregistret var dessa två ärenden fortfarande under utredning i slutet av 2014.

De utredningssvårigheter som kännetecknar den här kategorin av bedrägerier får också en bekräftelse av att det inte finns några ärenden av dessa typer i Brås särskilda urval av domar. Det innebär också att det inte finns ett underlag i Brås material för att beskriva hur dessa typer av bedrägerihändelser har hanterats i tingsrätterna.

Utredning kräver samarbete och specialistkompetens

Enligt intervjuade experter finns tre huvudsakliga spår som kan följas vid utredning av dessa typer av bedrägerier. Det ena handlar om att följa pengarna, om det skett en överföring. I ärenden där den utsatte har kontaktats via mejl, till exempel vid phishing, kan det finnas möjlighet att spåra mejlkommunikationen. Det finns också särskilda spårningsmöjligheter vid bedrägerier som sker med hjälp av skadlig kod. Många typer av skadlig kod innehåller instruktioner att ta kontakt med, eller ”ropar hem” till, gärningspersonen (t.ex. Aquilina m.fl. 2008). Enligt intervjupersoner ger en analys av den skadliga koden därmed möjlighet att kontrollera vart någonstans den ”ropar hem”.

Enligt intervjupersoner är det endast det första av dessa tre spår som faller inom ramen för bedrägeriutredares vanliga kompetensområde. Att spåra mejl samt analys och spårning av skadlig kod kräver specialistkunskaper som i stället finns hos polisens it-brottscentrum. It-brottscentrumet har också viktiga kontakter med internationella samarbetspartners, inte minst Europol. Inom Europol delas information om bland annat aktuella bedrägerimodus mellan de brottsbekämpande myndigheterna i olika länder. Brås intervjupersoner menar att åtgärder mot den här typen av brottslighet ofta kräver internationella samarbeten. Dels finns möjlighet att ha en gemensam utredning, där brottsbekämpande myndigheter från olika länder deltar samtidigt, men det kan också handla om att man enbart bidrar med information och bevisning som kan användas i en redan pågående brottsutredning i ett annat land.

För att utreda den här typen av bedrägerier krävs således ofta ett samarbete mellan bedrägeriutredare och it-brottscentrumet samt även internationellt. Det innebär enligt intervjupersoner att det är viktigt att det sker en samordning av den här typen av bedrägeriärenden. Samtidigt menar intervjupersoner att det numera finns en mycket bättre samordning av dessa ärenden genom polisens Nationella bedrägericenter (NBC), som i sin tur har löpande kontakter med it-brottscentrumet. Inom ramen för dessa kontakter kan it-brottscentrumet bedöma möjliga framgångsfaktorer för att utreda dessa brott när det gäller spårning av skadlig kod eller mejlkommunikationer, vilket ger NBC möjlighet att göra en bedömning av var bedrägeriutredarnas resurser ska koncentreras.

NBC kan sedan förmedla it-brottscentrumets syn på de tekniska aspekterna av brottsligheten till bedrägeriutredare ute i landet.

Det är samtidigt viktigt att påpeka att intervjuade experter från både Sverige och Storbritannien menar att även om man följer upp de olika möjliga spåren, så kan det ofta visa sig att det inte går att komma så mycket längre i utredningen, bland annat på grund av svårigheter med att få ut information från hostingtjänster i andra länder.

Bidragsbrott och andra välfärdsbedrägerier

En bidragstagare lämnar felaktig information för att få en högre utbetalning från välfärdssystemen än vad denne är berättigad till. Alternativt underrättar personen inte den utbetalande myndigheten eller organisationen om ändrade förhållanden, och får därigenom för mycket utbetalt.

Detta avsnitt handlar om bidragsbrotten – och andra välfärdsbedrägerier mot utbetalande myndigheter och organisationer. Eftersom dessa bedrägerier skiljer sig från de tidigare redovisade genom att samtliga riktar sig mot myndigheter och organisationer har avsnittet en lite annorlunda disposition. Inledningsvis beskrivs grundläggande villkor inom välfärdssystemet och vilka myndigheter som drabbas. Därpå beskrivs hur tillvägagångssättet ser ut när det gäller respektive utbetalare. Ett längre avsnitt ägnas åt vilka som är gärningspersoner vid bidragsbrott, då det förekommer relativt stora skillnader mot personer som begår brottsbalksbedrägerier. Avslutningsvis beskrivs rättsväsendets hantering av bidragsbrott.

Typiska tillvägagångssätt

Bakgrund: två typer av bidrag

Det går att tala om två typer av bidrag från välfärdssystemen. De första är *generella*, där alla som uppfyller villkoren får ett fastställt belopp oavsett inkomst och situation. Exempel på detta är barnbidrag och tandvårdsbidrag. Dessa är mycket ovanliga bland upptäckt brottslighet, det finns enbart enstaka fall i denna studies material. Den andra och klart vanligare kategorin är *behovsprövade bidrag* (Department for Work and Pensions 2011). Beloppet som betalas ut avgörs av uppgifter om tidigare och nuvarande inkomst. Till detta kommer vilken situation man befinner sig i – om man är sjuk, studerar eller saknar arbete. Exempel är sjukpen-

ning, föräldrapenning, arbetslöshetsersättning och studiemedel. De flesta ärendena finns inom denna kategori.

Redan här antyds att den stora delen av den anmälda bidragsbrottsligheten rör felaktig information om tidigare eller aktuella inkomster. Generellt innebär detta att gärningspersonerna anger för hög tidigare inkomst och för låg aktuell inkomst för att få ett högre bidrag än de är berättigade till. Eller att de inte underrättat utbetalaren om att de fått förändrade (typiskt sett högre) inkomster.

Försäkringskassan och arbetslöshetskassorna anmäler flest bidragsbrott

I denna kartläggning drogs ett särskilt urval på 50 ärenden gällande bidragsbrott. Hur ärendena i urvalet fördelar sig på de utbetalande myndigheterna och organisationerna redovisas i tabell 17.

Tabell 17. Bidragsbrott, fördelning över de utbetalande aktörerna. Polisanmälda ärenden första halvåret 2013.

Bidragsbrott mot:	Antal	Procent
Försäkringskassan	21	42
Arbetslöshetskassorna	18	36
Kommunerna	9	18
CSN	1	2
Pensionsmyndigheten	1	2
Totalt	**50**	**100**

Fördelningen mellan utbetalande myndighet eller organisation i Brås urval motsvarar i stora drag situationen vid de anmälda bidragsbrotten generellt.

Eftersom det är ett ganska litet urval saknas dock Migrationsverket och Arbetsförmedlingen, som också omfattas av bidragsbrottslagen, helt i urvalet. När det gäller Arbetsförmedlingen är förklaringen att deras allra flesta utbetalningar inte faller inom ramen för bidragsbrottslagen utan den generella bedrägeribestämmelsen (SOU 2008:74, SOU 2014:16).

I Migrationsverkets fall har det tidigare konstaterats att de gör få polisanmälningar (SOU 2011:3). En förklaring är dels att de hittar få felaktigheter, en annan att beloppen som betalas ut till asylsökande är så låga att de inte uppgår till sådana summor att de ska polisanmälas ens som ringa bidragsbrott (Riksrevisionen 2011).

Nedan beskrivs bidragsbrotten utifrån vilken myndighet eller organisation de riktar sig mot. Beskrivningen baseras främst på

ärendegranskningen, men där ärenden saknas används intervjuer och tidigare studier för att visa hur bidragsbrotten och välfärdsbedrägerierna kan se ut. Till skillnad från brottsbalksbedrägerierna finns många studier utförda både på Brå och på andra håll om bidragsbrott och välfärdsbedrägerier.

Höga belopp som faktiskt betalats ut

Samtliga fall i ärendegranskningen är fullbordade brott, i bemärkelsen att pengar har betalats ut. Med andra ord har det inte varit *fara* för utbetalning utan det rör sig om en ekonomisk skada för målsägaren.

I 46 av de 50 ärendena finns uppgifter om vilket belopp som betalats ut felaktigt. Det lägsta beloppet är strax över 1 500, det högsta närmare 19 miljoner kronor.[40] Medelbeloppet är 462 000 kr, medianen ca 14 000 kr. Ungefär hälften (23) av ärendena rör belopp i storleksordningen 6 000–19 000 kronor. Med andra ord är spridningen stor, och i urvalet med anmälda ärenden finns en hel del brott med lägre belopp.

I 10 ärenden överskrider det utbetalade beloppet 100 000 kronor, vilket innebär att utbetalningen motsvarar inkomster för en längre tidsperiod som betalats ut felaktigt. I de allra största fallen handlar det om personlig assistans under flera års tid.

Inslaget av upprepade bidragsbrott relativt stort

I ungefär hälften av ärendena handlar det om enstaka brottstillfällen. Anmälan och förundersökning avslöjar ingen systematik eller tecken på upprepad brottslighet. I ungefär hälften av fallen finns dock sådana tecken.

Systematiken är ofta tämligen enkel, det handlar om att en sökande har uppgett en liknande felaktighet eller underlåtit att anmäla ändrade förhållanden – vilket lett till fler felaktiga utbetalningar av bidrag (jfr Åklagarmyndigheten 2015). Brotten har löpt under en tid, på i stort sett samma sätt. Med andra ord handlar det i många fall om upprepning av samma gärning snarare än en utpräglad systematik. Det förklarar också varför ungefär hälften av ärendena uppvisar tecken på systematik eller upprepning, men bara tre ärenden är anmälda som grova bidragsbrott.

Även om det ofta saknas systematik i den misstänkta brottsligheten har personen ofta ansökt om bidrag flera gånger eller tidigare haft ersättning. Det finns alltså en ”relation” till målsäganden, i detta fall en utbetalande myndighet eller organisation. En

[40] Det vill säga samtliga är över Åklagarmyndighetens riktvärde för vårdslöst bidragsbrott som är 5 000 kr, och över gränsen till bidragsbrott av normalgraden – 1 500 kr.

väsentlig skillnad mellan bidragsbrott och brottsbalksbedrägerier är att den utbetalande myndigheten eller organisationen ofta har kunnat gå tillbaka och granska den sökandes historik. Det innebär att det är betydligt mer troligt att upptäcka en systematik i bidragsbrotten än vid många brottsbalksbedrägerier.

Vilka är de inblandade?

Försäkringskassan

Ärendena med anmälda bidragsbrott mot Försäkringskassan avser tre olika typer av förmåner:

1. De som ersätter kostnader (bostadsbidrag, bostadstillägg) eller stöd till barnfamiljer (underhållsstöd, barnbidrag, flerbarnstillägg).
2. Ersättningar som ska ersätta lön, men där det misstänks att personen haft inkomster från arbete samtidigt (sjukpenning, sjukersättning eller föräldrapenning) eller fått för hög ersättning genom felaktig sjukpenninggrundande inkomst.
3. Assistansersättning, där man begärt ersättning för fler timmar personlig assistans än vad som utförts och betalats ut av anordnaren. Alternativt att brukaren överdrivit sitt behov, men assistenter varit på plats.

Bidrag som ersätter kostnader

Ärendena i den första kategorin omfattar lägst belopp. Det handlar om några tusenlappar och uppåt, beroende på antalet utbetalningar. I en handfull akter i granskningen har en person fått bostadsbidrag eller bostadstillägg för en bostad de inte längre bor i. Alla uppgifter i ärendena talar för att den första utbetalningen var korrekt, men sedan har situationen förändrats. Det finns dock exempel i intervjumaterialet på att hyreskontraktet varit förfalskat från början.

I andra ärenden har par skenseparerat eller flyttat ihop utan att anmäla detta. Vid sidan av bostadsbidrag finns också felaktiga utbetalningar av underhållsstöd i sådana ärenden. Bland exemplen finns också personer som bott utomlands och därmed inte har haft rätt till barnbidrag eller flerbarnstillägg. Här är Försäkringskassan beroende av korrekta uppgifter från Skatteverkets folkbokföring för att inte enbart behöva förlita sig på den sökandes uppgifter (jfr även SOU 2008:74, Brå 2015:8).

Bidrag som ersätter inkomstbortfall

Den andra kategorin innehåller typiskt sett större misstänkt felaktigt utbetalda belopp. I en handfull ärenden har en person med sjukersättning inte anmält förbättrad arbetsförmåga till Försäk-

ringskassan. Det finns också enstaka exempel där en förälder har haft föräldrapenning samtidigt som den arbetat, eller åtminstone fått lön.[41] I några fall hänvisar den misstänkte till oklara regelverk. Till detta kommer ärenden där personen fått lön för fler timmar än vad den enligt läkarintyg varit arbetsför och därmed fått ersättning från både Försäkringskassan och arbetsgivaren för samma timmar.

Enstaka misstänkta personer anger i utredningarna att de haft dålig ekonomi eller varit skuldsatta. Därför har de försökt få in lite mer pengar från Försäkringskassan, pengar som de tänkt betala tillbaka när ekonomin tillät.

Att den sökande från början har korrekta läkarintyg och har varit sjukskriven korrekt, men med tiden glider in i bidragsfusk har konstaterats även i tidigare studier (ISF och Brå 2011:12, Brå 2015:8). Särskilt svårt blir det när personen arbetar i ett eget företag som inte går runt. Det definieras inte av företagaren som arbete – då det inte ger lön, men enligt regelverken är sådant arbete i ett företag ett tydligt tecken på arbetsförmåga. Ett av de granskade ärendena verkar vara av detta slag.

I vissa fall i ärendegranskningen har dock inträdet i sjukförsäkringen eller föräldraförsäkringen varit bedrägligt. I några ärenden har personer lämnat in felaktiga arbetsgivarintyg och lönespecifikationer, som visat på en högre lön än de haft, och därmed gett en högre sjukpenninggrundande inkomst. I förlängningen har de fått för hög ersättning utbetald (sjukpenning, sjukersättning, föräldrapenning, tillfällig föräldrapenning).

Även detta är känt från tidigare studier, och tillhör de svåraste ärendena att upptäcka för Försäkringskassan (Brå 2015:8). I ett ärende i föreliggande undersökning menar den misstänkta att hon haft den lön hon uppgett, men svart. Det är mycket svårt för Försäkringskassan att upptäcka och dokumentera att en person har haft svarta inkomster. Här är myndigheten beroende av framför allt uppgifter från Skatteverket, exempelvis från revisioner och skattebrottsutredningar (se ISF och Brå 2011:12).

Assistansersättning

Något förenklat kan personer med funktionsnedsättning (enligt vissa kriterier) få ersättning för att anlita personliga assistenter. Den tredje kategorin brott mot Försäkringskassan består av några granskade akter om assistansersättningen. I ett fall finns också misstankar om bedrägerier mot Arbetsförmedlingens nystartsjobb.

[41] Vid vissa bidragsbrott räcker det att visa att personen fått lön. Det är ovidkommande om arbete utförts eller inte. Bidraget är för att ersätta försörjningsförmåga, vilket en person med lön uppvisar.

Grunden i dessa bedrägerier är att assistenterna inte arbetat alls, mindre eller till en väsentligt lägre kostnad än anordnaren uppger till Försäkringskassan. Några ärenden kompliceras av att andra personer än de anställda assistenterna utfört viss assistans, men tidrapporter och arbetsgivarintyg är felaktiga.

Åklagarmyndigheten skiljer i ett rätts-pm mellan två typer av assistansbedrägerier (Åklagarmyndigheten 2015). Det första kallas utnyttjandefall; där utnyttjar assistenter, anordnare eller gode män en brukare med reella assistansbehov. Brukaren omges av en liten krets personer, ofta anhöriga, vilket minskar risken för att någon tipsar myndigheterna om brottsligheten och försvårar att brukaren får adekvat hjälp (ISF och Brå 2011:12, Åklagarmyndigheten 2015, Brå 2015:8).

I vissa fall samarbetar flera gärningspersoner vilket försvårar upptäckt. Någon, exempelvis en assistent, god man eller anordnaren, för brukarens talan mot sjukvårdspersonal och myndigheter. Anordnarnas faktiska kostnader för assistansen hålls på en minimal nivå genom låga löner och i vissa fall svartavlönade assistenter. Exempel finns i forskningen där den utbetalade redovisade lönen – som bygger på de uppgifter som lämnas till Försäkringskassan i tidrapporterna – tas ut i kontanter och lämnas tillbaka till organisatören (ISF och Brå 2011:12).

Den andra kategorin kallas simulantfall (Åklagarmyndigheten 2015). Där är brukaren aktiv i bedrägeriet och överdriver eller konstruerar sitt assistansbehov. Rättsfall finns där assistenter eller anordnare har duperats av sådana brukare och inte varit medvetna om brottsligheten (Brå 2015:8, ISF och Brå 2011:12, Åklagarmyndigheten 2015). Där har fiktiva assistenter eller vänner till brukaren fått lön och lämnat över hela eller delar av beloppen till brukaren.

Arbetslöshetskassorna

Det finns 28 arbetslöshetskassor i Sverige. De skiljer sig från exempelvis Försäkringskassan genom att de är medlemsorganisationer, inte en myndighet.

När det gäller bidragsbrott mot arbetslöshetsersättningen handlar fallen i ärendegranskningen om att medlemmen inte varit arbetslös eller om att den lämnat felaktiga uppgifter för att inte drabbas av vad den troligen ser som bristfälliga regelverk. I det senare fallet finns exempelvis en misstänkt som lämnat ett felaktigt intyg som säger att anställning upphört till följd av arbetsbrist – när det i själva verket var den misstänkte som sade upp sig. Detta intyg syftade till att få arbetslöshetsersättning och slippa en längre karenstid som man riskerar om man själv har sagt upp sig.

I ett par ärenden har de misstänkta inte redovisat deltidsarbete – för att komma runt regelverken om deltidsersättning. Oklarheter om hur regelverket säger att man ska räkna antal timmar finns också för personer som arbetar som frilans eller i ett fall som tolk. Här har det funnits olika syn från medlem respektive arbetslöshetskassa på vad som är en arbetstimme. I dessa fall har kassakorten varit felaktigt ifyllda, vilket föranlett polisanmälan.

Det vanligaste i ärendegranskningen är dock att de misstänkta har haft arbetslöshetsersättning samtidigt med andra ersättningar. Det har varit ersättning för sjukdom eller föräldrapenning från Försäkringskassan och studiestöd från CSN. Det finns också en handfull ärenden där personen arbetat svart eller vitt samtidigt som den har haft arbetslöshetsersättning. Ett av ärendena kretsar kring en oklar näringsverksamhet. Den misstänkte uppger att den säljer saker på en säljsajt för att kunna betala sina skulder etc. Till följd av sin ekonomi kan personen inte få F-skattsedel och bedriva näringsverksamhet, men Skatteverket menar att hans omsättning är av sådan storlek att det blir fråga om företagande. Det är Skatteverket som meddelar arbetslöshetskassan om detta arbete.

Ytterligare ett exempel från anmälningarna är att man funderar på att starta ett företag och testar att bygga upp det för att se om det bär sig medan man uppbär arbetslöshetsersättning. Medlemmar som inte upplever att deras livssituation speglar regelverken är något som också framgick i en annan studie (Brå 2007:23). Ett exempel från den tidigare studien var personer som studerade på prov, med arbetslöshetsersättning i stället för studiemedel.

Andra skäl som framkommer i ärendegranskningen tycks vara språksvårigheter, okunskap om regelverken och att det i själva verket är någon *annan* som fyllt i handlingarna och lämnat oriktiga uppgifter.

Kommunerna

De 290 kommunerna är det sista skyddet för medborgarna. Om man saknar inkomster eller har väldigt låga inkomster, samtidigt som man inte uppfyller villkoren för exempelvis bidrag från Försäkringskassan är det kommunernas ekonomiska bistånd som kan bli aktuellt.

Ärendena i ärendegranskningen som rör ekonomiskt bistånd handlar dels om att bidragstagaren har andra dolda inkomster, dels att den uppgett för höga kostnader för hyra. I fallen med andra inkomster handlar det om svartarbete, deltidsarbete eller studier. I något fall finns från den misstänktes sida oklarheter om vad man får ha för inkomster parallellt med ekonomiskt bistånd. Ett exempel på detta är en person som pantsatt smycken, men

inte insett att det räcker med en sådan liten ”inkomst” för att kommunen ska reducera det ekonomiska biståndet. I vissa av dessa ärenden har den sökande sannolikt visat upp felaktiga kontoutdrag som döljer inkomster (Brå 2015:8).

Den andra kategorin, som avser hyran, handlar om att personen har haft sambo eller inneboende – men inte uppgett dessa i sin ansökan och därmed fått för mycket pengar för hyran. I vissa av ärendena är det tydligt att personerna av olika skäl är skuldsatta eller upplever att de har svårt att klara sig på pengarna från socialtjänsten och därför söker extrainkomster. Skulderna är ett uttryck för att de länge har haft ont om pengar och lånat och tagit krediter, men de kan även vara en följd av exempelvis ett missbruk.

Slutligen finns några tidigare identifierade former av bidragsbrott mot kommuner som saknas i urvalet. En tidigare Brå-rapport har noterat fusk med olika typer av kvitton, exempelvis kvitton för läkemedelsinköp eller kostnader för flytt för att få engångssummor felaktigt utbetalda från kommunen (Brå 2015:8). En annan studie lyfter även fusk med hemtjänst, där kommunen betalar ut ersättning för fler timmar än vad som motsvarar det utförda arbetet (Rönnblom, Skinnari och Korsell 2015). Enstaka härvor har avslöjats där klienterna är med på bedrägerierna. Deras anhöriga rapporterar arbetade timmar mot att få sjukpenninggrundande inkomst. På så sätt liknar brotten dem som begås med assistansersättning.

Övriga myndigheter

I det granskade materialet finns ett ärende från Pensionsmyndigheten, och det rör misstänkt brott med efterlevandestöd. Det är ett stöd som går till barn, vars föräldrar inte lever. I detta fall var mamman inte alls avliden, utan har agerat som en äldre släkting till barnet och ansökt om efterlevandestöd. Falska dödsfallsintyg förekommer ibland i dessa ärenden (Brå 2015:8). Eftersom barnet självt är minderårigt och inte ansökt om stödet är det den vuxne som ansökt om stödet som misstänks för brottet.

I de ärenden i ärendegranskningen och intervjuer som rör CSN har personer uppgett att de ska studera utomlands, men studierna har aldrig genomförts. I ett fall var syftet aldrig att studera utan studiemedlen användes till att betala skulder. I ett annat ärende kan den misstänkte ha haft avsikter att studera, men studierna har i vart fall inte genomförts. Som skäl hänvisar den misstänkte till bristande hälsa, och läkarintyg som ska styrka detta bifogas. Dessa resultat är också i linje med resultaten i en tidigare studie, där fler ärenden från CSN ingick (Brå 2015:8).

Ärendena mot Arbetsförmedlingen är nästan helt frånvarande i ärendegranskningen, av de skäl som tidigare angetts i rapporten – myndigheten hanterar primärt ersättningar som inte är för personligt ändamål. Arbetsgivarstöden och deras övriga program riktar sig till företag, för att exempelvis kompensera för att de anställer personer som står långt från arbetsmarknaden. Det fanns visserligen tecken på bedrägerier med nystartsjobb i ett uppklarat fall som kommit med i urvalet eftersom det också innehåller bidragsbrott mot Försäkringskassan. Delen som rör Arbetsförmedlingen är med andra ord ett brottsbalksbedrägeri, men beskrivs här eftersom det handlar om utbetalningar från välfärden.

En tidigare statlig utredning har konstaterat att det finns arbetsgivare som systematiskt utnyttjar arbetsgivarstöden (SOU 2014:16, jfr även Statskontoret 2009:13). Enligt en tidigare studie är det typiska fallet att en arbetsgivare anställer personer och uppger att de har högre löner eller mer arbetstid än vad som är fallet. Arbetsgivaren får därför ut mer ersättning än den har i faktiska lönekostnader (Brå 2015:8, se även kapitlet Identitetsmissbruk). Mer erfarna arbetsgivare håller papper och ansökningar i ordning och redovisar skatter och avgifter, även om de inte betalas in som de ska. I de grövsta fallen har den ”anställde” inte alls arbetat, utan förekommer bara på pappret, för att säkra upp ersättning från Arbetsförmedlingen (Brå 2015:8, Brå 2011:7). Exempel finns också där det är oklart om lönerna faktiskt har betalats ut – eftersom den anställde har fått kontant lön och handskrivna lönespecifikationer – som snarare liknar kvitton (Brå 2015:8).

Slutligen nämner tidigare studier även fusk med den statliga lönegarantin, som betalas ut av sju av landets länsstyrelser. Här består felaktigheterna i att personer som aldrig arbetat, alternativt arbetat svart på ett företag, skrivs in som anställda inför en konkurs. En konkursförvaltare fattar beslut om lönegaranti och den betalas ut till de ”anställda”. När detta sker med enskilda personer i företag som blandar svart och vit verksamhet kan det vara mycket svårt för myndigheterna att upptäcka (Brå 2011:7). Det finns också fall där gärningspersonerna har kapat/lånat identiteter och anställt personer som inte finns (Brå 2015:8). Genom att ha bankkonton och internetbank i dessa identiteters namn har gärningspersonerna själva tagit pengarna.

Gärningspersonerna

I 47 av de 50 ärendena som rör bidragsbrott fanns en misstänkt gärningsperson, i resten flera. Gärningspersonernas kön framgår i 49 av ärendena. I 31 fall var det enbart män, i 15 enbart kvinnor. I tre ärenden fanns både kvinnor och män bland de misstänkta personerna. Det innebär att männen är något överrepresenterade

i Brås urval, eftersom statistiken över misstänkta personer visar en mer jämn fördelning mellan kvinnor och män.

De misstänkta personerna var mellan 21 och 61 år gamla vid det sista brottstillfället som finns med i utredningen. Medelåldern var högre än vid brottsbalksbedrägerier, 41 år.

I det följande beskrivs gärningspersonerna vid bidragsbrott och välfärdsbedrägerier djupare, eftersom de till viss del skiljer sig från andra bedrägerier. Inte minst inslaget av ”vanliga” bidragstagare som slarvat skiljer sig från brottsbalksbedrägerierna. De mest organiserade härvorna påminner om och kan även vara del av omfattande faktura- eller kreditbedrägerier. Vilka är då brottslingarna? De granskade ärendena ger samma bild som intervjuer och tidigare studier. Här beskrivs de något förenklat som tre kategorier.

Kategori 1: Låg regelförståelse, slarv och personlig kris
Den klart dominerande gruppen av de tre är inte några brottsbelastade eller aktivt kriminella personer. Tvärtom andas förundersökningar, domar och intervjuer att det är ”vanliga” medborgare där livet kom lite emellan. Den tidigare i rapporten redovisade statistiken visar samma sak; jämfört med andra bedragare har bidragsbrottslingar låg tidigare brottsbelastning.

De misstänkta pratar i förhören om att de befann sig i en svår period i livet, det var därför de behövde bidragen. Exempel från ärenden och intervjuer handlar om svåra situationer i arbetet, där det egna företaget inte bär sig eller man till slut säger upp sig själv för att man inte klarar av att vara kvar. Andra fall handlar om för tidigt födda eller sjuka barn, skulder, missbruksproblem. Till detta kommer att de misstänkta har svårt att förstå myndighetssvenskan, språket som beskriver villkoren för förmånerna och hur man fyller i blanketter. Detta resulterar också i att de bett andra personer om hjälp och ibland fått dåliga råd om villkoren för bidraget samt hur de ska fylla i blanketterna.

En mellanvariant mellan de ”vanliga” medborgarna och mer kvalificerade bidragsbrottslingar exemplifieras av en intervjuperson. Han beskriver hur han tidigt blev skuldsatt genom ett återkrav från CSN. Det var inget han planerat att göra, utan han hade för mycket frånvaro, vilket upptäcktes först efter att många utbetalningar hade gjorts. Hans bild var att myndigheterna generellt var snabbare i dag med att stoppa utbetalningar och därmed undvika stora återkrav. Han hade inga ekonomiska förutsättningar att betala av detta, utan fortsatte i kriminalitet och gjorde sig skyldig till bidragsbrott med andra bidrag. På så sätt övergick han till att bli en mer planerande bedragare.

Kategori 2: Pengar från välfärdssystemen, ibland också från andra brott

De mer planerande och kvalificerade bidragsbrottslingarna syns i de granskade ärendena, intervjuer och tidigare forskning. Denna andra kategori består av personer som lärt sig brotten och hur man utnyttjar välfärdssystemen av vänner eller familj. Ärendena på detta tema innehåller personer som arbetar svart i stor omfattning och har en hel ersättning från Försäkringskassan, kommunen eller en arbetslöshetskassa.

Det förekommer även att man i större omfattning kombinerar olika bidrag. Sådana personer har exempelvis arbetslöshetsersättning, ekonomiskt bistånd, föräldrapenning eller sjukpenning samtidigt som de har skenseparerat och på så sätt får för högt bostadsbidrag och kanske också underhållsstöd. Eftersom vissa begår brott mot såväl Försäkringskassan som andra aktörer som arbetslöshetskassan eller kommunen kan det vara svårt för de utbetalande organisationerna att utreda och slå fast de felaktiga utbetalningarna. Även om handläggaren har fattat misstankar på basis av personernas beteende ser de inte nödvändigtvis hela bilden, brotten kan mycket väl riktas mot en annan organisation. Utbetalningen från Försäkringskassan kan vara korrekt, men den kan inte kombineras med ytterligare utbetalningar. Eller så har man lämnat uppgifter om låga inkomster till kommunen, men tidigare höga inkomster till Försäkringskassan eller arbetslöshetskassan för att få en större utbetalning därifrån.

Som kommer att utvecklas i kapitlet om identitetsmissbruk finns gärningspersoner som har flera identiteter (Brå 2015:8, NUC 2015a). Det innebär att en och samma fysiska person kombinerar arbete och bidrag i olika identiteter och utgör ett tydligt tecken på mer planerade och utstuderade bidragsbrott. Vissa har en ”ren” identitet och begår brott i en eller flera andra identiteter.

I praktiken kan det vara svårt att skilja många kvalificerade bidragsbrottslingar från den första kategorin där uppsåt ibland saknas. Skälet är att gärningspersonerna i denna andra kategori tycks besvara myndighetsfrågor på samma sätt som personerna i den första och skylla på slarv och okunskap. Det blir därför troligen särskilt centralt att de utbetalande organisationerna har dokumenterat väl i ärendet och har blanketter som tydligt beskriver den enskildes ansvar och villkoren för att få bidraget. På så sätt kan man slå hål på bortförklaringar om att gärningspersonen saknar information om vad som är tillåtet med det aktuella bidraget.

I denna andra kategori återfinns också personer som begår andra bedrägerier, skattebrott eller andra typer av brott. Ett sådant exempel som också identifierats i tidigare studier är egenföre-

tagare eller personer som arbetat svart som må ha ett korrekt läkarintyg om sjukskrivning eller de facto är arbetslösa – men som aldrig kvalificerat sig för arbetslöshetsersättning eller en högre sjukpenninggrundande inkomst (se även Brå 2015:8, ISF och Brå 2011:12). De blir bidragsbrottslingar genom ett felaktigt arbetsgivarintyg, som de tar fram på egen hand eller med hjälp av en arbetsgivare eller redovisningsansvarig (för egenföretagarna). Detta intyg visar på en hög lön under tillräckligt lång tid för att generera ett helt felaktigt eller för högt bidrag.

Kategori 3: Brottsplan med företag

Den tredje kategorin består av personer inom lite mer storskalig ekonomisk brottslighet eller organiserad brottslighet, som ofta med hjälp av företag begår välfärdsbedrägerier. Ofta bygger dessa bedrägerier på att gärningspersonerna identifierat kryphål i regelverk eller kontroll och utnyttjar dessa i omfattande skala. Det handlar i princip alltid om bedrägerier från ett par hundra tusen till flera miljoner kronor. När det gäller assistansbedrägerier är välfärdsbedrägeriet ofta huvudbrottet. I övriga fall används Arbetsförmedlingens stöd till företag eller länsstyrelsens lönegaranti som komplement eller en utbyggnad av andra ekobrott. En gärningsperson besvarar frågan om man använder stöd från Arbetsförmedlingen i bolagen som begår bedrägerier:

> *Det händer. Det händer väldigt ofta. De kan anställa folk på lönebidrag, och det är egentligen bara en front för att ge dem mer pengar medan de håller på med såna här grejer [kreditbedrägerier].*

Företagen kan vara assistansanordnare eller företagare i andra branscher som anställer personer som står långt ifrån arbetsmarknaden för att ta del av Arbetsförmedlingens förmåner. I bedrägerifallen arbetar personerna svart eller klart mindre än arbetsgivaren får betalt för. För att organisatörerna, som sällan är arbetstagare i dessa härvor, ska få ut brottsvinsterna gör de sig ofta skyldiga till bokföringsbrott och andra skatterelaterade brott. Till detta kommer att vissa företag används som brottsverktyg i andra bedrägerier.

Exempel finns i både intervjuer och ärenden på att personer anställts som säljare i telemarketing- och andra typer av fakturabedrägerier. Det förekommer också att arbetstagarna luras på sina löner. En gärningsperson pratar också om ett systematiskt utnyttjande av praktikanter från Arbetsförmedlingen. Systematiken är tydlig för gärningspersonerna, men behöver inte vara det för Arbetsförmedlingen då bolagen ständigt byts ut när myndigheterna kommer huvudbrottsligheten (oftast skattebrott) på spåren (jfr även Brå 2011:7). I vissa härvor används också falska

eller kapade identiteter, och dessa närmast ”pappersidentiteter” anställs och genererar bidrag till arbetsgivaren.

När myndigheterna är företagen på spåren sätts bolagen ofta i konkurs, vilket kan medföra bedrägerier med lönegaranti, genom att man ”hittar på” anställda. Med andra ord handlar dessa bedrägerier om att lura alla som kan luras för att få ut så mycket pengar som möjligt, och det är troligtvis Arbetsförmedlingen (som betalar ut anställningsstöden) och länsstyrelsen (som betalar ut lönegarantin) som har sämst möjligheter av alla målsägare att upptäcka brottsligheten, en fråga som vi återkommer till i kapitlet De utbetalande myndigheterna och organisationerna.

Myndigheterna har breddat sin syn på gärningspersonerna
Synen på vilken av de tre typerna av bidragsbrottslingar som ses som ”problemet” har svängt med tiden. Från att ha pratat om att det finns ett visst överutnyttjande i god tro – vilket motsvarar den största och första kategorin, de ”slarviga medborgarna” – har man skärpt språkbruket och pratar om bedrägerier och bidragsbrott (Korsell, Hagstedt och Skinnari 2008, Johnson och Larsson 2011). Det motsvarade länge primärt den andra kategorin, med enskilda personer, vars brott täcks av bidragsbrottslagen. Den tredje kategorin, företag som begår välfärdsbrott har identifierats först de senaste åren (Brå 2015:8, NUC 2015a, SOU 2014:16, SOU 2012:6).

När rättsväsendet tar vid

Hög andel personuppklarade brott jämfört med flera andra bedrägerityper

Jämfört med de flesta brottsbalksbedrägerier är det en relativt hög andel av anmälningarna om brott mot bidragsbrottslagen som lett till personuppklaring (närmare 3 av 10). Sex procent av anmälningarna har lagts ner genom ett beslut om förundersökningsbegränsning och ytterligare åtta procent av anmälningarna var fortfarande under utredning i slutet av 2014 (tabell 18).

Det som skiljer bidragsbrotten från många av de tidigare beskrivna bedrägerierna är att det inte är en enskild person som kontaktar polisen och anmäler ett brott. De utbetalande myndigheterna och organisationerna har egna kontrollutredare eller motsvarande som sammanställer den information som finns om brottet och lämnar in en polisanmälan, ofta via brev. Dessutom är gärningspersonen i de allra flesta fall känd – det är personen som har fått bidraget utbetalt till sig. Det är faktorer som gör mediantiden till åtal eller strafföreläggande kort i jämförelse med många brottsbalksbedrägerier.

Trots de anmälande myndigheternas förarbete är dock inte uppklaringen hundraprocentig. Det finns trots allt vissa svårigheter för polis och åklagare.

Tabell 18. Personuppklaringsbeslut, ärenden fortfarande under utredning och nedlagda ärenden efter nedläggningsorsak. Brott mot bidragsbrottslagen. (n = 50)

	Antal	Procent
Personuppklarade ärenden	**14**	**28**
Åtal	11	22
Strafföreläggande	3	6
Fortfarande under utredning 2014-12-31	**4**	**8**
Nedlagda ärenden*	**32**	**64**
Preskriberat	1	2
Ej brott	5	10
Misstänkt lämnat landet	3	6
Bevisproblem (misstänkt identifierad)	20	40
Förundersökningsbegränsning	3	6
Totalt	**50**	**100**

* För en beskrivning av hur nedläggningsbesluten har kodats, se bilaga 2.

Bevisproblem den vanligaste anledningen till nedläggning

Den enskilt vanligaste anledningen till att anmälningar om brott mot bidragsbrottslagen har lagts ner av polisen eller åklagare är bevisproblem. Ibland visar nedläggningsmotiveringen att det beror på att det inte ansetts möjligt att styrka de objektiva rekvisiten för brottet, till exempel att man inte kunnat visa vad bidragstagaren haft för inkomst vid sidan om bidraget. I flera fall handlar det emellertid om problem med att styrka att den misstänkte haft uppsåt eller varit tillräckligt oaktsam för att kunna åtalas för brott. Det kan till exempel handla om att man tagit emot ekonomiskt bistånd från kommunen samtidigt som man haft en person inneboende, utan att ha insett att man skulle rapporterat detta. Andra exempel är att man inte förstått att försäljning av varor via annonssidor på internet skulle räknas som inkomst, eller att den misstänkte menat att det alltid varit meningen att rapportera in ändrade förhållanden till arbetslöshetskassan, men att man gjort det för sent.

Ibland framgår att beslutet att lägga ner förundersökningen har baserats på en kombination av uppsåtsbedömningen och en bedömning av brottets grovhet. I dessa fall har det inte ansetts styrkt att gärningen begåtts uppsåtligen, och brottet har inte

ansetts tillräckligt allvarligt för att föranleda ansvar för vårdslöst bidragsbrott enligt 4 § bidragsbrottslagen. I enstaka ärenden i Brås material har polisen lagt ner anmälan med en anmärkning om att underlaget från den utbetalande myndigheten är för bristfälligt för att kunna styrka brottet.

De ärenden som ingår i kategorin *ej brott* avser anmälningar som antingen lagts ner av åklagare med motiveringen att det handlar om ringa fall, eller som lagts ner av polisen med motiveringen att det inte finns anledning att tro att den misstänkte har begått brott som hör under allmänt åtal. Det handlar bland annat om ärenden där den misstänkte mottagit försörjningsstöd under ett fåtal dagar och samtidigt haft en annan inkomst, eller där den misstänkte skickat in ifyllda kassakort, och sedan blivit förälder och fått både föräldrapenning och utbetalningar från arbetslöshetskassan under en kortare period.

Större inslag av systematik bland de ärenden som lett till personuppklaring

Ett ganska tydligt mönster i materialet är att andelen anmälningar som avser felaktiga utbetalningar som pågått under längre tid är betydligt högre bland de ärenden som resulterat i personuppklaring än bland de nedlagda. Bland de anmälningar som lett till åtal eller ett strafföreläggande är det 9 av 14, eller över 60 procent, som ingår i utredningar som avser misstänkta som tagit emot felaktiga utbetalningar under en period av mer än ett år. Detsamma gäller för tre av de fyra anmälningar som fortfarande var under utredning i slutet av 2014. Motsvarande andel bland de anmälningar som lagts ner är 20 procent. En inte orimlig förklaring till detta mönster är att systematiken kan användas för att visa att det funnits uppsåt.

När åtal väckts

Brås särskilda urval av domar innehåller 18 domar avseende bidragsbrott. De flesta domar avser en enda tilltalad, och könsfördelningen bland de tilltalade är ganska jämn, med en viss övervikt av män. Domarna domineras av brott mot arbetslöshetskassorna (8 st.) respektive Försäkringskassan (7 st.). Två domar avser brott mot CSN, en avser brott mot kommunerna.

Domarna speglar variationen i de anmälda brotten

De bidragsbrott som beskrivs i domarna speglar den stora variation som beskrivits ovan med utgångspunkt i de anmälda brotten. Brotten mot arbetslöshetskassorna avser framför allt ärenden där gärningspersonerna samtidigt fått andra typer av ersättningar i

form av föräldrapenning, sjukpenning eller utbetalningar från CSN. I enstaka ärenden har gärningspersonen anmält sig som heltidsarbetslös till arbetslöshetskassan och samtidigt arbetat på deltid.

Brotten mot Försäkringskassan avser felaktigt utbetalda ersättningar i form av bostadsbidrag eller bostadstillägg, underhållsstöd, sjukersättning eller föräldrapenning. En av domarna avser en större assistansbedrägeriutredning. I domen avseende bidragsbrott mot kommunerna har två tilltalade ansökt om försörjningsstöd utan att uppge inkomster i form av CSN-utbetalningar respektive arbetslöshetsersättning. Brotten mot CSN avser personer som har beviljats och fått studiemedel för studier utomlands och som sedan behållit pengarna trots att studierna inte har genomförts.

Stor variation i storleken på de felaktiga utbetalningarna

Det finns en stor variation i värdet på de felaktiga utbetalningarna som framgår av domarna, från närmare 8 000 kronor till flera miljoner, med ett medianbelopp på drygt 40 000 kronor. Omfattningen av de felaktiga utbetalningar är generellt något lägre för brotten mot arbetslöshetskassorna (där medianbeloppet är drygt 18 000 kronor), jämfört med brotten mot Försäkringskassan (där medianbeloppet ligger på drygt 90 000 kronor). Det finns tre domar i materialet där värdet på den åtalade brottsligheten uppgår till över 100 000 kronor. Två av dessa avser felaktiga utbetalningar av sjukersättning över en längre period, den tredje avser det ovan nämnda assistansbedrägerimålet.

Främst skriftlig bevisning som åberopas

Bevisningsunderlaget i målen varierar beroende på den typen av bidragsbrott som målen avser. Utöver förhör med den tilltalade består underlaget framför allt av skriftlig bevisning. Exempel är kontoutdrag, intyg om studier eller om att man inte påbörjat studier, handlingar som styrker att den tilltalade haft ett arbete eller ansökningar om parallella ersättningar vid andra myndigheter. I vissa mål förekommer även vittnesförhör med exempelvis socialsekreterare eller handläggare från den utbetalande myndigheten.

Assistansbedrägerimålet utgör ett undantag både när det gäller antalet tilltalade personer och omfattningen av bevisningsunderlaget. Målet utgör ett exempel på ett så kallat utnyttjandefall, där åtal väcktes mot ett flertal personer inklusive företrädare för ett assistansföretag och assistenter, för att dessa lämnat oriktiga uppgifter till Försäkringskassan avseende vem som utfört assistans och hur många assistanstimmar som utförts av olika personer. Vissa av de tilltalade åtalades även för bokföringsbrott och skattebrott. Enligt åklagaren hade brottsligheten pågått i flera år

och bevisningen i målet innehöll, utöver förhör med de tilltalade och vittnen, mycket omfattande skriftlig bevisning med alltifrån tidrapporter, protokoll från personalmöten, kontrolluppgifter och skattedeklarationer till it-forensiska analyser av datorer och utskrifter från avlyssnade telefonsamtal. Huvudförhandlingen i detta mål pågick i över sex veckor, vilket kan jämföras med de övriga målen avseende bidragsbrott, där stämningsansökan i de flesta fall skattade att handläggningstiden i rätten skulle uppgå till mellan 45 minuter och, i undantagsfall, en heldag.

Fällande domar för bidragsbrott i de flesta mål

I de flesta mål dömdes de tilltalade för bidragsbrott i enlighet med åtalet. Åtalen för bidragsbrott ogillades i fyra av målen. I tre av dessa mål, som avsåg felaktiga utbetalningar av studiemedel, sjukersättning respektive arbetslöshetsersättning ansåg tingsrätten att det inte var visat att de tilltalade hade lämnat de oriktiga uppgifterna uppsåtligen. I det ena fallet handlade det om att den tilltalade hade lidit av psykiska problem vid den tidpunkt då uppgifterna hade lämnats, medan rätten i de övriga två fallen ansåg att det inte var bevisat att de tilltalade hade varit medvetna om villkoren för den utbetalade ersättningen respektive om sina skyldigheter att anmäla förändrade förhållanden.

Samtliga åtalspunkter avseende bidragsbrott ogillades även i det stora assistansbedrägerimålet. Enligt rätten var det styrkt att oriktiga uppgifter hade lämnats till Försäkringskassan om vilka som utfört assistans och i vilken omfattning. Försvaret hade dock invänt, att även om uppgifterna i de tidrapporter som lämnats till Försäkringskassan var oriktiga, så hade assistans ändå lämnats till de aktuella brukarna i den utsträckning som hade redovisats till Försäkringskassan, men av andra personer. Tingsrätten ansåg att åklagarens utredning inte hade vederlagt denna invändning. Det innebar i sin tur att det inte var klarlagt att de oriktiga uppgifterna som lämnats till Försäkringskassan hade medfört någon fara för att för mycket assistansersättning skulle betalas ut. Rättens slutsats var därför att det objektivt sett inte hade begåtts något bidragsbrott.

Enligt Åklagarmyndigheten (2015) överklagades denna dom först till hovrätten, som fastställde tingsrättens dom med avseende på bidragsbrotten, och därefter till Högsta domstolen, som inte meddelade prövningstillstånd. Inom ramen för ett projekt gällande assistansbedrägerier fann Utvecklingscentrum Stockholm (ibid.) att åklagare och poliser ansåg att rättsläget hade blivit problematiskt till följd av denna dom. Det har sedan dess kommit en annan dom som säger att enbart de som försöker förmå Försäkringskassan att felaktigt betala ut ersättning har ett intresse av att så genomgående lämna oriktiga uppgifter.

Del 3. Fördjupningskapitel om aktörer och verktyg

Hittills har bedrägeribrottslighetens omfattning och struktur beskrivits särskilt på basis av anmälningar, förundersökningar, domar och befintlig statistik – med stöd i annan forskning. För att få en djupare förståelse av dessa brott kommer nu fem kapitel som fördjupar några centrala aspekter hos brottsligheten. I det första kapitlet beskrivs vilka som drabbas av bedrägerier och vilka gärningspersonerna är. Eftersom materialet innehåller intervjuer med just gärningspersoner får de i slutet av kapitlet själva komma till tals.

Efter detta följer ett kapitel om identitetsstölder och andra former av identitetsmissbruk, som var en särskild del av uppdraget. Som redan framgått förutsätter eller underlättas många bedrägerier av identitetsmissbruk.

Lika centralt för att förstå bedrägeribrottens struktur som för att föreslå förebyggande åtgärder är det att analysera näringslivets roll i sammanhanget. Då den sällan framgår av statistik eller granskade ärenden, utgår kapitlet framför allt från intervjuer som ger en bild av hur näringslivet skapar möjligheter till och berörs av bedrägerier.

Denna del av rapporten avslutas med två kapitel som tar sikte på hur bedrägerierna hanteras av myndigheterna. För det första beskrivs hur utbetalande myndigheter och organisationer själva upptäcker och utreder bidragsbrott, som sedan anmäls. Vidare beskrivs hur bedrägerier hanteras av rättsväsendet. Dessa analyser blir sedan en brygga till rapportens slutsatser och förslag.

Brottsutsatta och gärningspersoner

I detta kapitel beskrivs först de utsatta utifrån statistik och granskade ärenden. Sedan följer ett avsnitt om gärningspersonerna, som till stor del bygger på intervjuer med bedragare.

Vilka är de som drabbas av bedrägeribrott?

Mindre könsskillnad i utsattheten än vid andra brott, enligt NTU

Som redovisats tidigare (kapitlet om Bedrägerier enligt befintliga källor) har det under stora delen av den för NTU aktuella mätperioden varit en något större andel män än kvinnor som uppgett att de utsatts för bedrägeri, men 2014 var andelarna för första gången nästan lika stora oavsett kön (3,1 % för män, 3,0 % för kvinnor).

Till skillnad från övriga brott mot enskild person, som riktar sig mest mot yngre, fördelas utsatthet för bedrägerier relativt jämnt mellan åldersgrupperna, med högsta nivån i åldersgruppen 45–54 år enligt den senaste mätningen. Åren fram till dess var det dock unga vuxna i 20–34 års ålder som rapporterade högst utsatthet. Personer över 65 år är minst utsatta. Vidare uppger utrikes födda personer och de med två utrikes födda föräldrar att de utsatts för bedrägeri i något större utsträckning än inrikes födda med minst en inrikes född förälder. Ensamstående drabbas, enligt egen uppgift, i högre grad än sammanboende personer, liksom boende i flerfamiljshus drabbas oftare än boende i småhus. Dessutom rapporterar personer som bor i storstadsregionerna en högre bedrägeriutsatthet än bosatta i övriga delar av landet (Brå 2016:1).

På flera sätt tillhör alltså personer som uppger sig ha blivit utsatta för ett bedrägeri samma sociodemografiska grupper som personer som tenderar att oftare utsättas för annan traditionell brottslighet. Samtidigt är fördelningen enligt den senaste mät-

ningen mycket jämn beträffande både kön och ålder, vilket skiljer bedrägerier från många andra brott mot enskilda personer.

Nedan beskrivs personer som figurerar som anmälare eller målsägare i de ärenden som Brå har granskat.

Anmälda bedrägerier: Anmälare, målsägare och de som lidit ekonomisk skada

I de flesta granskade ärenden var målsägare samma person (eller företag/myndighet) som den som anmält brottet, dock inte alltid (se tabell 19). Det är dessutom inte alltid enbart den som lidit ekonomisk skada som får en målsägarstatus. Målsägare i de granskade ärendena är oftast privatpersoner, men även företag har ibland registrerats som målsägare – framför allt vid fakturabedrägerier. Kortbedrägerier anmäls exempelvis nästan alltid av privatpersoner som också initialt registreras som målsägare, men från domarna framgår att de som registreras som målsägare i tingsrätten vanligen är även banker, kortutgivare, företag inom handeln eller företag vilkas kontokort har missbrukats. Det är också främst banker, kortutgivare och företag inom handel som

Tabell 19. Sammanfattande tabell över anmälare, målsägare och de som lidit ekonomisk skada vid olika kategorier av polisanmälda bedrägeribrott.

	Brotten anmäls framför allt av:	Målsägare i tingsrätten är:	Vilka som lidit förlusten
Annonsbedrägerier	Privatpersoner	Privatpersoner	Privatpersoner
Fakturabedrägerier	Företag(are)/ privatpersoner	Företag(are)/ privatpersoner	Företag(are)/ privatpersoner
Kortbedrägerier	Privatpersoner	Kortutgivare/ banker Företag inom handeln Privatpersoner Andra företag (då företagskort använts)	Främst banker/kortutgivare/företag inom handeln
Kreditbedrägerier	Privatpersoner	Kreditföretag Faktureringsbolag Finansbolag/ Banker Företag inom handeln Privatpersoner (främst ID-bestulna)	Kreditföretag Faktureringsbolag Finansbolag/ Banker Företag inom handeln
Övriga telefon- och internetbedrägerier	Privatpersoner	-	Privatpersoner, företag
Brott mot välfärden	Utbetalande myndigheter och organisationer	Utbetalande myndigheter och organisationer	Utbetalande myndigheterna, organisationerna och skattebetalarna

de facto får stå för den ekonomiska förlusten. Privatpersoner drabbas främst på andra sätt, genom att deras identitet eller kort har missbrukats.

Ett liknande scenario finns även vid kreditbedrägerier; privatpersoner anmäler ofta och kan initialt registreras som målsägare i utredningen. I rätten blir det sedan även kreditföretag, faktureringsbolag, finansbolag eller företag inom handel som figurerar som målsägare. Det är också dessa som typiskt sett lider en ekonomisk förlust. Beträffande övriga telefon- och internetbedrägerier är det nästan uteslutande privatpersoner som anmäler och lider ekonomisk skada. Även företag kan drabbas. Då inga granskade ärenden av denna typ hamnat i tingsrätten saknas information om vilka som registreras som målsägare.

När det kommer till bidragsbrott och övriga välfärdsbedrägerier är det de utbetalande myndigheterna och organisationerna som anmäler brottet till polisen. Dessa är också målsägare i de fall som kommer till rätten. Vem som lider en ekonomisk skada är här mer diffust, men då brotten avser bedrägligt bruk av skattemedel kan det konstateras att de, indirekt, drabbar allmänheten.

För att summera drabbar bedrägeribrottsligheten många olika delar av samhället. Även om det är privatpersoner som lägger märke till bedrägerier riktade mot deras ekonomi är det i slutändan inte alltid de som blir ekonomiskt lidande. I många fall är det olika delar av näringslivet som lider en ekonomisk skada. Privatpersoner drabbas självfallet också – både ekonomiskt men även på andra sätt, genom konsekvenser som exempelvis identitetsstöld kan leda till.

I det följande beskrivs egenskaper, i huvudsak kön, ålder och relation till gärningspersonen, hos de privatpersoner som registrerades som målsägare i de granskade ärendena (om information fanns).

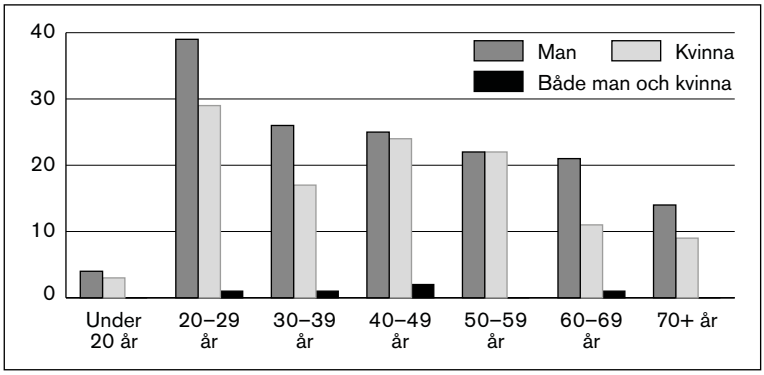
Unga män den enskilt största målsägargruppen

Figur 5 visar antal kvinnor respektive män inom olika ålderskategorier i samtliga granskade ärenden som avser brottsbalksbedrägerier. I 275 (närmare 70 procent) av ärendena fanns uppgifter om målsägarens ålder. Sammanlagt 8 procent av de utsatta var över 70 år, den äldsta var 96 år gammal.

I samtliga åldrar är det män som dominerar bilden, men skillnaden är störst bland yngre och äldre, det vill säga personer under 40 år respektive 60 år eller äldre. I synnerhet bland äldre tycks män vara överrepresenterade. Utan hänsyn till kön är det samtidigt tydligt att det, trots de äldres generellt sett större sårbarhet,

framför allt är unga personer som drabbas – eller oftare anmäler sin utsatthet. Män i 20–29 års åldern är den enskilt största gruppen av målsägare i det studerade materialet. Kreditbedrägerier och kortbedrägerier står tillsammans för hälften av ärendena med unga män som målsägare.

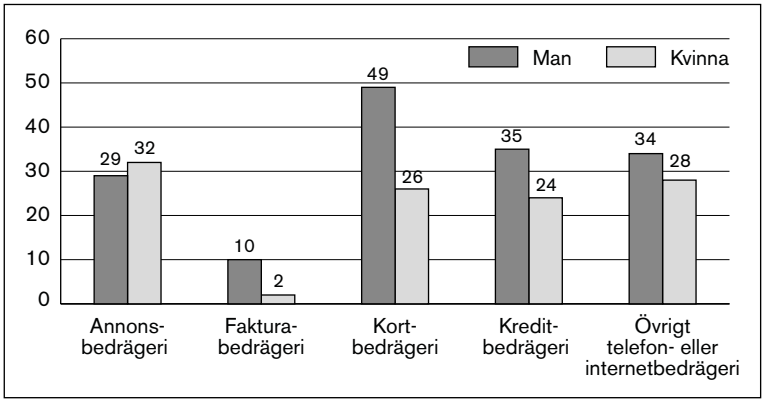
Figur 5. Antal manliga och kvinnliga målsägare inom olika ålderskategorier. Brottsbalksbedrägerier. Polisanmälda ärenden första halvåret 2013.



Fler manliga målsägare vid kort- och kreditbedrägerier

Det finns relativt sett något fler män (56 procent) än kvinnor bland målsägare i de bedrägeriärenden som riktats mot privatpersoner och där uppgifter om målsägarens kön finns (325 ärenden, inklusive kategorier av övriga bedrägerier). Könsskillnaden är störst vid kort- och kreditbedrägerier, genom att betydligt fler män är målsägare vid dessa brott. Beträffande kortbedrägerier är antalet manliga målsägare nästan dubbelt så högt jämfört med kvinnliga, som framgår av figur 6.

Figur 6. Antal manliga och kvinnliga målsägare per bedrägerityp. Polisanmälda ärenden första halvåret 2013.



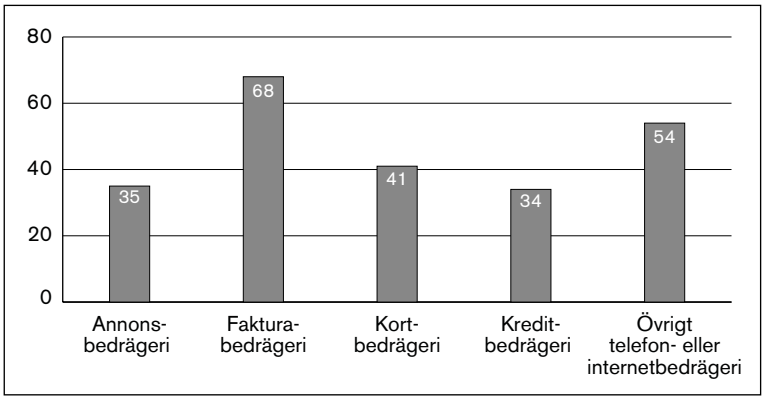
Åldringsbrott: De flesta målsägare är unga, men äldre utgör en sårbar grupp

Bedrägerier mot äldre har särskilt uppmärksammats i forskningen (t.ex. Youngblood 2015), då en persons höga ålder kan underlätta vilseledandet i vissa fall – exempelvis i samband med kontokortstölder eller vid avtalsrelaterade fakturabedrägerier där någon form av kontakt har förekommit. Enligt Nationellt bedrägericenter (NBC) ökade bedrägerier mot äldre år 2014 med hela 40 procent och den uppåtgående trenden höll i sig under första halvåret 2015. Under andra halvåret skedde däremot enligt NBC en stor minskning i inflödet av anmälda bedrägeribrott mot äldre (NBC 2015a). NBC har under 2015 koordinerat samverkan med PRO, SPF Seniorerna och BOJ för att ta fram en nationell preventiv strategi i syfte att minska bedrägerier mot äldre. Arbetet har resulterat i ett utbildningspaket som lanserades under hösten 2015.

Vilseledda genom direkt kontakt

Medianåldern i samtliga granskade bedrägeriärenden var 43 år, men som framgår i figur 7 så är det framför allt vid fakturabedrägerier och övriga telefon- och internetbedrägerier som målsägarens ålder ligger betydligt högre. Vid fakturabedrägerier är medianåldern 68 år och i samband med övriga telefon- och internetbedrägerier motsvarar den 54 år. När det gäller den sistnämnda kategorin är det framför allt bedrägerier där gärningspersonen låtsas vara en vän i nöd, som anmälts av äldre personer.

Figur 7. Målsägarens medianålder i ärenden gällande brottsbalksbedrägeri. Polisanmälda ärenden första halvåret 2013.



Vid fakturabedrägerier är det främst de fall där någon form av kommunikation ägt rum innan och där det hänvisas till avtal.

Liksom vid ”vän i nöd”-bedrägerierna påbörjas alltså vilseledandet med en direkt kontakt, som enligt följande anmälan:

> *Målsägaren har försökt säga upp fakturan från [företag] genom att hänvisa till de 14 dagar som ska stå i avtalet (troligen tecknat via telefon), men företaget hänvisar till 12 månader. I det bifogade avtalet står 12 mån ikryssat. Målsägaren, en äldre man, säger att han redan har ett annat telefonabonnemang. Har försökt att bestrida fakturorna men de fortsätter att komma.*

Intervjuade poliser bekräftar det litteraturen visar, att äldre i relativt stor utsträckning drabbas även av olika former av kortbedrägerier (CP), t.ex. shoulder-surfing (se avsnittet om Kortbedrägerier) eller en stöld av bankkort med påföljande uttag eller köp. Då just kortbedrägerier i sig är en mycket omfattande kategori avspeglas dock detta inte i ålderns medianvärde. Det finns dock flera fall av just shoulder-surfing mot äldre i det granskade materialet, liksom ett antal andra kortbedrägerier (CP).

Utifrån polisens bedrägeriärenden är det sammanfattningsvis främst unga som är målsägare vid brottsbalksbedrägerier, något som även korresponderar med resultat från NTU. Skälet är troligen att unga i större uträckning använder internet för sina transaktioner, samt kan vara mer kreditstarka. Å andra sidan är äldre sannolikt mer sårbara för de typer av bedrägerier som innebär ett mer aktivt vilseledande från gärningspersonens sida, där någon form av direkt kontakt äger rum. På så sätt utgör målsägarens höga ålder ett direkt led i det bedrägliga förfarandet, vilket motiverar mer riktade preventiva åtgärder.

Relation mellan bedragaren och den utsatte

I 32 (8 procent) av de granskade ärendena fanns uppgifter om att målsägaren inte var helt obekant med gärningspersonen. Som tidigare nämnts är det främst vid kreditbedrägerier som andelen brott där de involverade har en närmare relation med varandra är relativt stort. Det finns även andra exempel på bedrägerier där parterna på något sätt känner varandra. Det kan handla om en gärningsperson som kommer över sin väns dosa och gör en överföring, eller en god man till målsägaren som utnyttjar situationen. Två ärenden avser uteblivna löner, där anställda anmälde sin chef.

Bedrägerier mot bekanta kan till sin karaktär utgöra en särskilt stor kränkning mot den som utsätts för ett sådant brott. Men till antalet tycks de vara av mindre omfattning. Stora bedrägerihärvor med hjälp av fakturor eller kortuppgifter kännetecknas tvärtom av att det inte finns någon personlig relation mellan bedragaren och den utsatte, om det ens förekommer en direkt kontakt. Detsamma gäller även övriga telefon- och internetbedrägerier.

Vilka är gärningspersonerna?

Begränsad information om gärningspersoner i ärendegranskning

De granskade ärendena ger en skev bild av gärningspersoner. Lagföringsfrekvensen skiljer sig väsentligt beroende på vilken typ av bedrägeri det rör sig om, vilket innebär att vi vet mer om förövare vid vissa bedrägerityper än andra. Framför allt annonsbedrägerier, där uppläggen är relativt enkla och gärningspersonerna i behov av snabba pengar och därmed mindre försiktiga, uppvisar en större andel uppklarade ärenden och synliggör relativt väl vilka gärningspersonerna är. Det är inte ovanligt att dessa personer lider av någon form av missbruk eller fysisk ohälsa, eller har andra personliga problem – enligt vad som framkommit i ärendedokumentationen. När det däremot gäller vilka som begår exempelvis kortbedrägerier och övriga telefon- och internetbedrägerier, är uppklaringen mycket låg och informationen närmast obefintlig.

Misstänkta och lagförda personer: jämnare könsfördelning och högre åldrar än vid andra brott

Även den officiella kriminalstatistiken innehåller relativt få uppgifter om gärningspersonerna. Då personuppklaringen skiljer sig för de olika bedrägerityperna ger statistiken över misstänkta och lagförda personer samma skeva bild av bedragarna som ärendegranskningen. Nedan sammanfattas kort vad som tidigare redovisats i kapitlet om Bedrägeriutvecklingen enligt befintliga källor.

År 2014 misstänktes drygt 3 600 personer för brottsbalksbedrägerier och 967 personer för bidragsbrott. Samma år lagfördes sammanlagt 1 157 personer för brottsbalksbedrägerier och 370 personer för bidragsbrott. Under 2008–2014 var andelen kvinnor lagförda för brottsbalksbedrägerier 30 procent, medan motsvarande andel gällande lagförda för bidragsbrott var högre, 41 procent. När det gäller brottsbalksbedrägerier har andelen kvinnor bland de lagförda minskat över tid.

Det var väldigt ovanligt att unga under 21 år lagfördes för bidragsbrott (1 procent av samtliga lagförda för dessa brott under perioden 2008–2014). Även när det gäller andelen unga bland lagförda för brottsbalksbedrägerier var denna jämförelsevis låg (14 procent).

Låg tidigare belastning bland lagförda för bidragsbrott

Det är betydligt mindre vanligt att personer som lagförs för bidragsbrott har någon tidigare registrerad brottsbelastning (60 procent ostraffade), jämfört med personer lagförda för brotts-

balksbedrägerier (41 procent ostraffade). Uppgifterna avser även i detta fall perioden 2008–2014. Motsvarande andel bland lagförda för samtliga brott mot brottsbalken ligger mellan dessa två (47 procent). Med andra ord har lagförda bedragare oftare än andra kriminella en tidigare brottskarriär, medan motsatsen gäller bidragsbrottslingar. Det finns samtidigt en trend över tid mot en högre brottsbelastning bland personer som lagförs för bedrägerier enligt brottsbalken. Andelen ostraffade minskar, och andelen med flertalet tidigare lagföringar ökar under den studerade perioden. Bland dem som lagfördes för brottsbalksbedrägerier 2014 var 38 procent utan tidigare lagföring (jfr 48 procent år 2008), och 23 procent hade minst fem tidigare lagföringar (15 procent år 2008). Liknande utveckling observeras även för personer lagförda för samtliga brott mot brottsbalken, men inte i samma omfattning.

Bedragarnas egna röster

I detta avsnitt beskrivs några centrala gärningspersonstyper utifrån deras motiv, roller och egenskaper – såsom de gestaltar sig i Brås intervjumaterial.

Bred uppsättning gärningspersoner

Den stora variationen i bedrägerityper motsvaras av en bred uppsättning gärningspersoner. Gärningspersonerna har skiftande egenskaper, drivkrafter och funktioner. Även här är det emellertid en begränsad bild av gärningspersonerna som fås genom intervjuerna. Vissa bedrägerityper och grupper av gärningspersoner figurerar mer sällan. Exempelvis förekommer gärningspersoner högre upp i den kriminella hierarkin mer sällan bland de intervjuade. Däremot figurerar personer på lägre positioner i den kriminella hierarkin, som målvakter, oftare i både kriminalstatistiken och intervjuer. Även gärningspersoner som befinner sig utomlands är underrepresenterade i olika datakällor, menar intervjuade poliser.

”Drabbar ingen fattig”

Flera intervjuade gärningspersoner menar att bedrägerier upplevs som mindre moraliskt klandervärda än många andra brott. Detta kopplas ihop med att en stor del bedrägerier begås via datorer och internet, vilket bidrar till att skapa distans och anonymitet mellan gärningsperson och utsatt. Anonymiteten anges vara ett skäl till att ”vem som helst”, även personer utan tidigare kriminell bakgrund, kan begå bedrägerier, enligt de intervjuade. Somliga fortsätter sedan när de ser att det fungerar, menar gärningspersoner.

Det finns också en bild av att ”ingen fattig drabbas” av bedrägerier. Vissa intervjupersoner hänvisar till att den bedragne ofta ersätts ekonomiskt av t.ex. banken eller försäkringsbolaget.

Bedrägerier ses inte som ett ”smutsigt” brott

Företrädare för näringslivet och rättsväsendet vittnar om gärningspersoner med missbruksproblematik och småkriminell bakgrund. Men det finns även personer med kopplingar till ekonomisk eller organiserad brottslighet. I dessa nätverk finns ofta en rollfördelning med en eller flera gärningspersoner på planerande funktioner och olika typer av specialister och medhjälpare längre ner i hierarkin. Det finns också en grupp gärningspersoner som saknar tidigare brottsbelastning, och som skiljer sig från misstänkta för exempelvis stölder och snatterier, enligt intervjupersoner.

Bland personer med tidigare brottsbelastning och någon form av kriminell livsstil tycks bedrägerier inte uppfattas vara ett lika ”smutsigt” brott som exempelvis stölder. Det är en uppfattning som tydligt speglas i många gärningspersonsintervjuer. Vissa menar att de i viss utsträckning har övergått till att begå bedrägerier, eftersom det upplevs som mer lönsamt och mindre riskfyllt än rån och stölder. En gärningsperson ser bedrägerier som ett mindre dåligt alternativ för att skaffa pengar:

> *Jag slapp gå på gatan, men framför allt – det här låter helt vansinnigt – men för mig var det så stort att inte vara tjuv. Jag har alltid hatat tjuvar, och alltid tyckt de varit de lägst stående varelserna av mina bekanta. Så jag kände mig förmer än dem. Jag var ingen tjuv och behövde inte gå på gatan.*

Ekonomiska motiv, men även livsstil, identitet och spänning

Gärningspersoner beskriver framför allt olika former av ekonomiska motiv, men andra drivkrafter finns ofta med i bilden. De ekonomiska behoven kan ha varierande orsaker. Finansiering av missbruk eller återbetalning av skulder orsakade av missbruk är vanliga skäl. Ekonomiska behov orsakade av till exempel konkurser eller arbetslöshet är också en bakgrund som intervjuade poliser vittnar om. För personer som på olika sätt är socialt och ekonomiskt utsatta kan ett målvaktsuppdrag vara ett sätt att tjäna pengar på.

Att skaffa pengar för att upprätthålla en ”lyxig livsstil” kan vara ett annat motiv, enligt flera gärningspersoner. Sådana pengar upplevs ge erkännande och status i såväl kriminella som icke-kriminella kretsar. Andra gärningspersoner betonar snarare tillhörigheten och identiteten i att vara kriminell som motiv. Behovet

av spänning och ”kickar” beskrivs av flera gärningspersoner som ett huvudsakligt skäl till att de begår bedrägerier. Flera gärningspersoner med legala inkomster menar att behovet av kickar har lockat dem till att fortsätta att begå bedrägerier, trots att de egentligen inte behöver inkomsten från brott.

Samtliga dessa faktorer har också identifierats i tidigare forskning om narkotikadistributörer, utpressare och organiserad brottslighet generellt (Brå 2007:4, Brå 2007:7, Korsell, Skinnari och Vesterhav 2009, Brå 2012:12, Brå 2015:22). En gärningsperson ger sin bild:

> *Det är väldigt fokuserat; pengar, pengar, pengar ... hela tiden. Det är nästan lite som heroinisten som jagar nästa fix. Man jagar hela tiden nästa upplägg, nästa betalning.*

En vilja att utmana sig själv och pröva nya saker anges också vara orsaker till att man prövar att begå bedrägerier. Ett upparbetat kunskapskapital anges vara ett skäl till att man både börjar och fortsätter att begå bedrägerier trots att man inte behöver av ekonomiska skäl. Företagskunskap, juridisk kunskap och specialiserad kunskap i vissa brottsliga tillvägagångssätt kan användas för att begå olika typer av bedrägerier liksom andra typer av ekobrott (jfr Brå 2011:7). En gärningsperson menar att kunskapen leder till nya bedrägerier: *Det här kan jag aldrig sluta med. Jag har för mycket information.*

Att utveckla och förändra tillvägagångssätt mot mindre riskfyllda och mer vinstbärande brottstyper är en drivkraft som kan identifieras såväl hos mer som hos mindre organiserade gärningspersoner. Kunskapen överförs därför i regel till nya områden. Flera intervjupersoner beskriver att gärningspersoner som tidigare sysslade med kortbedrägerier och fakturabedrägerier alltmer övergått till exempelvis kreditbedrägerier i takt med att medvetenheten och åtgärderna ökat gällande de första två bedrägerityperna.

Målvakter och medhjälpare

Målvakter och andra medhjälpare har viktiga roller i många typer av bedrägerier. Målvakten används generellt för att minska exponeringen och risken för huvudgärningspersonen genom att genomföra de mer riskfyllda momenten och ta det juridiska ansvaret. Olika egenskaper efterfrågas hos målvakten beroende på vilken funktion den ska fylla. Flera gärningspersoner menar att målvakter generellt får så lite information som möjligt för att minska risken för personerna högre upp i hierarkin. På så sätt skapas en slags brandvägg mellan målvakten och huvudgärningspersonerna, menar en gärningsperson. Dessa brandväggar har också nämnts av gärningspersoner i studier om storskaliga skattebrott respektive narkotikabrott (Brå 2011:7, Brå 2007:7).

Trovärdiga personer med förmåga att vilseleda
Ett vanligt förekommande exempel på en medhjälpares uppdrag är att personen får listor på varor som ska hämtas ut i butiker och en falsk id-handling. Personen hämtar varorna på kredit och lämnar dem till huvudgärningspersonen mot viss ersättning. Trovärdighet och förmåga att vilseleda är därmed centrala egenskaper för denna typ av roll. Flera gärningspersoner beskriver hur huvudgärningspersonen lär ut metoder i syfte att öka trovärdigheten. Dessa metoder innefattar att vara välklädd, titta folk i ögonen och le, samt vara trevlig och vältalig. En gärningsperson är inne på att legitimiteten i ett upplägg ökade genom att de synliga gärningspersonerna hade omgett sig med förtroendeingivande medhjälpare. I exempelvis ett internetbedrägeri användes en advokat och en präst för att försöka öka trovärdigheten när brottsoffret uppmanades att skicka pengar.

Gärningspersonerna kalkylerar med risken att brottsupplägget upptäcks, och vissa målvakter får därför ett inövat manus att utgå från. Det är också känt från en tidigare studie (Brå 2011:7). Att ”vara en bra skådespelare” beskrivs som en bra målvaktsegenskap – både i samband med det brottsliga förfarandet och vid eventuell kontakt med rättsväsendet.

Utsatta personer och missbrukare
Personer som på olika sätt är socialt och ekonomiskt utsatta är sårbara för att rekryteras som målvakter. I synnerhet när funktionen är att ta på sig skulden vid en bolagstömning är personer som har ”lite eller inget ytterligare att förlora” särskilt attraktiva att rekrytera, menar en gärningsperson:

(…) de människor som vill ha pengar är de som är lättast att motivera. Och de människorna finns det ingen brist på. Speciellt inte i ett samhälle där pengar är en bristvara i den utsträckningen som det är. Vissa människor tjänar ju ganska mycket, vissa människor tjänar ingenting.

Om personerna har skulder och betalningsanmärkningar kan de vara mindre sårbara för ytterligare skulder. I en tidigare studie kallades sådana målvakter för ”straffimmuna” (Brå 2011:7). Ett fängelsestraff kan också ha liten avskräckande effekt för en person som exempelvis är hemlös. Många av personerna har ett missbruk av något slag, antingen alkohol-, narkotika- eller spelmissbruk, enligt flera utredare inom rättsväsendet. En gärningsperson som själv agerat i mellanskiktet vid kreditbedrägerier berättar:

Missbrukare gör det för att kunna förse sitt missbruk. Det finns alltså en underliggande motivation hos alla de här människorna som är väldigt allvarlig. Och ju mindre pengar en

människa har och ju sämre situation de sitter i ... Om de har väldigt tungt missbruk, då skiter de i konsekvenserna.

Personer som har skulder till kriminella är särskilt utsatta. De kan tvingas genomföra bedrägerier för att betala av på sina skulder. Det förekommer att kriminella förser missbrukare med droger, för att på så sätt skapa ett beroende och en skuld som sedan måste betalas av genom målvaktsjobb, enligt gärningspersoner.

Yngre och arbetslösa personer

Poliser berättar att de ofta ser hur yngre människor agerar som målvakter eller medhjälpare, exempelvis som telefonförsäljare vid fakturabedrägerier. Arbetslösa är ytterligare en grupp som enligt intervjupersoner utnyttjas som målvakter. En gärningsperson beskriver det på följande sätt:

Arbetslösa som vill ha en praktikplats, de kan bli lurade till det här. Du kan få ett jobb, men då får du göra det här först för att visa att du kan. Och man kör så hårt man kan för man vill visa framfötterna. Man fattar inte att det är något fel förrän man sitter där på polisförhöret.

I synnerhet unga arbetslösa med en ”strulig”, småkriminell bakgrund rekryteras. Ungdomarna får på så sätt en inkomst, vilket i förlängningen kvalificerar för arbetslöshetsersättning och andra bidrag. De kan vara omedvetna om det brottsliga syftet. Det förekommer att unga personer börjar sin kriminella karriär som medhjälpare för att sedan röra sig uppåt i den kriminella hierarkin.

Skötsamma personer som bolagsmålvakter

Intervjupersoner inom rättsväsendet menar att man alltmer sett en övergång till att ”skötsamma personer” agerar som målvakter i situationer där förtroendekapital är nödvändigt. Detta har också noterats i en tidigare studie om skattebrott (Brå 2011:7). Personer utan missbruk, skulder, domar eller anmärkningar är särskilt attraktiva att placera i bolagsstyrelser. En intervjuperson från rättsväsendet säger:

Det var nog vanligare för några år sedan att man såg de här målvakterna som såg rätt risiga ut ... massa konkurser. Det ser man inte riktigt nu, utan de är städade och fina de som sitter där.

I synnerhet om en målvakt ska in i ett företag med långsiktig planering inför ett kreditbedrägeri söker man personer med god kreditvärdighet. ”En skötsam person som är i ekonomisk nöd” är särskilt attraktiv i sammanhanget, enligt intervjuade gärningspersoner. Vissa gärningspersoner upplever att det är enkelt att få tag på ”vanliga personer” som vill tjäna pengar genom att agera

bolagsmålvakter. I senare skeden, när det enbart handlar om att lägga det juridiska ansvaret på en annan, kan även personer utan förtroendekapital tillsättas som bolagsmålvakter. Verksamhetstiden för en bolagsmålvakt är begränsad eftersom personen synliggörs inför myndigheterna. Efter ett antal konkurser, större personliga skulder och eventuella domar minskar möjligheten att agera bolagsmålvakt.

En person som en gång har försatts i personlig konkurs och fått skulder måste i allmänhet betala en del av en legal inkomst i avbetalningar och utmätningar. Detta kan driva på fortsatt kriminalitet, och är enligt utredare inom rättsväsendet ett motiv till att återigen begå bedrägerier.

Att rekrytera medhjälpare och målvakter

Den sociala förmågan och förtroendekapitalet används även vid rekrytering av medhjälpare till organiserade bedrägerier, enligt intervjupersoner. Rekryteringen av målvakter kan ske genom att huvudgärningspersonen tar kontakt med en lämplig person. Man försöker sedan upprätta förtroende på olika sätt. En gärningsperson beskriver hur han som nyintagen på en kriminalvårdsanstalt blev kontaktad av en person som ville anlita en bolagsmålvakt:

> *Jag fick telefonkort och han fjäskade, han köpte cigaretter till mig och han skickade in lite pengar till mig utifrån. Och då fick man ju ett förtroende för honom: Det här är fan en schysst person (…) Men det visade sig ju att det var en hal typ, han satte mig i värsta situationen. För eftersom jag har läs- och skrivsvårigheter, så hade jag ju litat på hans ord, eftersom jag inte visste vad det stod på pappren.*

Intervjuerna talar för att tillvägagångssätten vid rekryteringar kan skifta snabbt mellan hot och löften om förmåner. Ibland använder olika huvudgärningspersoner motstridiga metoder vid samma rekryteringstillfälle:

> *I ena sekunden blir man hotad, andra sekunden så ... Det är pinnen och moroten helt enkelt. Så man har olika tillvägagångssätt, kan man inte motivera en människa med pengar, så motiverar man hellre med våld, eller ännu värre.*

Huvudgärningspersonerna beskrivs sällan själva som våldsamma, men kan ha kopplingar till organiserad brottslighet, och sägs kunna anlita våldsamma personer. Det förekommer mycket hot, och det förekommer att vissa hot verkställs, enligt en annan gärningsperson.

Räknar med att åka fast

Flera gärningspersoner som själva varit involverade i storskaliga bedrägerier beskriver hur ett fängelsestraff nästan ingår som en

del i uppdraget som medhjälpare eller målvakt. Tiden på anstalt kan också vägas in i den ekonomiska ersättningen för uppdraget. Vissa personer kan bli omhändertagna av övriga gärningspersoner under tiden de sitter inne och ha en undanstoppad brottsvinst som väntar vid frigivning. Flera gärningspersoner beskriver dock hur man ofta blir lurad på pengarna medan man sitter inne och inte heller får det omhändertagande man blivit utlovad. För många målvakter är också vinsten väsentligt lägre i förhållande till de skulder de får och i förhållande till risken att åka fast. En gärningsperson beskriver målvaktens utsatthet:

> *Det är ju fortfarande han som tjänar minst pengar. De andra som står bakom och flinar, sitter inte på kåken och har skapat allting ... de tjänar in massor med pengar. Kanske inte alla gånger men oftast.*

Straffskalan upplevs generellt av flera gärningspersoner som låg i förhållande till den vinning som kan göras på bedrägerier. En gärningsperson som begått omfattande kreditbedrägerier menar att ”vem som helst kan tänka sig att sitta inne några år för att göra en stor vinst när man kommer ut”. Detta har också noterats i tidigare forskning om narkotikadistributörer och skattebrottslingar (gärningspersonsintervjuer i Brå 2007:7, Brå 2011:7).

Falska eller utnyttjade identiteter i stället för målvakt

Identitetsuppgifter utnyttjas i samma syfte som målvakter och medhjälpare: att minska exponering och risk för huvudgärningspersonen. Några intervjupersoner är inne på att vissa aktörer använder falska identiteter som de själva kontrollerar, i stället för att ta in målvakter. På så sätt minskar kostnader för och risker med samarbeten med fysiska målvakter. EU-migranters identiteter beskrivs av flera intervjuade myndighetspersoner vara ”den nya tidens målvakter”. Identiteterna utnyttjas genom att dessa exempelvis sätts i en bolagsstyrelse inför kreditbedrägerier eller välfärdsbedrägerier. (Se även kapitlet Identitetsmissbruk).

Kreativa personer på ledande positioner

Gärningspersoner som har en planerande och ledande roll vid bedrägerier beskrivs vara kreativa och sociala personer. De kan också vara duktiga på att se möjligheter och hitta luckor och svagheter i system som kan utnyttjas. En brottsutredare beskriver huvudgärningspersoner som *”intelligenta, inga våldsverkare. De ägnar rätt mycket av sin vakna tid till att hitta hål i systemet”*.

Tålamod och förmåga till långsiktig planering beskrivs också som centrala egenskaper för gärningspersoner i ledande positioner, i synnerhet vid mer organiserade bedrägerier med företag.

Ledande gärningspersoner kan planera i flera månader upp till år innan bedrägeriet fullbordas.

Huvudgärningspersonen kan ha stora kontaktnät och där verka som spindeln i nätet för att sammanföra rätt personer för ett visst upplägg. En intervjuperson som begått bedrägerier med företag beskriver hur dennes roll var att planera upplägg och därefter hitta rätt personer för bedrägeriet. Intervjupersonen betonade att det var viktigt att kunna hitta svagheter som kan utnyttjas hos de personer man vill rekrytera och att se möjligheter att använda andras olika kompetenser i ett tänkt upplägg. Det förekommer även personer som agerar som kriminella bemanningskonsulter. De tar emot förfrågningar och förmedlar personer med efterfrågad kompetens.

Företagare som glidit in: gråzoner mellan legalt och illegalt

Det förekommer att gärningspersonerna har eller har haft egna legala företag och därigenom fått kunskaper som de senare utnyttjar. En gärningsperson som själv agerat i ledande positioner vid bedrägerier beskriver det på följande sätt:

> *Det kan vara egna företagare, det kan vara anställda i bolag, det kan vara chefer eller VD:s eller aktieägare till och med som planerar de här kupperna. Och utför dem flera år senare, när de inte längre sitter i styrelsen. De får en insikt i systemet som ger dem en möjlighet att planera.*

En anställd på Ekobrottsmyndigheten menar att personer som begår bedrägerier med företag i regel är driftiga och skickliga, och hade kunnat vara framgångsrika legala företagsledare. Flera gärningspersoner berättar om hur de startade företag med legala syften som så småningom utvecklades till illegal verksamhet. De upplevde att de snarast har ”glidit in” i gråzoner och sedan börjat med kriminell verksamhet. Andra driver legal och illegal verksamhet parallellt. Denna övergång och dylika överlappningar har också noterats i annan forskning (se exempelvis Levi 2008, Brå 2011:7, ISF och Brå 2011:12). En gärningsperson förklarar:

> *Det var inte något bedrägeri med uppsåtligt syfte, det var marknaden som brast. Det var då jag började lära mig affärslivet, det finns en väldigt tunn linje mellan legalt och illegalt. Många befinner sig i gråzonen. Det är ett fruktansvärt fulspel inom finansbranschen. Jag ledsnade på affärs- och finanslivet. Det går ut på att lura folk, annars får de inte in och ut pengar.*

Den tunna gränsen mellan legalt och illegalt har påtalats i flera intervjuer med gärningspersoner. Upplevelsen av att det existerar gråzoner kan bidra till att personer tar klivet från den legala till den illegala affärsvärlden. Normer som uppfattas vara accepterade och inbyggda i den legala företagsvärlden kan på så sätt bidra

till att legitimera bedrägerier. Denna studies gärningspersoner ger uttryck för att de inte gör fel – liksom gärningspersoner inom skattebrott, narkotikahandel och bedrägerier i tidigare studier (Brå 2011:7, Brå 2007:7, jfr Levi 2008). Tvärtom anser de sig vara mycket duktigare företagare än de som låter sig begränsas av alla regelverk.

Specialistkompetens

Olika typer av kunskap och specialistkompetens krävs ofta vid exempelvis fakturabedrägerier och organiserade kredit- och kortbedrägerier. Information om upplägg, brister och sårbarheter inom olika system sprids via internet eller via kontakter. Ofta sker spridningen snabbt, och när ett upplägg visar sig fungera kopieras det av andra, menar en intervjuperson från rättsväsendet. Färdiga upplägg och planer för olika typer av bedrägerier säljs också, enligt gärningspersoner. Även anstalter kan verka som en plats för kunskapsspridning.

Kompetens inom juridik, ekonomi och it är eftertraktad. Även tekniska färdigheter efterfrågas, som hantering av telefonväxlar och datasystem samt tillverkning av kort, identitetshandlingar och fakturor. Enligt de intervjuade gärningspersonerna är det enkelt att få tag på och anlita specialister i kriminella syften. Det finns också de som medverkar utan vetskap om det kriminella uppsåtet eller till följd av hot och utpressning.

Juridisk kompetens. Vid fakturabedrägerier används juridiskt kunniga personer för att formulera finstilta avtal och utnyttja kryphål i lagen samt för att bemöta bestridanden av fakturor. Juridiskt kunniga personer knyts tidigt till det kriminella företaget, menar en intervjuad polis. Jurister kan också anlitas via juristbyråer. En gärningsperson menar att ”gråzons-advokater” är attraktiva medhjälpare.

Personer med ekonomisk kompetens som bokförare och revisorer används, i synnerhet om ett bolag används vid bedrägeriet. Deras uppgift är ofta att hjälpa till med att skapa och upprätthålla en legal fasad på ett företag som ska användas för bedrägerier. Det sker genom att kreditvärdigheten på ett företag manipuleras, till exempel genom att årsbokslut och intyg förfalskas. Annan hjälp som efterfrågas är att medverka i andra ekobrott och penningtvätt. En brottsutredare och en gärningsperson hade erfarenhet av att bokförare tipsat om företag nära konkurs som kriminella kan köpa. Även bolagsförmedlare har identifierats som en viktig funktion i tidigare forskning (Brå 2011:7). Det finns också uppgifter om att enskilda konkursförvaltare förmåtts att släppa igenom konkurser med bedrägligt uppsåt.

It-kunniga personer efterfrågas till exempel för att genomföra olika avancerade dataintrångsrelaterade bedrägerier. Det förekommer också att it-kompetens används för att radera spår efter ett genomfört bedrägeri. I vissa fall delar it-skickliga personer med sig av kunskaper utan kostnad via internetsidor, i andra har gärningspersonerna egna it-kunskaper. Enligt intervjupersoner begås en del avancerade internetrelaterade bedrägerier som inbegriper stöld av kortuppgifter utomlands.

Insider

En insider definieras här som en medhjälpare som befinner sig inom en legal verksamhet. Gärningspersonen använder en insider för att få kunskap om och utnyttja sårbarheter inom en bransch eller organisation. Det kan ske genom att insidern kommer över och läcker uppgifter eller manipulerar intyg och dokument. Ett exempel är mäklarbyråer som används för att manipulera intyg och höja värden på fastigheter. Genom manipulerade intyg kan högre lån tas på falska grunder. Eftersom mäklare upplevs vara trovärdiga tycks banken ofta godkänna värderingsintyget utan djupare kontroll, menar en intervjuperson från näringslivet.

I vissa fall drar insidern nytta av sin position på ett företag för att själv planera och utföra bedrägerier (jfr Brå 2014:4, Gounev 2012). Enligt intervjuerna förekommer att insider verkar t.ex. inom banker, på advokatbyråer, inom handeln och fastighetsbranschen.

Intervjupersoner menar att även försäljare inom handeln i vissa fall anlitas för att begå bedrägerier. Säljaren mutas för att sänka priset på en vara eller gör olovliga återköp. Upptäcktsrisken för en säljare som hjälper till som insider är liten, givet kulturen att en säljare ska sträva efter hög försäljning, menar en gärningsperson. Inom spelbranschen kan en croupier anlitas till att manipulera med insatsen för att gärningspersonen ska göra en vinst.

Vilka blir insider?

De intervjupersoner Brå talat med menar att en insider ofta agerar för egen vinnings skull. Hot förekommer, men ofta handlar det om ett påhittat hot som anges som en bortförklaring när en insider åker fast, menar företrädare för näringslivet. Detta vinner visst stöd även i annan kvalitativ forskning om insider (se Brå 2014:4).

En riskfaktor är större företag, eftersom de upplevs innebära mindre risk för upptäckt, menar en gärningsperson. Även om bedrägeriet skulle upptäckas, blir det svårt att spåra och koppla en specifik person till brottet. På mindre företag kan dock en insider

hävda att han eller hon agerat i god tro och på så sätt komma undan anklagelser om delaktighet.

Personen som agerar insider beskrivs av flera intervjupersoner som en högpresterande individ som är skicklig på att övertala andra. Företrädare för näringslivet menar att de sällan ser nyanställda som insider utan snarare personer som jobbat länge. Personer på lägre positioner förekommer också mer sällan som insider, enligt intervjupersoner. Riskpositioner uppges vara mellanpositioner, och i synnerhet chefspositioner. Personer högre upp i hierarkin känner ofta till rutiner och har maktresurser att förfoga över, vilket ger möjligheter att missbruka dessa. De är oftast svåra att ifrågasätta, menar en företrädare för näringslivet. Dessa riskfaktorer är kända i forskningen på detta område (se vidare Brå 2014:4).

Tala tyst om insider

En del företag lägger tid och resurser på att utreda och anmäla misstänkta insiderfall. Men vissa företag som upptäckt en insider vill tala tyst om detta. I synnerhet tycks förtroendebranscher, exempelvis banksektorn, i allmänhet vara mer förtegna om utsattheten. En insider uppfattas skada varumärket och kundernas förtroende för företaget. En säkerhetsexpert inom handeln menar att de ser att företag inte polisanmäler upptäckta insider, utan i stället uppmanar dem att självmant säga upp sig. Ju högre upp i företagshierarkin en insider befinner sig, desto känsligare blir det att anmäla och offentliggöra brottet, menar intervjupersoner från näringslivet.

Genom att en insider inte polisanmäls möjliggörs att den kan söka ny anställning och där fortsätta agera i brottsliga syften (se även Brå 2014:4, jfr Engdahl 2010). Intervjuade polisanställda känner till flera sådana tillfällen, där en person återigen blivit insider efter att ha fått goda vitsord av arbetsgivaren.

Identitetsmissbruk

Med *identitetsmissbruk* menas användning av falska eller stulna (det vill säga osanna) identiteter i ett bedrägligt syfte. Identiteten kan tillhöra en privatperson eller ett företag, en organisation eller en myndighet.

Identitetsstöld är en typ av identitetsmissbruk, där identitet tillhörande en existerande person olovligen använts vid bedrägeri.

Detta kapitel ägnas åt definitioner, avgränsningar och beräkningar av omfattningen och karaktären av identitetsmissbruk som ett led i bedrägeribrottsligheten. Med utgångspunkt i resultaten identifieras även relaterade problemområden.

Att utge sig för att vara någon annan – oavsett om personen existerar eller ej – är ett centralt moment vid många bedrägerier. Dels kan man vilseleda en person genom att etablera ett förtroende inför brottet (exempelvis utge sig för att vara en vän genom att kapa dennes mejlkonto), dels kan gärningspersoner använda osanna identiteter för att dölja den egna och vilseleda spåren efter brottet (exempelvis genom att ange felaktigt namn och mejladress vid ett annonsbedrägeri). De bedrägerier som oftast förknippas med identitetsmissbruk är dock de tidigare beskrivna kreditbedrägerierna, som närmast förutsätter att gärningspersonen använder någon annans identitetsuppgifter.

Olovlig användning av andras identiteter, ofta refererat till som id-stöld eller id-kapning, har under senare tid fått mycket uppmärksamhet, både i media, hos rättsväsendet och politiskt.[42] Enligt befintliga kartläggningar (se bilaga 4) finns det indikationer på att användningen av stulna och falska identiteter ökar i Sverige (NBC 2015b, UC AB 2015) och att det inte sällan har

[42] Förutom förslaget om att kriminalisera olovlig identitetsanvändning (se bilaga 5) finns det t.ex. ett lagförslag gällande missbruk av svenska pass, Ds 2015:12. Inte minst är också direktivet till Brå gällande detta bedrägeriuppdrag, enligt vilket identitetsstöld särskilt ska uppmärksammas, ett tecken på en ökad politisk vilja att behandla det växande problemet.

kopplingar till organiserad brottslighet (NUC 2015b). I en kartläggning som Stöldskyddsföreningen (2013) har gjort framgår att två av fem personer är mycket eller ganska oroliga för att bli utsatta för en identitetskapning.

Som bakgrund till denna utveckling anges den tekniska utvecklingen med ökat internetanvändande i kombination med det faktum att enskildas personuppgifter är lättillgängliga för allmänheten i Sverige. En annan för Sverige utmärkande omständighet är det stora antalet godkända identitetshandlingar (olika typer av id-kort, körkort, pass) som gör det svårare att kontrollera identiteterna och lättare att förfalska handlingarna (NFC 2015).

På internet kan man enkelt kartlägga en persons livssituation, inkomst, sysselsättning och hemvist. Dels lägger många ut dessa uppgifter självmant i olika internetfora, dels finns det sidor som erbjuder informationen mot betalning. Mycket av utvecklingen kan vidare tillskrivas ändrade köp- och betalningsvanor, då både köp, beviljande av lån och betalningar i dag oftast sker utan direkt fysisk kontakt (SOU 2013:85).

Stöld, kapning, intrång eller förfalskning?

Många olika begrepp används för att beskriva bruket av stulna eller falska identiteter, och det tycks i dag inte föreligga någon konsensus om definitionen bland berörda aktörer. Förutom rena kapningar eller stölder[43] av andras identiteter är det i bedrägerisammanhang inte ovanligt att en person frivilligt, alternativt under hot, lånar ut sina identitetsuppgifter och på så sätt fungerar som en så kallad målvakt. I liknande fall kan det vara missvisande att tala om identitetskapning eller -stöld, men handlingen utgör ändå ett intrång[44] i en annan persons identitet. Dessutom förekommer att gärningspersonen utger sig för att vara en icke existerande person. Det rör sig då vare sig om stöld, kapning eller intrång i en annans identitet; däremot handlar det om en falsk identitet.

[43] När det kommer till det i sammanhanget kanske vanligaste begreppet ”identitetsstöld” kan man invända att gärningen inte utgör en faktisk stöld. Den bestulne har sin identitet kvar, även om en annan person nu kan utge sig för att vara han eller hon. Då identitetsstöld är ett etablerat begrepp och används när existerande personers identiteter har tagits över av någon annan i ett brottsligt syfte, används benämningen även här för att beskriva liknande situationer. Det gäller främst kreditbedrägerier.

[44] Ett förslag om att kriminalisera identitetsintrång (SOU 2013:85) beskrivs längre fram.

Inte alltid stöld: ”luftslott” bakom många falska identiteter

Bruket av helt falska identiteter utan några kopplingar till existerande personer utgör, enligt de aktörer som Brå har intervjuat, ett omfattande och inte speciellt uppmärksammat problem med både ekonomiska och andra konsekvenser. Att skaffa sig en helt falsk identitet är inte speciellt svårt, enligt intervjupersoner inom både rättsväsendet och andra myndigheter. Det förekommer exempelvis att bedragare skapar multipla falska identiteter kopplade till en och samma ursprungsidentitet. I vissa fall används stulna utländska pass för att skapa nya identiteter i Sverige. I ytterligare några fall kan de utländska passen vara helt falska, och nya identiteter som bygger på dessa handlingar saknar därmed helt koppling till en existerande person:

> En myndighetsrepresentant: *Vi har ju oftast en identitet på ett papper, och vi vet ju inte ens om det finns någon person bakom, det kan vara ett luftslott*.

Självklart innebär dessa helt falska identiteter, och brister i folkbokföringen, stora problem för själva välfärdssystemet samtidigt som de nyttjas vid bedrägerier.

Företags, organisationers och privatpersoners identitet

En annan fråga som kan diskuteras när det gäller identitetsmissbruk är huruvida även så kallade juridiska personers identiteter bör omfattas. När frågan uppmärksammas är det vanligen missbruk av privatpersoners identiteter som åsyftas. Också identiteter hos företag, myndigheter eller organisationer kan dock användas i ett bedrägligt syfte.[45] Ett exempel kan vara nätfiske, då gärningspersonen låtsas vara ett etablerat företag vars domän kapats. En annan variant är en form av skadlig kod, så kallad ransomware (de tidigare nämnda falska betalkraven från ”polisen”) eller bedrägerier med kapade fakturor från etablerade företag, myndigheter eller organisationer.

Gränserna är samtidigt inte skarpa mellan hur privatpersoners respektive företagsidentiteter kan kapas och användas för ekonomisk vinning. En del bedrägerier av större format sker med hjälp av kapning av kreditvärdiga bolag, och dessa kapningar påbörjas inte sällan exempelvis med en registrering av styrelsemedlemmar under falska identiteter. Stora härvor av liknande slag har på senare tid avslöjats, där exempelvis migranters identiteter har använts för att starta bolag i deras namn (NUC 2015b).

[45] Detta har bl.a. påpekats i flera remissvar till Egendomsskyddsutredningen (SOU 2013:85).

Kontokort bör omfattas

Enligt Brås bedömning (jfr NBC 2015b) uppfyller även kontokort eller elektroniska kortuppgifter kriterierna för att kunna betraktas som identitetsuppgifter, då de är kopplade till en viss persons identitet. Korten är dessutom skyddade med både chip och pinkod, och för att använda elektroniska uppgifter vid exempelvis internetköp krävs inte sällan någon form av autentisering (e-legitimation, bankdosa eller engångslösenord). Som en av intervjupersonerna uttryckte det när kontokortens status som identitetsuppgifter diskuterades: *Hela den finansiella sektorn är ju personnummerstyrd, precis som Skatteverket*.

Att låtsas vara någon man inte är

Förutom ovan beskrivna scenarion kan det förekomma bedrägerier där gärningspersonen på ett relativt enkelt vis låtsas vara någon annan, ibland en existerande, ibland en påhittad person. Ett exempel är att lämna ut falska eller stulna kontaktuppgifter vid bedräglig försäljning. Även i samband med exempelvis romansbedrägerier använder förövaren av naturliga skäl vanligtvis en annan identitet. En mer avancerad form av identitetsstöld sker när bedragaren kapar ett mejlkonto tillhörande offrets bekant, vän eller släkting och utger sig för att vara denna person i en nödsituation. Den gemensamma nämnaren är att bedragaren på olika sätt, med eller utan stöld av identitetsuppgifter, utger sig för att vara en annan person (existerande eller ej).

Brås definition: identitetsmissbruk och osanna identiteter

Brå har valt att använda en bred definition där samtliga hittills beskrivna former av användning av falska eller stulna identiteter inkluderas. Då det inte alltid rör sig om rena stölder har Brå valt benämningen *identitetsmissbruk*. Med det åsyftas samtliga situationer där bedragaren, i ett vilseledande syfte, utger sig för att vara någon denne inte är. *Identitetsstöld* refererar i den följande texten enbart till olovligt bruk av existerande identiteter. För att med ett ord beskriva både stulna och helt falska identiteter kommer begreppet *osanna identiteter*[46] att användas.

Identitets- eller personuppgifter

En definition av *identitetsuppgifter* har föreslagits av Egendomsskyddsutredningen (SOU 2013:85); enligt denna avses uppgifter

[46] Observera att det finns en skillnad mellan identiteter och identitetshandlingar (se tabell 22 längre fram). Begreppet ”osanna identiteter” refererar här inte till identitetshandlingar.

som var och en eller tillsammans gör det möjligt att identifiera en fysisk, icke avliden person. Det kan vara en mejladress tillsammans med ett telefonnummer eller bild, eller en fysisk adress med ett namn. På så sätt är identitetsuppgifter en något smalare kategori än *personuppgifter*, såsom de sistnämnda definieras enligt 3 § personuppgiftslagen. Här anges att personuppgifter är all slags information som direkt eller indirekt kan *hänföras* till en fysisk person som är i livet. Skillnaden har dock inte en avgörande betydelse i bedrägerisammanhang; i de flesta fall rör det sig om samma slags uppgifter.

I fortsättningen kommer begreppet *identitetsuppgifter* att användas. *Personuppgifter* kommer enbart att referera till uppgifter *registrerade vid myndigheter* (t.ex. vid kreditbedrägerier eller bidragsbrott).

Olika typer av identitetsmissbruk enligt Brås granskning

Identitetsmissbruk förekommer inom samtliga bedrägerityper

I de ärenden Brå har granskat är det inte alltid klarlagt och dokumenterat om osanna identiteter använts i samband med det aktuella brottet. Resultaten ska därför betraktas som minimiskattningar. Med andra ord kan identitetsmissbruk utgöra ett led i fler bedrägeriärenden än vad som här identifierats.

Det skattade antalet bedrägeriärenden som innehåller någon form av identitetsmissbruk är dessutom direkt beroende av vilken definition som tillämpas. Givet den breda definitionen Brå har valt kan det konstateras att någon form av identitetsmissbruk kan förekomma i samband med samtliga de huvudkategorier av brottsbalksbedrägerier som beskrivits tidigare, och även vid bidragsbrott. Enbart vid kreditbedrägerier, som nästan alltid innebär lån eller köp i annans namn, är dock identitetsmissbruk, eller i detta fall en ren identitetsstöld, mer eller mindre en förutsättning för brottet.

Enligt Brås granskning ingår identitetsmissbruk i drygt tre av fem (63 procent) polisanmälda brottsbalksbedrägerier. Utifrån Brås definition har sammanlagt sju olika typer av identitetsmissbruk kunnat identifieras i granskningen. Dessa beskrivs i tabell 20.

Tabell 20. Olika typer av identitetsmissbruk bland brottsbalksbedrägerier. Anmälda ärenden första halvåret 2013.

	Antal	Procent
Ej identitetsmissbruk	147	37
Kortbedrägeri med privata kontokort	83	21
Kreditköp eller -lån i annans namn	62	15,5
Falskt bruk av företags-, organisations- eller myndighetsnamn	57	14
Försäljning i annans namn	23	6
”Vän i nöd”	10	2,5
Falsk namnteckning	6	1,5
Övrigt	12	3
Totalt	**400**	**100**

Vanligaste typen av identitetsmissbruk: kortbedrägeri med privata kontokort

Den storleksmässigt största kategorin när det gäller identitetsmissbruk i bedrägligt syfte består av bedrägerier med privatpersoners kontokort. Cirka en femtedel (83 ärenden) av de polisanmälda brottsbalksbedrägerierna innehåller identitetsmissbruk av denna typ. Det sker antingen genom att gärningspersonen använder en annan individs elektroniska kortuppgifter för exempelvis bedrägliga internetköp *(card not present, CNP)*, eller det fysiska stulna eller skimmade kortet för köp i butik eller uttag *(card present, CP)*. Även om själva tillvägagångssättet skiljer sig är den grundläggande metoden i bägge fallen att bedragaren vilseleder banken att tro att han eller hon är kortinnehavaren och att pengar dras från kortkundens konto utan dennes vetskap. För mer detaljerade beskrivningar av olika tillvägagångssätt, se tidigare avsnitt om Kortbedrägerier.

Kreditköp eller -lån i annans namn: urtypen av identitetsmissbruk

Som nämnts tidigare är kreditbedrägerier den enda kategorin där en identitetsstöld ofta är en direkt förutsättning. När identitetsstölder beskrivs, inte minst i mediala sammanhang, är det oftast just kreditbedrägerier som åsyftas. Som kartläggningarna från exempelvis UC AB (f.d. Upplysningscentralen, 2015) visar är kreditbedrägerier med identitetsstölder ett växande problem som drabbar enskilda, men främst näringslivet, mycket hårt. Enligt en intervjuad representant för kreditföretagen är det så att ”*… företagen förlorar nästan mer nu på grund av id-stölder än på rena kreditförluster.”*

Sammanlagt 62 kreditbedrägeriärenden (16 procent av de anmälda brottsbalksbedrägerierna) innehåller identitetsmissbruk, där privatpersoners identiteter har stulits och använts vid bedrägliga kreditköp eller lån. Fyra av fem fall handlar om köp, en femtedel består av lån i annans namn. Till detta kommer dessutom kreditbedrägerier med hjälp av företagskapning; användning av företagsidentiteter beskrivs dock som en egen kategori av identitetsmissbruk längre fram.

Kreditköp i annans namn

Vad som typiskt sett sker är att gärningspersonen beställer en vara i en annan persons namn, på internet eller i fysisk butik. Varan levereras sedan till gärningspersonen (eller till en medhjälpare som ska hämta varan) och fakturan skickas till den vars identitet har använts. Ett mycket vanligt kreditköp med stulen identitet, sett till en specifik vara, avser mobiler med abonnemang, men även köp av datorer, elektronik, möbler, kläder, resebiljetter med mera förekommer.

Ibland handlar bedragaren med falska identitetshandlingar direkt i butiken. Eftersom fysiska möten innebär större risker att bli avslöjad, och eftersom butiker (dvs. elektronikkedjor, telekombutiker och liknande) har mer noggranna identitetskontroller vid kreditköp än olika utlämningsställen, är det sannolikt vanligast för bedragare att beställa varor eller tjänster på internet.[47] En annan anledning är att det är lättare att utföra ett stort antal brott från en dator i stället för enskilda brott i olika butiker.[48] För mer detaljer om tillvägagångssättet vid bedrägliga kreditköp, se avsnittet om Kreditbedrägerier.

Enkelt att handla med annans personuppgifter

De uppgifter som gärningspersonen behöver visa upp för att styrka sin identitet vid köpet kan variera; ibland räcker det med namn och adress, medan man på vissa internetsidor behöver skapa ett konto och ange ett personnummer. I Sverige är det inte svårt att skaffa alla dessa uppgifter. Dataintrång är inte ovanligt, men information om personnummer kan man egentligen enkelt få genom att ringa Skatteverket eller köpa uppgiften på internet. Det förekommer även att gärningspersonen skaffar sig tillgång

[47] Butiker har i större utsträckning kameraövervakning som kan verka avskräckande. Det tar dessutom mer tid att teckna ett avtal, med de kontroller det möjliggör.

[48] Det går visserligen, som de intervjuade lyfte fram, även att resonera som att det kan vara lättare att få ut en telefon i butik än att beställa en vara via internet, då provisionsbelönade telefonförsäljare främst vill sälja varor, och kunden slipper hämta ut ett paket med legitimation efteråt, utan får mobilen direkt i handen i en fysisk butik. Men troligtvis är upptäcktsrisken lägre vid köp över nätet och vid uthämtning av paket jämfört med köp i fysisk butik.

till en annan persons post; många brev – exempelvis räkningar – innehåller alla personuppgifter en bedragare kan önska sig.

Betaltjänstföretag och kreditupplysningsföretag genomför en hel del kontroller i detta tidiga skede, det vill säga i samband med kundens beställning. Det leder till att många försök till bedrägliga kreditköp (liksom kortbedrägerier) stoppas tidigt. Ofta blir det dock först när några bedrägerier hunnit äga rum och ett avvikande köpmönster identifierats. I kapitlet om Näringslivets roller beskrivs detta mer ingående.

Att styra om och hämta ut försändelsen

Om bedrägeriet inte stoppas redan vid beställningen skickas försändelsen till ett utlämningsställe.[49] Bedragaren behöver då så snabbt som möjligt, innan processen hunnit avslöjas och stoppas, hämta varorna, vanligtvis mot uppvisande av falska identitetshandlingar. Detsamma gäller även om varan inte beställs på internet utan köps direkt i butik. Det är vanligt att medhjälpare används direkt i butiken i samband beställningen och vid hämtningen av försändelser, för att skydda huvudmännen. För att få avin innan den når den person vars identitet har använts krävs att gärningspersonen bevakar dennes post och stjäl avin från postlådan eller brevbärarens vagn.

> En gärningsperson: … *de sätter upp en c/o adress på någon där man vet vilken brevlåda man ska titta i … så att man kan vittja brevlådorna några dagar efter beställning.*

Ett annat alternativ är att bedragaren vid beställningen anger att han eller hon vill ha sms-avisering till en egen mobiltelefon, vanligen med kontantkort. Det går ibland även att välja en annan leveransadress än faktureringsadress. Ibland använder sig gärningspersoner dessutom av adressändring, då det är enkelt att via en internettjänst adressändra åt en annan person.

Bedrägliga lån – gärningsperson inte sällan bekant

Förutom kreditköp kan en bedragare även ta lån i annans namn. Att låna pengar med osann identitet är inte lika vanligt som bedrägliga kreditköp, men förekommer i nio av de granskade ärendena; i två fall rör det sig om sms-lån, i övrigt är det banklån.

Jämfört med andra bedrägerier är det något vanligare vid kreditbedrägerier, och i synnerhet lån, att de inblandade parterna på något sätt känner varandra. Det underlättar tillgången till personuppgifterna. I tre av de ärenden som avsåg banklån hade

[49] Det finns ca 1 600 certifierade ombud.

bedragaren en närmare relation med målsägaren.[50] I dessa fall har gärningspersonen och målsägaren varit gifta, och först under skilsmässan framkom att gärningspersonen tagit lån i målsägarens namn, med en förfalskad namnteckning.

En särskild typ av bedrägliga lån i annans namn har varit snabba sms-lån, som lanserades 2006. Dessa tycks dock ha minskat efter bl.a. ökade krav på användning av BankID och krav på att samtliga långivare måste ha en licens från Finansinspektionen (för mer detaljer, se Näringslivets roller).

Falskt bruk av företags-, organisations- eller myndighetsidentiteter

Även om identitetsstöld vanligen refererar till privatpersoner kan även företagsidentiteter kapas i ett bedrägligt syfte. Någon form av olovligt bruk av företagsidentiteter har förekommit i sammanlagt 57 av de granskade ärendena (15 procent). Exempel på detta återfinns inom i stort sett samtliga av de fem huvudkategorierna av brottsbalksbedrägerier, men framför allt bland övriga telefon- och internetbedrägerier (se tabell 21).

Tabell 21. Olika typer av brottsbalksbedrägerier där företagsidentiteter missbrukas. Anmälda ärenden första halvåret 2013.

	Antal	Procent
Övriga telefon- och internetbedrägerier	39	68
Ransomware	(23)	(40)
Annat nätfiske/domänkapning	(12)	(21)
Microsoftbedrägeri eller liknande	(4)	(7)
Kreditbedrägeri	5	9
Kortbedrägeri (företagskort)	4	7
Fakturabedrägeri (kapad faktura)	8	14
Övrig bedräglig försäljning	1	2
Totalt	**57**	**100**

Domänkapning vanligt

De vanligaste händelserna i denna kategori av identitetsmissbruk innehåller en slags domänkapning. Bedragaren utger sig, oftast på internet, men ibland på telefon, för att vara ett etablerat företag eller en myndighet och försöker i dess namn nätfiska efter person- och/eller kontouppgifter hos kunderna. Meddelandet kan komma med myndighetens logotyp och vara mycket trovärdigt.

[50] Enligt UC AB:s enkät var enbart 1–2 procent av dem som spärrat sin identitet på grund av stöld bekanta med gärningspersonen. Denna information är dock inte direkt jämförbar med polisanmälda bedrägerier.

Den absolut vanligaste typen av ett sådant upplägg i det granskade materialet är dock så kallad ransomware, i dessa fall en form av skadlig kod med polisens logotyp (se avsnittet om Övrigt telefon- och internetbedrägeri).

I det granskade materialet fanns även fyra kortbedrägeriärenden där stulna eller skimmade företagskort användes, vanligen för att tanka bensin. Dessutom fanns här åtta bedrägerier med kapad faktura – det vill säga en faktura från ett till synes seriöst företag, men med manipulerade uppgifter för att styra om betalningen.

Identiteter tillhörande andra EU-medborgare missbrukas vid bolagskapningar

En annan typ av bedrägeri där företagsidentiteter olovligt används är kreditbedrägerihärvor med kapade bolag. Troligtvis är liknande, ofta mycket omfattande och organiserade brott, vanligare än vad som framgår i Brås ärendegranskning. Där beskrivs i enskilda anmälningar vanligtvis enbart olika pusselbitar. Om det finns kopplingar till andra ärenden framkommer det först i ett senare skede av utredningen – i bästa fall. Enligt flera av Brås intervjuer utgör dock denna typ av bedrägeribrottslighet ett omfattande problem. I dessa fall kan både bruket av kapade företagsidentiteter och privatpersoners osanna identiteter användas. Som tidigare nämnts används inte sällan utländska identiteter på så sätt att en medborgare från ett annat EU-land folkbokförs i Sverige och placeras i styrelsen på ett kreditvärdigt bolag, som sedan genomför omfattande kreditköp innan det försätts i konkurs. Identiteterna kan tillhöra personer som mot betalning tillfälligt hämtas in för ett snabbt besök i Sverige och folkbokförs som inflyttad arbetskraft. Med hjälp av falska arbetsgivarintyg får de ett personnummer som sedan används i brottsligt syfte av huvudmännen. Vid behov hämtas personerna för en kort tid tillbaka till Sverige för att ställa upp vid en eventuell identitetskontroll, enligt uppgifter från intervjuade myndighetsrepresentanter. Ett annat alternativ är att identiteter tillhörande EU-migranter som redan befinner sig i Sverige utnyttjas i liknande syfte.

Svårt att kontrollera företagsidentiteter

När det gäller bedrägerier i fraktkedjan menar företrädare för utlämningsställen att svårigheten i att kontrollera identiteter är särskilt stor när företag är inblandade. Enligt intervjupersonen från ett fraktbolag behöver företagets anställda i allmänhet inte fullmakt eller bevis på sin rätt att hämta ut varor för företaget. Det räcker i regel med en leveransavisering och en egen legitimation. Flera intervjupersoner menar att även om personen legitimerar sig som kontaktperson hos företaget, har säljaren svårt att

kontrollera om det är rätt person. En företrädare för näringslivet beskriver problemet:

(…) det är ingen som har kontroll på om du jobbar på det här företaget eller inte, eller att man är firmatecknare eller inte. Så om vi skickar i väg ett paket som ser helt korrekt ut, allt ser jättebra ut, så släpper ju ombuden det. För det finns ingen kontroll.

Försäljning i annans namn: annonsbedrägerier

En mindre avancerad form av bedrägerier med hjälp av osann identitet är att gärningspersonen, vanligtvis via annons, försöker sälja varor eller hyra ut en bostad under annat namn. I cirka en tredjedel av de granskade annonsbedrägerierna (23 ärenden, eller 6 procent av samtliga anmälda brottsbalksbedrägerier) har dokumentationen innehållit information om att någon form av identitetsmissbruk varit en del av brottet. Troligen förekommer falska kontaktuppgifter betydligt oftare vid bedräglig annonsförsäljning, men det framkommer inte alltid tydligt i gärningsbeskrivningen.

Det är relativt ovanligt att andras personnummer utnyttjas, men det kan förekomma när gärningspersonen öppnar ett konto i annans namn på en annonssida. Mer typiskt vid dessa brott är att gärningspersonen använder en annan persons mejlkonto, skapar en mejladress i annans namn eller kapar ett befintligt konto på en annonssida.

Annonsbedrägerier kan alltså ske med hjälp av både stulna och falska identiteter, det vill säga namnet och kontakten kan tillhöra en existerande person eller vara helt påhittade. Bedragaren har samtidigt i dessa fall lite att vinna på att kapa en existerande persons identitet, då syftet framför allt är att dölja sin egen. En typ av annonsbedrägeri där en stulen identitet dock är direkt nödvändig är uthyrning av bostad på falsk grund. Sammanlagt sju av annonsbedrägerierna var av denna typ. Bedragaren uppger i dessa fall en annan persons adress, och inte sällan är det många intressenter som vid samma tillfälle blir lurade på en handpenning.

”Vän i nöd”, falska namnteckningar och övriga typer av identitetsmissbruk

Ytterligare en variant av identitetsmissbruk i bedrägligt syfte går ut på att gärningspersonen låtsas vara en vän, bekant eller släkting till målsägaren genom ett kapat mejl- eller Facebook-konto. Från detta konto skickas ett trovärdigt meddelande om att han eller hon befinner sig i ett utsatt läge, vanligtvis i utlandet, och antingen behöver pengar eller målsägarens kontouppgifter. Sammanlagt tio sådana ärenden (2,5 procent) finns i det granskade materialet.

I ytterligare sex ärenden framgick att gärningspersonen förfalskade en namnteckning i bedrägligt syfte. Två av dessa gäller affärer med bil respektive husvagn, där gärningspersonen förfalskat en namnunderskrift i samband med ägarbytet. Ett annat fall avser ett bedrägeri där en ekonomiansvarig på ett assistansföretag olovligen undertecknat målsägarens ansökan om vilande sjuk- och aktivitetsersättning och skickat det till Försäkringskassan. Ett ärende gäller falska resecheckar och ett annat olovligt byte av abonnemang genom en urkundsförfalskning.

I Brås granskning identifierades slutligen ett antal ärenden med bedrägeri enligt brottsbalken där identitetsmissbruk förekommer utan att dessa kan sägas tillhöra en större kategori. Två ärenden avser lån med ett stulet eller borttappat bibliotekskort; i det ena fallet har gärningspersonen lånat böcker och musik till ett värde av 6 000 kronor och inte återlämnat lånet. Ytterligare exempel på ”övrigt” identitetsmissbruk var ett fall av romansbedrägerier med osanna kontaktuppgifter, två fall av nätfiske utan domänkapning (målsägare ska ha vunnit i en tävling eller lotteri och ombeds lämna sina kontouppgifter), samt ett antal bedrägerier med falska registreringsskyltar (räkningar för tullavgifter i utlandet) och parkeringsböter för en bil som målsägaren inte äger.

Identitetsmissbruk vid bidragsbrott och andra välfärdsbedrägerier

Vid bidragsbrott saknas oftast skäl för bedragaren att vilseleda med hjälp av sin identitet, utan det är typiskt sett andra uppgifter om denne som inte stämmer. Även om en bidragssökande med bedrägligt uppsåt vanligen inte har något att vinna på att använda en osann identitet i kontakten med den utbetalande myndigheten, kan det vid bidragsbrott förekomma falska eller manipulerade intyg av olika slag – sjukintyg, arbetsgivarintyg eller liknande. Bland de 50 bidragsbrottsärenden som Brå har granskat har det visserligen förekommit få indikationer på att falska intyg använts som ett led i brottet, men det kan snarare handla om bristande dokumentation i ärenden. Från andra studier finns exempel på förfalskade namnteckningar på arbetsgivarintyg, läkarintyg, närvarointyg, studieintyg och tidrapporter (se vidare Brå 2015:8).

Tidigare studier har identifierat att enskilda personer har haft multipla identiteter, ibland med bidrag i flera identiteter parallellt (Brå 2015:8, NUC 2015b). Även om identitetsmissbruk sannolikt är ett vanligare inslag i brottsbalksbedrägerier, är den identitetsrelaterade bidragsbrottsligheten ett uppenbart missbruk av systemen och ett sätt för en enskild person att nå stora volymer av utbetalade bidrag genom sin brottslighet. Därför kan dessa brott ses som särskilt allvarliga – och i nuvarande situation svåra att förebygga och motverka.

Inte bara ekonomiska konsekvenser

Stulna identiteter: tids- och energikrävande åtgärder för den som drabbas

De ekonomiska förlusterna vid rena kreditbedrägerier genom köp eller lån i annans namn drabbar främst de säljande företagen. Även för enskilda har dessa brott stora konsekvenser, dock främst i andra termer än ekonomiska; den drabbade slipper vanligtvis betalningsansvar om köpet eller fakturan bestrids, identiteten spärras för nya kreditköp och händelsen polisanmäls. Däremot krävs det mycket arbete för att spärra själva identitetshandlingen; det sker genom ett samtal till någon av utfärdarna eller tillverkarna av identitetshandlingar.[51] Vidare bör den drabbade spärra sin identitet för kreditköp. I dagsläget finns ett tjugotal olika, av Datainspektionen godkända, kreditupplysningsföretag.[52] Bedragarna har ofta en god kännedom om vilka företag som använder mindre kreditupplysningsföretag och utnyttjar detta. UC AB svarar i dag för en övervägande majoritet av kreditupplysningsmarknaden, vilket gör att spärrarna där är de mest effektiva. Det näst största kreditupplysningsföretaget är Bisnode.

Det är uppenbart att det stora antalet aktörer och den i dag obefintliga samverkan[53] mellan dem gör det både oöverskådligt och mycket tidskrävande för den enskilde att försäkra sig om att man inte fortsätter att missbruka hans eller hennes identitet. Även om både identitetshandlingen och möjligheten till kreditköp spärras, kan dessutom bedragaren använda den stulna identiteten i kontakt med myndigheter eller inom sjukvården. Den spärrade identiteten för kreditköp skapar även problem vid legitima köp under en tid framöver, och det finns inga generella rekommendationer för hur länge personen bör behålla kreditköpsspärren (se även NUC 2015b).

Falska identiteter: stora konsekvenser för välfärdssystemet

Även om användning av falska identiteter, utan koppling till existerande personer, inte skadar en enskild på samma omedelbara

---

[51] Gällande körkort är det Transportstyrelsen, gällande Skatteverkets kort och SIS-märkta kort är det Oberthur eller Gemalto, för pass eller nationellt id-kort är det polisen man bör kontakta.

[52] http://www.datainspektionen.se/lagar-och-regler/kreditupplysningslagen/gallande-tillstand/. Samtidigt har det i intervjuer framgått att det enbart finns 5-6 aktiva bolag i dag, dvs. betydligt färre än antal tillstånd från Datainspektionen.

[53] För närvarande pågår dock ett utvecklingsprojekt där samtliga 6 aktiva bolag under 2015 utvecklat en systemlösning som innebär att den person som drabbas av en identitetsstöld bara ska behöva kontakta ett av bolagen för att anmäla händelsen. Det bolaget ska då kontakta samtliga övriga bolag som även de lägger en spärr i sina system. Detta ska även fungera när personen vill häva sin spärr. Systemet kommer att testas i början av 2016, men kvalitetskraven är höga och när den slutgiltiga lösningen finns på marknaden är i dag oklart.

vis som en ren identitetsstöld, utgör de ett omfattande problem för välfärdssystemet liksom för näringslivets funktioner. I förlängningen drabbar den även enskilda i form av högre priser och kostnader för vissa tjänster.

Även om det inte ligger ett intrång i eller en stöld av en persons identitet bakom falska identitetshandlingar, är gränsen mellan stulna och falska identiteter flytande. Sannolikt rör det sig relativt sällan om rena ”luftslott”, utan det kan finnas kopplingar till en existerande person – om än i flera led, avlägsna i både tid och rum. Däremot motsvarar långt ifrån alltid en falsk identitet en äkta sådan, utan en äkta identitet kan generera många falska. Det innebär att det förekommer en mängd felaktigheter redan i själva folkbokföringen, som alla övriga system som arbetar med personuppgifter stödjer sig mot. De intervjuade myndighetspersonerna menar dessutom att det inte rör sig om några försumbara brister, utan att problemet är av relativt stor omfattning, med betydande konsekvenser för välfärden. Samtidigt är det oklart i vilken grad dessa helt falska identiteter används just vid bedrägerier; enligt intervjupersonerna har det primära syftet i dessa fall oftast varit annat än kriminell verksamhet (t.ex. att få uppehållstillstånd). Att falska identiteter utnyttjas i bedrägligt syfte tycks dock vara ett faktum.

Inte ett brott i dag

Olovligt bruk av annans identitet som innebär en skada eller olägenhet för den vars identitet har använts är inte ett självständigt brott i dag. Det finns dock en rad bestämmelser som tangerar området; framför allt gäller det gärningar som regleras enligt kap. 14 (Om förfalskningsbrott) och 15 (Om mened, falskt åtal och annan osann utsaga) BrB. I vissa fall kan identitetsmissbruk lagföras som ett förberedelsebrott.

Egendomsskyddsutredningen (SOU 2013:85) har lämnat ett förslag på att kriminalisera *identitetsintrång*. Det nya brottet skulle omfatta olovligt bruk av uppgifter som kan användas för att identifiera en levande fysisk person. Med sådana uppgifter menas exempelvis personnummer, samordningsnummer, namn och adress. Enligt utredningen skulle det nya brottet bland annat göra det lättare för samhället att ingripa mot vissa systematiska bedrägerier på ett tidigt stadium.

I en lagrådsremiss (2016-02-11) har regeringen föreslagit att ett nytt brott ska införas i brottsbalken under namnet *olovlig identitetsanvändning*. Syftet är, enligt remissen, att motverka missbruk av identitetsuppgifter och ge skydd mot den integritetskränkning det innebär att få dessa utnyttjade. Genom att kriminalisera dessa gärningar får drabbade bättre möjlighet att ta vara på sin

rätt.[54] För straffansvar krävs att gärningspersonen utger sig för att vara någon annan genom att olovligen använda den personens identitetsuppgifter och på så sätt ge upphov till skada eller olägenhet för denne. Som bestämmelsen är formulerad innebär det viss vidgning av utredningens förslag.[55] Straffet föreslås vara böter eller fängelse i högst två år. Till skillnad från utredningens förslag ska brottet inte falla under allmänt åtal. Lagändringarna ska träda i kraft 1 juli 2016. För mer detaljer kring närliggande lagstiftning samt det nya lagförslaget, se bilaga 5.

Felande länkar och förbättringspotential

Det finns många tänkbara sätt att bekämpa den växande problematiken med användning av osanna identiteter. När åtgärder för att bekämpa identitetsmissbruk diskuterats med olika aktörer tenderar fokus att hamna på kontroller av befintliga identitetshandlingar. Grundfrågan är dock hur osanna identiteter blir till, det vill säga hur falska identiteter skapas eller äkta identiteter kapas – och hur dessa processer kan förhindras.

Bristande ursprungsidentifiering

Som tidigare beskrivits har det i intervjuerna med berörda aktörer framkommit att folkbokföringsregistret, som både andra myndigheter och företag förlitar sig på när det gäller uppgifter om enskildas identiteter, innehåller en mängd felaktigheter. Ett stort problem tycks vara att det bakom ett flertal identiteter kan finnas en och samma person, till exempel någon som invandrat till Sverige ett antal gånger med enbart marginellt ändrade identitetsuppgifter. Det innebär att det förekommer personnummer utan någon koppling till en unik existerande person. Personen i fråga kan sedan begå brott under vissa av dessa identiteter och leva ett ordnat liv under andra. Förutom att detta skapar förutsättningar för omfattande och systematisk brottslighet äventyrar det i förlängningen själva rättssystemet, eftersom – för att citera en intervjuad polis – ”*du vet till slut inte vem som blivit lagförd*”.

Behovet av säker ursprungsidentifiering,[56] som rimligtvis är att anse som det mest centrala för att motarbeta identitetsmissbruk,

[54] Utöver det föreslås att brottet olaga förföljelse ska omfatta gärningar som utgör olovlig identitetsanvändning.

[55] Bl.a. ska, i linje med Datainspektionens remissyttrande, även fotografier av en verklig person tillsammans med uppdiktade namn- och adressuppgifter (exempelvis falska konton på sociala medier) omfattas av vad som menas med identitetsuppgifter, enligt bestämmelsen.

[56] Att säkra ursprunget är inte enbart viktigt vid migration, men utgör där troligen den största utmaningen. Det är inte möjligt att alltid med säkerhet spåra en persons identitet före inresan, men i samband med registreringen i Sverige måste det finnas starka ambitioner att skapa en ytterst säker koppling mellan *en* person och *en* identitet. Självklart gäller det även personer födda i Sverige.

har också lyfts i en rad rapporter (Skatteverket 2014), och flera skrivelser från berörda aktörer har överlämnats till regeringen.[57]

Oklarheter kring lagstöd

Trots medvetenheten om problemet med identitetsmissbruk saknar myndigheterna verktyg för att motverka det. Vid misstanke om felaktiga identitetshandlingar sker det ibland en polisanmälan från myndigheterna, även om de inte har anmälningsplikt och även om det råder osäkerhet beträffande lagstöd. De fall som anmäls avser oftast brukande av falsk urkund eller förberedelse till brott, enligt de intervjuade. Myndigheterna menar dock att det förekommer en stor regional variation i hur dessa anmälningar tas emot och behandlas. Det finns med andra ord ingen samsyn i frågan om hur den rådande lagstiftningen kan eller bör tillämpas. Huruvida osanna identiteter betraktas som förberedelsebrott skiljer sig, enligt intervjuade poliser, mellan landets olika bedrägerirotlar. Behovet av att förtydliga vilket – om något – lagstöd som gäller, alternativt en ny lagstiftning, är uppenbart.[58]

Biometriska data – kontroversiellt men nödvändigt?

Med biometriska data menas uppgifter om en enskild persons fysiska, fysiologiska eller beteendemässiga kännetecken, som gör det möjligt att identifiera personen; det kan vara allt från ansiktsbilder, namnteckning, fingeravtryck till DNA-uppgifter. I många av Brås intervjuer har biometriska data beskrivits som den mest effektiva metoden för att både säkra ursprunget och förbättra identitetskontroller. Samtidigt finns det en utbredd uppfattning om att frågan är kontroversiell ur integritetssynpunkt. Faktum är dock att biometrisk identifiering redan används i ett stort antal andra länder, och i vissa sammanhang även i Sverige (pass, mobiltelefoni m.m.). Många av de intervjuade nämner fler lösningar som tänkbara i framtiden, när ”tiden är mogen”. Man menar att insikten om vikten att skydda sin identitet, och om konsekvenser av eventuellt missbruk, just har börjat växa fram både hos allmänheten och på en politisk nivå. Integritetsfrågor anses i dag många gånger väga tyngre än kontrollbehovet, men när insikten om skyddsbehovet har etablerats kommer frågan att kunna behandlas på ett annat sätt.

---

[57] Bland annat Svenska Bankföreningen, ”Ett initiativ för att minska antalet identitetsintrång: färre godkända ID-handlingar och bättre identitetskontroll”, daterad 2015-06-22, KRONAN Säkerhet AB, ”Från checkbedrägerier till identitetsintrång”. PM inför möte den 22 april 2015 med Justitieutskottet, daterat 2015-04-18.

[58] Förslaget om att kriminalisera olovlig identitetsanvändning (bilaga 5), träffar inte bruket av helt falska identiteter, som inte innebär ett intrång i en existerande persons identitet. I detta fall är åtgärder riktade mot en säkrare ursprungsidentifiering den mest angelägna strategin.

Olika former av biometrisk identifiering har diskuterats av de intervjuade; som ett exempel kan nämnas lagring av biometriska data (fingeravtryck, ansikte, iris) på identitetshandlingar med hjälp av chip och pin. Det kan finnas flera lösningar, men framför allt är det önskvärt att på ett eller annat sätt bygga in ytterligare säkerhetshöjande detaljer i de fysiska identitetshandlingarna i takt med att förfalskningarna blir bättre.

Förutom vid säkrare identitetshandlingar kan biometriska data även användas vid exempelvis kortbetalningar. Norge tycks exempelvis vara ledande i att testa kontaktlösa betalkort med fingeravtrycksidentifiering (Zwipe MasterCard) i stället för PIN-kod. Användning av liknande teknik är både säkrare ur identitetssynpunkt och snabbare och smidigare för kunden – ett exempel på att smidighet och kontroll inte behöver stå i konflikt.[59]

Många identitetshandlingar, ingen samordning

Identiteter och identitetshandlingar

Många bedrägerier där gärningspersoner vilseleder med hjälp av sin identitet sker utan något bruk av identitetshandlingar. Det är därför viktigt att hålla isär begreppen *identitet* och *identitetshandling*. I tabell 22 ges några exempel på tänkbara kombinationer relaterade till olika tillvägagångssätt vid identitetsmissbruk. Beskrivningen är på inget sätt uttömmande men syftar till att ge en bild av komplexiteten i frågan om identitetshandlingar. Inte sällan används identiteter och identitetshandlingar synonymt, vilket kan vara missvisande.

Som tidigare nämnts kan det förekomma både falska och stulna, men även utnyttjade identiteter, där någon under utpressning eller mot betalning lånar ut sin identitet. Förutom att medborgare i detta syfte hämtas från andra EU-länder för en snabb folkbokföring har det även framkommit att identiteter av EU-migranter som befinner sig i Sverige utnyttjas i brottsliga syften (NUC 2015b). I dessa fall är identitetshandlingarna äkta, men inte identiteten. Detsamma gäller även äkta identitetshandlingar utfärdade på basis av falska identiteter och äkta handlingar med stulna eller ”utlånade” identiteter (s.k. look alike). Bedrägerier med hjälp av äkta handlingar och osann identitet är rimligtvis mycket svåra att bekämpa.

[59] Då avläsning av biometriska data inte sällan sker med hjälp av FRID (Radio Frequency Identification) skapar det möjlighet för obehörig avläsning inom visst avstånd. Det innebär att även biometriska data kan kapas och användas vid tillverkning av nya identitetshandlingar. Att missbruka kapade biometriska uppgifter vid bedrägerier bör rimligtvis vara svårt, då de vid kontroll måste matcha en fysisk person. Problemet är dock att det i Sverige saknas teknisk utrustning för sådana kontroller.

Falska identitetshandlingar kan vidare basera sig både på helt falsk och på stulen identitet. Exempel på det sistnämnda är inte minst den omfattande tillverkningen som under 2015 avslöjades i Stockholmsområdet. Vid bedrägerier med falska identitetshandlingar och falska identiteter kan gärningspersonen exempelvis använda ett falskt utländskt pass som inte kan kopplas till en existerande person. Detta kan ske innan passet eventuellt bytts mot en annan äkta identitetshandling.

Slutligen förekommer även manipulerade handlingar där uppgifter ändras i en ursprungligen äkta identitetshandling. Även dessa kan bygga på falska identiteter (som när flera identiteter skapas genom att ändra ursprungliga riktiga uppgifter till nya, påhittade) eller stulna (när en annan persons äkta identitetshandling ändras, exempelvis genom utbytt bild, till förövarens identitetshandling).

Tabell 22. Osanna identiteter och olika typer av identitetshandlingar som används i ett vilseledande syfte.

	Osanna identiteter		
	Falsk identitet	**Stulen identitet**	**Utnyttjad (äkta) identitet**
Äkta id-handling	Luftslott, ingen koppling till en existerande person	”look alike”, stulna id-handlingar	”look alike”, utpressad målvakt, utnyttjade EU-migranter
Falsk id-handling	Falskt utländskt pass, ingen koppling till en existerande person	Falskt id-/körkort i annans namn	-
Manipulerad id-handling	Ursprungligen äkta utländskt pass med manipulerade uppgifter (för dubbel identitet)	T.ex. äkta körkort med annan bild	-

15-tal godkända identitetshandlingar

Ett starkt tema i Brås intervjuer, vid sidan av säkrare ursprungsidentifiering, var det stora antalet godkända identitetshandlingar i Sverige. Att antalet identitetshandlingar försvårar identitetskontroller och underlättar missbruket har även påpekats i en rad rapporter och lyfts som ett problem av flera aktörer.[60] I dag finns det cirka 15 godkända identitetshandlingar i Sverige, och dessa utfärdas av tre myndigheter – polisen, Skatteverket och Transportstyrelsen. Utöver det kan större banker utfärda SIS-godkända id-kort (SIS = Swedish Standards Institute) åt sina kunder, och även vissa företag och myndigheter får utfärda SIS-godkända id-kort till sina anställda.[61] Alla dessa handlingar håller en relativt

[60] Nationellt Forensiskt Centrum (2015) och Svenska Bankföringen (Ju2015/05176/L4).

[61] Norske Veritas Certification AB (DNV) ger tillstånd till företag och organisationer att utfärda SIS-märkta kort. För att kunna få tillstånd krävs att företaget varit etablerat i Sverige i minst ett år och har minst fem anställda. Ett annat kriterium är att företaget/myndigheten eller dess företrädare inte är registrerade för några brott och att företaget har god intern kontroll och säkerhet (NUC 2015a).

god säkerhetsstandard, men är utställda utifrån olika krav och vid olika tidpunkter. De senast producerade handlingarna håller en högre säkerhetsstandard, medan vissa – framför allt de äldre handlingarna – är lättare att förfalska. Det visar bland annat polisens kartläggningar (NBC 2015b).

Körkort som en identitetshandling

Flera aktörer har lyft frågan om lämpligheten i att svenskt körkort utgör en godkänd identitetshandling – något som inte är vanligt förekommande i andra länder. Det finns ingen skriven rättsregel som stadgar att svenskt körkort ska utformas så att det kan fungera som en legitimationshandling. Redan 1970 fastslog en statlig utredning att svenskt körkort av hävd har godtagits som legitimation (SOU 1970:26 s. 29). Denna hävd har kunnat upprätthållas i och med att regelverket och de myndigheter som har ansvarat för att utfärda körkort har följt med i utvecklingen av legitimationshandlingar.

Som ett av problemen har anförts att det är möjligt att byta in körkort utfärdade i andra länder inom EES samt i Japan och Schweiz mot svenska körkort och därmed få en giltig identitetshandling. Även om det i samband med detta görs identitetskontroller i Sverige kan man inte veta om ursprungslandet gjort en motsvarande korrekt kontroll inför utfärdande av körkort i det landet. I andra länder, där körkortet bara är en handling som bevisar förarbehörighet, är inte kontrollerna kring att fastställa rätt identitet av samma dignitet som om det vore en ansökan om en identitetshandling. Ytterligare ett problem som beskrivs av de intervjuade är den långa giltighetstiden; körkortet är den enda identitetshandlingen som är giltig i 10 år.[62] Samtidigt är i dag körkortet den handling som de flesta använder för att styrka sin identitet, och förändringar i detta avseende kan sakna förankring hos allmänheten. Det pågår ett arbete hos Transportstyrelsen som syftar till att kartlägga omständigheter som talar för respektive emot körkortets status som identitetshandling.

Avsaknad av en central aktör som garanterar säkra identitetshandlingar

Ett nationellt id-kort samt en central aktör, gärna en myndighet, som garanterar säkra identitetshandlingar är två åtgärder som efterfrågas från flera berörda myndigheter och delar av näringslivet. Om önskemål på en gemensam identitetshandling inte kan uppfyllas bör antalet godkända handlingar begränsas,

[62] Minimikrav för körkortsbehörigheten regleras genom Europaparlamentets och rådets direktiv 2006/126/EG om körkort. Direktivet ställer bl.a. hårda krav på kortets utseende, varför utrymme för säkerhetselement (s.k. dokumentsäkringar) begränsas.

menar flertalet aktörer. När det gäller frågan om en central aktör har Svenska Bankföreningen gjort en framställan till regeringen (Ju2015/05176/L4) som föreslår att en nationell gemensam utfärdandeprocess av svenska identitetshandlingar bör införas, och att staten bör ta på sig ansvaret i processens samtliga faser.

Behov av samordning och informationsflöde mellan myndigheterna

Både i andra kartläggningar (NUC 2015b) och i Brås intervjuer har det betonats att det är angeläget med en förbättrad samsyn på myndighetsnivå för att på ett tidigt stadium kunna förebygga identitetsmissbruk. Det betonas att det är viktigt för myndigheterna att tänka utifrån ett helhetsperspektiv och sträva efter ett effektivare sätt att utbyta information, om det finns en misstanke om att en identitet missbrukats. Det är angeläget att bl.a. skapa enhetlig tolkning av vilka uppgifter som får delas mellan myndigheter, något som saknas i dag. Det påpekas att servicefokus och kontrollverksamhet inte alltid är i balans, det vill säga kontrollen får stå tillbaka. Ett relaterat problem som försvårar tidiga kontroller är skyndsamhetskraven i handläggningen, något som minskar förutsättningar för att upptäcka en falsk eller manipulerad handling vid ansökan om en ny äkta id-handling (ibid).

Offentlighetsprincipen och sekretess

Vid sidan om de många identitetshandlingarna finns det en annan för Sverige utmärkande omständighet, nämligen att det är mycket lätt att få tillgång till andras personnummer. Som ett skäl till detta anges offentlighetsprincipen, som innebär att regeringens och andra myndigheters verksamheter ska vara öppna och transparenta. I tryckfrihetsförordningen, en av våra grundlagar, finns det bestämmelser om allmänhetens rätt att ta del av allmänna handlingar (Regeringskansliet, 2013). I praktiken innebär det bl.a. att vem som helst kan ta del av myndigheternas handlingar i den mån de inte omfattas av sekretess.

En del av de intervjuade menar dock att det faktum att personnummer är lättillgängliga för allmänheten inte kan hänföras till offentlighetsprincipen.[63] Denna princip är till för att allmänheten ska ha möjlighet att granska regeringens och myndigheternas verksamhet, vilket sällan är aktuellt när enskilda personer begär ut andras personuppgifter hos Skatteverket. För att införa en mer

[63] I Sverige får personnummer lämnas ut, utom när 22 kap. 1 § 1-2 st. offentlighet och sekretesslagen (2009:400) bör tillämpas. Enligt denna ska uppgifter från bl.a. folkbokföringen inte lämnas ut om det kan antas att den enskilde eller någon närstående till denne lider men om uppgiften röjs (en bedömning som i praktiken är omöjlig att göra under ett telefonsamtal, enligt de intervjuade).

restriktiv hållning till myndigheternas utlämnande av personnummer (eller andra personuppgifter) krävs alltså ingen ändring i grundlagen, utan en ändring av offentlighets- och sekretesslagen. En mer restriktiv syn i denna fråga skulle, enligt de intervjuade, förhindra många situationer där känsliga uppgifter hamnar i fel händer, inte minst hos personer med bedrägligt uppsåt. Man förespråkar en översyn av rutiner kring hantering av personnummer och hur dessa rutiner regleras.[64]

Säkrare kontroller på utlämningsställen

Viktigt att stoppa i ett tidigt skede

I Brås intervjuer om identitetsmissbruk har huvudfokus riktats mot bristande identitetskontroller inom fraktkedjans sista steg, det vill säga utlämning av försändelser, snarare än mot det vanligaste första steget – beställningen av varan på internet. Argumenten handlar, återigen, ofta om att internetköp bör vara enkla och smidiga, och att införande av extra säkerhetssteg kan leda till att konsumenterna väljer att handla på sidor som inte kräver dessa steg. Samma argument är dock applicerbara även på situationer i kassakön vid ett utlämningsställe. Att själva varuhandeln flyter på är en första prioritering för butikerna, ibland på bekostnad av identitetskontroller vid utlämnande av försändelser.[65]

Att handeln vet vem kunden är beskrivs som det centrala i förebyggandet av handelsrelaterade former av identitetsmissbruk. Det bör gälla lika mycket i samtliga faser av köpprocessen, det vill säga vid beställning/kortbetalning, eventuell kreditprövning och vid leverans/utlämning. Att avbryta det brottsliga förfarandet i ett så tidigt skede som möjligt, genom säkrare internetbeställningar, bör dock vara angeläget. Samtidigt innebär varuutlämning ett direkt fysiskt möte, vilket, utifrån de tekniska lösningar som är tillgängliga i dag, skapar bättre förutsättningar för kontroller. Det kommer även i fortsättningen alltid att vara nödvändigt att säkerställa att den person som hämtar ut varan verkligen är eller representerar den som beställt och ska betala för varan.

---

[64] I intervjuerna uttryckte exempelvis de berörda myndigheterna önskemål om att utlämnande av personuppgifter i högre grad och med större tydlighet bör sekretessbeläggas vid misstanke om identitetsmissbruk. Det bör vara tvingande för myndigheterna att anmäla misstanke om brott. Myndighetsrepresentanter menade att det även vore optimalt att alla förfrågningar gällande personuppgifter hos myndigheter registreras, så att varje individ har möjlighet att, i likhet med kreditprövning, kontrollera vilka som har begärt information om honom eller henne och i vilket syfte.

[65] Svenska Bankföreningen har även i sin skrivelse till regeringen (2015-06-22) lyft behovet av säkrare rutiner gällande försändelser med känsligt innehåll (exempelvis kontokort).

Incitament saknas för säkra kontroller

Arbetet med säkra utlämningar av försändelser är dock, liksom hela bedrägeriområdet, förknippat med en mängd dilemman. Förutom att mer noggranna kontroller förväntas skapa irritation hos kunderna, beskriver representanter för handeln även ett motstånd mot att informera om varför identitetskontrollerna behöver skärpas, då butiken inte vill förknippas med brottsrisker. Även i dessa sammanhang (liksom från myndigheternas håll) lyfts ibland att butikerna inte har en i första hand brottsförebyggande funktion, och det saknas därmed incitament att motverka identitetsmissbruk. Det är dessutom sällan själva butiken som drabbas av en ekonomisk skada vid bedrägeri med hjälp av identitetsmissbruk, då det är svårt att bevisa att identitetskontrollen har brustit. Samtidigt finns det verktyg som redan i dag underlättar kontrollerna, och fler moderna lösningar tycks – enligt vad som beskrivs nedan – vara på väg.

De sju stegen och nya tekniska lösningar

Som branschstandard används i dag handboken *De sju stegen*, en process för identitetskontroll som har tagits fram av Svenska Bankföreningen.[66] Enligt denna ska personalen vid identitetskontroll inför utlämning av försändelser följa sju manuella steg.

De sju stegen används i huvudsak av bankerna, vissa logistikföretag och andra aktörer som utsätts för bedrägerier kopplade till identitetsmissbruk. Det är oklart hur det (icke tvingande) bruket av *De sju stegen* fungerar i praktiken vid olika utlämningsställen. Att titta på legitimationen anses ofta räcka som identitetskontroll, menar intervjupersoner. Personalen som kontrollerar identiteten tittar på fotot och jämför med personen på plats. En representant för handeln säger:

> *Man tittar att det är samma figur. Man håller i id-handlingen och man kontrollerar. Då har man gjort det man ska.*

Dagens falsktillverkade handlingar är samtidigt väldigt svåra att skilja från äkta, enligt de intervjuade. I en stressad situation kan det vara svårt för kassapersonalen att noggrant följa alla stegen och göra rätt bedömning.

På senare tid har nya tekniska lösningar sökt sig till marknaden för att förbättra identifieringen och avlasta personalen inom handel och logistik. En sådan lösning är identifiering med hjälp av en scanner,[67] som tydligt skiljer mellan äkta och falsk handling. Samtliga i Sverige godkända identitetshandlingar, inklusive pass,

[66] http://www.desjustegen.se

[67] Tjänsten heter V*erified by 365id och* är en abonnemangstjänst framtagen i nära samarbete med näringslivet och företrädare inom säkerhetsfrågor. Tjänsten pilottestades under 2015 och beräknas vara klar för användning under 2016.

kontrolleras mot en central databas där även bilder på varje kontrollerad identitetshandling sparas under en period. En mängd olika tjänster kan kopplas till denna, så som spärrfunktioner eller själva kreditprövningen.

Tanken är att använda samma säkra identifiering inte enbart inom handeln utan även hos myndigheter och inom sjukvården. Om liknande lösningar får stor spridning kan många bedrägerier hindras där falska identitetshandlingar används. Även bedragare som använder äkta handlingar baserade på felaktiga personuppgifter eller stulna eller lånade handlingar med look-alike foto kan med hjälp av denna lösning stoppas tidigt, tack vare den heltäckande spärrfunktionen. Att bilderna sparas i en databas kan också underlätta polisens utredningsarbete, då det blir lättare att spåra bedrägerierna. Om metoden får fäste på marknaden tyder mycket på att en sådan lösning har en stor potential när det kommer till att förebygga identitetsrelaterade bedrägerier.

Bristande kontroller vid direktleverans

I vissa fall levereras beställda varor direkt till en hem- eller företagsadress, i stället för till ett utlämningsställe. I Brås intervjuer har det framkommit att det är oklart hur ofta någon form av identitetskontroll genomförs. Ibland kan det, enligt de intervjuade, räcka med att mottagaren kvitterar ut varan med en underskrift, inte sällan enbart en elektronisk sådan. En representant för ett fraktföretag beskriver följande problem:

> *När det är stora företag, gör de väl inte riktigt alla kontroller. De går ju med på att skicka godset till en adress, som det här företaget normalt sett inte har. För de är ofta redan kunder hos lasten till exempel. Så ringer någon och beställer telefoner och talar om att de öppnat ny lokal någonstans och vill ha grejerna dit. Sen gör de inte alltid kontroller.*

Vissa företag brukar även, enligt de intervjuade, sluta överenskommelser med fraktleverantören om att deras beställningar kan levereras till den aktuella adressen och lämnas där även när ingen fysisk mottagare är närvarande.[68] Självklart kan sådana rutiner utnyttjas av bedragare.

Om gärningspersonen har kunnat beställa en sms-bekräftelse till sitt eget mobilnummer (i stället för den kapade personens) kan denna räcka som identifiering vid en utlämning, menar intervjupersoner. Vissa fraktleverantörer anser att de utför tillräckliga kontroller om de kontrollerar att namnet på leveransen överensstämmer med den legitimerande personens. Det möjliggör att

[68] Det rör sig om tilläggstjänster som regleras i avtal. Fraktfirman får med andra ord inte på eget bevåg bara ställa ifrån sig godset.

gärningspersoner med samma namn som den vars identitet har stulits kunnat kvittera ut varor, menar intervjupersoner.

Att identifiera sig på internet

Som redan nämnts bör samtidigt större fokus riktas mot att stoppa bedrägerier tidigt, innan varan börjat följa fraktkedjan. Även vid beställning eller lån på internet behöver man vanligtvis identifiera sig, men säkerhetskraven är mycket olika på olika försäljningssidor. Vid beställning av varor räcker det inte sällan med ett personnummer, namn och adress. Handelns representanter befarar att fler säkerhetssteg i denna fas av transaktionen skulle leda till minskad försäljning. Enligt e-handelns egna analyser (Dibs 2015) avbryts drygt en tredjedel av internetköpen innan betalning, och det är vanligare bland vana konsumenter som ställer höga krav på smidiga, snabba köp. Enligt de intervjuade representanterna för handeln sjönk försäljningen när vissa sajter började använda säker autentisering (s.k. 3D secure[69]). Det ligger alltså en särskild utmaning i att få kunder att förstå vikten av säkra lösningar. Att införa branschgemensamma säkerhetsåtgärder kan också vara en del av ett framgångsrikt säkerhetsarbete.

BankID och andra e-legitimationer

Vid tecknande av lån eller vid större transaktioner på internet, liksom vid kontakter med myndigheter, behöver man ofta använda en elektronisk legitimation. Med hjälp av en e-legitimation kan man legitimera sig, logga in och skriva under avtal och godkänna transaktioner på olika myndigheters, bankers och företags sidor. I Sverige utfärdas e-legitimationer dels av Telia,[70] men framför allt av flera banker genom olika varianter av så kallad BankID. Denna e-legitimation finns både som smart kort med kortläsare, som fil som kan sparas på en dator och som en mobilapplikation. BankID är det absolut största e-legitimationssystemet i Sverige.[71]

Ett ökat användande av e-legitimationer har av många intervjuade beskrivits som en effektiv förebyggande åtgärd; olika finansiella tjänster[72] övergår från inloggning med exempelvis användarnamn och lösenord till inloggning med e-legitimation. En åtgärd som beskrivs av representanter för e-handel är att nya

[69] Verified by Visa/Mastercard Secure Code.

[70] Kopplat till id-kort från Skatteverket.

[71] Tjänsten förvaltas av företaget Finansiell ID-Teknik BID AB som ägs av flera svenska banker.

[72] Exempelvis kreditupplysningsföretagen, genom högre krav från Datainspektionen gällande säkerhet och autentisering (kontroll av uppgiven identitet). https://www.uc.se/kundservice/anvandarsupport-for-vara-tjanster/inloggning-till-vara-tjanster.html

kundprofiler på en del sajter skapas genom en verifiering med BankID (NBC 2015a). När sedan känslig information, som kontokortsuppgifter, uppdateras, verifieras dessa via BankID.

Att använda elektronisk legitimering bedöms som relativt säkert. De risker som finns ligger i första steget, det vill säga i samband med den fysiska identifieringsprocessen när en kund skaffar en e-legitimation. Alla banker kräver exempelvis inte att kunden personligen besöker kontoret i detta skede, utan ett BankID kan beställas via internet med hjälp av en bankdosa.[73] Om en bedragare lyckas komma över en annan persons bankdosa och kontouppgifter och med hjälp av dessa skaffa ett bedrägligt BankID, skapar det många möjligheter till systematisk bedrägeriverksamhet – med minimal upptäcktsrisk.

E-legitimationsnämnden planerar att under år 2016 införa ett valfrihetssystem för e-legitimation (Svensk e-legitimation) för att nå en gemensam standard för myndigheterna. Det bör rimligen utgöra ett steg mot de förbättringar i samverkan och informationsutbyte som många efterfrågar.[74] [75]

Identitetsmissbruk i huvuddrag

Det kan konstateras att olovligt bruk av andras identiteter i ett bedrägligt syfte är ett omfattande och växande problem i Sverige (Se bilaga 4). Både stulna och helt falska identiteter utan koppling till existerande personer används för att vilseleda en annan för egen vinning. Då det inte alltid rör sig om rena stölder av existerande identiteter har Brå valt att beskriva problemet som identitetsmissbruk. Det refererar till situationer då gärningspersonen helt enkelt låtsas vara någon annan i samband med ett bedrägeri – för att skaffa sig en vinning eller för att mörka spåren. Det kan ske med hjälp av identitetshandlingar (köp i annans namn vid kreditbedrägerier) eller utan (t.ex. falska kontaktuppgifter vid annonsbedrägerier). Någon form av identitetsmiss-

[73] Det finns fyra olika skyddsklasser, eller 'tillitsnivåer' som svarar mot olika grader av teknisk och operationell säkerhet hos utfärdaren och olika grader av kontroll av att en person som tilldelas en elektronisk identitet verkligen är den han eller hon utger sig för att vara. Nivåindelningen motsvarar den som används i den internationella standarden ISO/IEC 29115 (E-legitimationsnämnden 2015).

[74] Svensk e-legitimation underlättar dessutom den samordning och övergång som krävs utifrån nya EU-regler och krav på offentliga e-tjänsters legitimeringar och e-underskrifter.

[75] Det är upp till varje utfärdare att välja att ansöka om att gå med i Svensk e-legitimation, det vill säga både nuvarande och nya e-legitimationer har möjlighet att ingå i Svensk e-legitimation och följa regelverket. Målsättningen är att BankID deltar i detta projekt som leverantörer av eID-tjänst mot valfrihetssystemet. Upphandlingen av eID-leverantörer vänder sig till den offentliga sektorn, men avtalen med godkända e-legitimationsutfärdare (Svensk e-legitimation) kan användas i den privata sektorns upphandlingar, inte minst inom e-handeln. Vilka konsekvenser lösningen får för handeln är dock i dagsläget oklart.

bruk förekommer i alla typer av bedrägerier som identifierats i ärendegranskningen. Enligt en skattning ingår det som ett led i minst 63 procent av polisanmälda bedrägeriärenden. Många olika problemområden har identifierats av intervjupersonerna från myndigheter, rättsväsendet och näringslivet, men det som betonas mest är att en central aktör bör ansvara för all hantering av identitetshandlingar, och att det är särskilt viktigt att säkra ursprungsidentifieringen.

Näringslivets roller

Som framgått i redovisningen av brottsbalksbedrägerier spelar näringslivet en viktig roll. Ärendegranskningen visar att bedragare utnyttjar legala betalningssystem och logistik för att transportera varor. Således har näringslivet en viktig roll även som *möjliggörare*. Företag blir även *utsatta* för framför allt fakturabedrägerier, kreditbedrägerier och kortbedrägerier. Dessutom använder vissa gärningspersoner företag som *brottsverktyg* för att begå bedrägerierna. Sammantaget innebär detta att näringslivets tre roller är viktiga att förstå för att kunna förebygga bedrägerier.

Detta kapitel baseras främst på ärendegranskningen och intervjuerna, men även på tidigare studier. Här ges exempel från olika branscher på faktorer som påverkar näringslivets roller.

Näringslivets roll som möjliggörare

De system som möjliggör handel är desamma som möjliggör be-drägerier. I hur stor utsträckning bedrägerier möjliggörs avgörs exempelvis av hur stark säljkulturen är i förhållande till säkerhetskulturen. Vilken part som ersätter den ekonomiska förlusten vid ett bedrägeri är en faktor som kan påverka balansen mellan sälj- och säkerhetskultur. Slutligen beskrivs i detta avsnitt hur gråzoner inom telefonförsäljning samt bristande kontroller inom fraktkedjan kan möjliggöra bedrägerier.

Att locka bra kunder, men inte bedragare

Ett genomgående tema i intervjuerna med personer från näringslivet är utmaningen att hitta en balans mellan säkerhet (kontroll) och försäljning. Några intervjupersoner – såväl näringslivsföreträdare som gärningspersoner – menar att det går att förebygga i stort sett alla bedrägerier inom handeln, problemet är att man samtidigt avskräcker hederliga kunder.

Utgångspunkten är att de flesta kunder trots allt är hederliga, och att servicen ska vara god för dem, samtidigt som företaget inte får bli för sårbart för bedrägerier. Ett viss mått av tillit måste fin-

nas i ett gott affärsklimat, men utan att tilliten går över i naivitet, menar intervjupersoner. Som en företrädare för näringslivet uttrycker: *Det gäller att hitta balansen mellan att inte bli lurad och att göra bra affärer*.

Företrädare för näringslivet ser att höjningar av kontrollnivåer gör att gärningspersoner går till konkurrenter med lägre kontroll (jfr Brå 2011:4). Gärningspersonerna beskrivs vara bekväma i ett modus vilket gör det enklare att byta offer än att byta bransch och tillvägagångssätt (jfr Brå 2015:22). Man menar dock att även seriösa kunder går till andra försäljare vid ökade kontrollrutiner, vilket skulle leda till minskad försäljning. En säkerhetsansvarig inom telecombranschen beskriver detta resonemang:

> *Då kalkylerar ju alla med den risken; okej, hur mycket bedrägeri kan vi ha innan det är en förlustaffär. Det är bättre sälja 10 abonnemang och få ett bedrägeri än att sälja 5 abonnemang och inte ha något bedrägeri. Det är ju så de kalkylerar.*

Några intervjupersoner menar att kunden i allmänhet har förståelse för att kontroller behöver göras, och att detta till och med uppskattas av dem med ärliga avsikter. Det finns visserligen en risk för minskad försäljning vid ökad kontroll, menar en säkerhetschef inom näringslivet, men till viss del kan det också handla om en *föreställning* om att kunder byter butik – eller försäljningssajt – om kontrollrutinerna skärps. Kundens behov av snabba affärer kanske inte är så stor som näringslivet tror.

Försäljningskulturen olika stark mellan och inom företag

Inom vissa branscher tycks det finnas ett större motstånd mot höjda kontrollnivåer än inom andra. Det gäller i synnerhet inom branscher med hård konkurrens. Hög konkurrens i kombination med låg samordning av säkerhetsarbete inom branschen förefaller öka risken för att säkerhetsnivåerna blir ett konkurrensmedel.

Även *inom* ett företag varierar kontrollviljan hos chefer och säljare. Intervjupersoner inom handeln menar att kontrollen sänks när fokus ensidigt ligger på att ge kunden ett bra bemötande och god service. Denna kundfokusering kan till exempel innebära att säljaren genomför köp trots att kunden säger sig ha glömt legitimationen eller koden till sitt betalkort, menar en företrädare för näringslivet. Om den enskilde försäljaren har en provisionsbaserad lön kan det finnas än större drivkrafter att se mellan fingrarna och låta bli att göra fördjupade kontroller trots risksignaler. Så länge bedrägeriet inte upptäcks har säljaren ofta mycket att vinna på att inte kontrollera, enligt intervjupersoner. Säljaren kan hänvisa till viljan att få goda försäljningssiffror.

Inom vissa branscher har man förtydligat ansvaret för säljarna och återförsäljarna genom avtal och ekonomiska styrmedel. Provisionen betalas till exempel inte ut om ett bedrägligt köp kan härledas till säljaren, oavsett säljarens uppsåt. En intervjuperson inom handeln berättar:

Tänk dig då om du har en återförsäljare som aldrig behöver stå för några kostnader, oavsett hur fult de säljer, hur bedrägligt de säljer, eller hur dåliga de är på att ta leg och sånt där – då skulle de ju aldrig göra det. Då skulle de ju bara tjäna en jäkla massa pengar – och ju mer okontrollerade de är, desto mer kommer de att kunna sälja.

Teknisk utveckling utgör en utmaning

Särskilt handeln och betalsystemet ställs inför nya utmaningar med nya försäljningsmöjligheter som ställer krav på att utveckla anpassade säkerhetslösningar. E-handeln utvecklas snabbt, liksom möjligheten att med mobiler och surfplattor genomföra köp. Utmaningen ligger framför allt i att kontrollera att köp genomförs av rätt person med en legitim identitet eller ett legitimt betalkort.

Snabba och enkla betalningar i butik

En diskussion som tydliggör de motsatta intressena av snabba affärer och säkerhet rör genomförandet av betalningar. Att betala med kort är i dag det vanligaste betalsättet. Kortbetalningar innebär bland annat lägre kostnader och en ökad snabbhet. Det innebär att omsättningen och därmed intäkterna kan öka. Sedan kravet på chip och pinkod infördes har skimning av kort i svenska butiker minskat och till viss del flyttat till länder med lägre säkerhetskrav och till utländska e-butiker, uppger intervjupersoner från rättsväsendet. Butiker som inte har betalterminaler med chipläsare blir i allmänhet ersättningsskyldiga vid ett upptäckt bedrägeri.

Gärningspersoner som tidigare begått kortbedrägerier vittnar också om att det blivit svårare att begå sådana under de senaste åren. Kort med chip och pin är svårare att manipulera och kopiera. Förekomsten av magnetspåret på kortet innebär dock att man fortfarande kan använda detta hos vissa butiker och restauranger och därmed kringgå användning av chip och pin, menar gärningspersoner.

Vissa intervjupersoner inom näringslivet menar dock att kortbetalningar tar för lång tid. Tiden det tar att knappa in pinkoden vid ett kortköp anses stoppa upp försäljningen. I synnerhet inom branscher med högt kundtryck upplevs varje sekund vara värdefull. Därför har såväl banker som handeln ett stort intresse av att

utveckla snabbare betalsätt. Redan nu finns exempelvis lösningar för köp med faktura med sparade betaluppgifter och olika typer av betalningar som genomförs med mobiltelefoner. Dessa betalsätt förväntas bli allt vanligare (Dibs 2015).

Ett annat exempel på betalmedel som håller på att införas är så kallade kontaktlösa betalningar. Det har införts bland annat inom restaurangbranschen och matbutiker. Kortet har ett chip men det krävs ingen pinkod, utan kortet läggs direkt mot en läsare som registrerar köpet. Kontaktlösa betalningar frångår alltså de tidigare kraven, som krävde chip och pinkod för att genomföra köp. Det innebär att bedrägeririsken kan komma att öka.

En intervjuperson påpekar att handeln inte riskerar så mycket även om bedrägerierna skulle öka. Detta eftersom de branscher som hittills infört kontaktlösa kort framför allt har försäljning av konsumtionsvaror. Det innebär att riskerna för mer ekonomiskt omfattande bedrägerier är små, menar intervjupersoner inom branscher som infört betalsättet. Det huvudsakliga ersättningsansvaret vid ett bedrägeri är också bankens och systemleverantörernas, påpekar en företrädare för näringslivet. Vem som har det ekonomiska ersättningsansvaret påverkar alltså benägenheten att ta vissa risker vid införandet av nya betalsätt. Allmänhetens oro för säkerheten kring nya betalsätt är dock en faktor som hindrar utvecklingen av nya snabbare betalsätt, menar en forskare (Arvidsson 2009).

Förtroende särskilt viktigt för bankerna

Utmaningen att optimera både försäljning och säkerhet finns inom hela näringslivet. För banker och andra aktörer inom betalsystemen är den dock ännu mer tillspetsad. Har kunder inte förtroende för dessa grundläggande system drabbar det affärerna i betydligt större utsträckning än om kunder undviker en och annan butik.

Bland andra Finansinspektionen (2009) har konstaterat att kunder i vissa fall avstår från kortköp av rädsla för bedrägerier. Om kunder förlorar förtroendet för kort som betalmedel riskerar både handeln och bankerna att förlora intäkter. De har därför intresse av att stärka kundernas förtroende för och öka användningen av kortbetalningar. Det kan göras genom att minska både den faktiska och den upplevda risken för bedrägerier.

Ett sätt att minska den faktiska risken för bedrägerier är att höja kontrollnivåerna i betalsystemet. Det kan ske exempelvis genom justeringar av de system som utarbetats av banker och systemleverantörer. Banken har möjligheter att vid misstänkta transaktioner kontakta kunden och spärra kort och konto för köp och uttag. Ju högre risknivåerna skruvas upp, desto fler transaktioner

kommer också att klassas som risktransaktioner och stoppas (Goldberg och Larsson 2014). Transaktionerna riskerar därmed att dels gå långsammare, dels minska i volym, vilket bankerna och handeln av förklarliga skäl vill undvika. Kontrollnivåerna balanseras därför noggrant. Hårddraget kan man säga att bankerna hellre ersätter kunder än höjer kontrollnivån, så länge det är mer lönsamt. Att ersätta såväl brottsutsatta kunder som butiker relativt generöst, kan också skapa en positiv inställning till bankerna hos de utsatta (Goldberg och Larsson 2014).

En strategi för att minska den *upplevda* risken för bedrägerier och upprätthålla förtroendet är att inte skylta med utsattheten. Flera intervjupersoner betonar att bankerna generellt är förtegna om omfattningen av de ekonomiska förluster som bedrägerier orsakar. En gärningsperson beskriver hur en bank förnekat att de blivit bedragna på flera miljoner kronor, även när bevisning fanns i fallet. Flera intervjupersoner menar att de ekonomiska förlusterna är ett mindre problem för bankerna än risken för dålig publicitet och förtroendeförluster vid ett uppmärksammat bedrägeri.

Banker och systemleverantörer tar ofta ekonomiskt ansvar för kortbedrägerier

Eftersom ett köp kan involvera så många parter (kortinnehavare, säljföretag, kortutgivare, fraktleverantör,[76] systemleverantör, utlämningsställe[77] etc.) är det inte alltid vid första anblick uppenbart vem som ses som ansvarig och får ta den ekonomiska förlusten. När ansvaret prövas är det centrala att visa att man följt säkerhetsrutinerna. Bankerna står ofta för den ekonomiska ersättningen vid ett kortbedrägeri. Systemleverantörerna VISA och Mastercard har ett allmänt ersättningsansvar för bedrägerier förutsatt att drabbade banker, kunder och butiker följt sina säkerhetskrav.

Enligt intervjupersoner från näringslivet ger de flesta banker kortinnehavaren ansvaret att polisanmäla ett bedrägeri och kontrollerar därefter att kortinnehavaren har följt de aktsamhetskrav som banken kräver. Om ett uttag eller en betalning har gjorts med kundens kod får kunden i allmänhet stå för förlusten. Om kunden varit uppenbart försumlig med kortet kan banken också neka ersättning. Men i allmänhet ersätts den brottsutsatta individen. Detta är huvudregeln även vid andra typer av bedrägerier, något som några intervjupersoner inom handeln menar kan leda till risker för så kallad friendly fraud. Friendly fraud innebär att

[76] Med fraktleverantör menas här den som fraktar en vara från exempelvis en butik till ett ombud eller hem till kunden.

[77] Utlämningsställe definieras här som en aktör som lämnar ut paket eller brev.

en person som inte kan eller vill betala för en vara hävdar att han eller hon är utsatt för ett bedrägeri.

Den butik som drabbats av ett bedrägeri kan också ersättas av banken om butiken uppfyllt avtalade säkerhetskrav. Vissa intervjupersoner menar att detta långtgående betalningsansvar skapar incitament framför allt för banker och systemleverantörer att utveckla säkerhetssystem. Systemleverantörer har till exempel tillsammans med bankerna utvecklat olika former av övervakningssystem som registrerar och sammanställer information kring genomförda transaktioner. Uppgifterna används som underlag för att bl.a. identifiera misstänkta transaktioner (Goldberg och Larsson 2014). Privatpersoner, handeln och fraktkedjan däremot behöver ”bara” följa säkerhetsrutinerna. En intervjuperson inom näringslivet menar dock att dessa försäkringar bakas in i kortavgifterna och därmed inte kostar näringslivet alltför mycket.

Samtidigt menar flera personer att bankernas ersättningsbelopp för exempelvis kortbedrägerier har ökat och börjat bli för stora. Ett alltför generöst ersättningssystem riskerar också att överutnyttjas av kunder och andra företag, enligt intervjupersoner från näringslivet. Det kan innebära att banker på sikt kommer att kräva att kunden tar större ansvar för att hantera kort och kortuppgifter på ett säkert sätt, menar intervjupersoner. Man kan även införa ökade säkerhetskrav på andra aktörer för att sänka bankernas kostnader för bedrägerier.

Många potentiellt ansvariga inom fraktkedjan

I och med e-handelns framväxt har aktörerna i fraktkedjan fått en allt viktigare roll genom att varorna ska fraktas till kunden, ofta via ett utlämningsställe.[78] I fraktkedjan hanteras också värdehandlingar som bankkort, identitets- och avtalsdokument och postavier för uthämtning av varor. För att genomföra och fullborda bedrägerier söker därför gärningspersoner kontroll över försändelserna i postflödet. Ett vanligt sätt att komma över försändelser är, enligt flera fraktleverantörer, att helt enkelt stjäla post från brevbäraren, brevlådor eller postboxar. Det förekommer också att gärningspersoner genom adressändring dirigerar om posten till adresser som de kontrollerar.

Utlämningsställen kan också utsättas för inbrott och stöld av värdefulla leveranser. Fraktleverantörer ser exempel där gärningspersoner systematiskt beställer varor under falsk identitet till ett utlämningsställe som sedan utsätts för inbrott.

[78] Det är i regel en kiosk eller butik som har utlämning av paket. Posten har också företagscenter, som en motsvarighet till postombud för företag. För enkelhetens skull omnämns samtliga aktörer som utlämningsställen.

I andra fall hämtar gärningspersonerna ut varan på utlämningsstället. Även om personalen på utlämningsstället gör en identitetskontroll handlar en stor del av intervjumaterialet om svårigheterna att upptäcka identitetsmissbruk. Falska legitimationer beskrivs hålla hög kvalitet vilket innebär att utlämningsstället upplever att de är hänvisade till att göra en rituell okulär kontroll. Det är ofta oklart exakt vad man ska titta efter, eller vad uppgifterna på kortet ska kontrolleras mot. Situationen kan dessutom vara stressig. De anställda upplever därför att de har begränsade möjligheter att avgöra om det är rätt person som hämtar ut en försändelse.

Företrädare för fraktkedjan menar att bedrägerier kan förebyggas om aktörer i de initiala faserna av ett köp tar större ansvar för att köpet genomförs av rätt person med legitima handlingar. Butikerna bör också ta större ansvar genom att använda säkrare leveransalternativ, menar intervjupersoner. Ett exempel på åtgärder som vidtagits inom e-handeln är krav på leverans av varor till en köpares folkbokföringsadress. Företag som har infört detta har sett att åtgärden lett till att en stor del bedrägerier stoppas vid försök till brott. Andra intervjupersoner menar att folkbokföringsadresser kan innebära en falsk trygghet, eftersom de uppgifter som finns registrerade i folkbokföringsregistret inte alltid är korrekta (se mer i kapitlet Identitetsmissbruk).

När en vara hämtats ut av en bedragare kan det ekonomiska ansvaret delas mellan flera aktörer. Om det är visat att butiken gjort en bristfällig identitetskontroll ges butiken ansvaret. Annars läggs kostnaden i regel på banken, kreditgivaren eller fraktleverantören, eller delas mellan parterna beroende på avtal.

Företrädare för handeln menar att fraktleverantörerna och utlämningsställena spelar en central roll i att möjliggöra bedrägerier genom att göra otillräckliga identitetskontroller. Det splittrade ekonomiska ansvaret för bedrägerier innebär försvagade incitament för enskilda aktörer inom fraktkedjan att genomföra kontroller, menar en säkerhetschef inom näringslivet.

Kundanpassade leveranslösningar skapar risker i fraktkedjan

Allt fler e-butiker erbjuder så kallade flexibla leveranslösningar för att tillmötesgå kundernas efterfrågan på att smidigt få hem beställda varor. En del leveranslösningar har inneburit en ökad risk för bedrägerier, menar företrädare för fraktkedjan och anställda inom polisen. Det förekommer exempelvis butiker som erbjuder hemkörning av värdefulla varor som lämnas vid tomtgränsen, på trappen eller utanför dörren. Flera intervjupersoner vittnar om bristande identitetskontroll vid denna typ av utlämning.

Det förekommer också att butiker sänder värdefulla varor som brev. Det innebär ofta lägre fraktkostnader för butiken, men också lägre krav på kontroller för utlämningsstället. Legitimation behövs i allmänhet inte för att hämta ut ett brev. Om varan däremot skickas med ett rekommenderat brev innebär det större krav på utlämningsställets kontroller, och fraktleverantören står då också för ersättningen om varan försvunnit.

Bedragare utnyttjar också att företag har möjligheter att få stora leveranser utkörda till adresser där gärningspersonerna utan närmare kontroll kan kvittera ut försändelser. Ibland försöker gärningspersonerna på olika sätt ge intryck av att det är det aktuella företagets lokaler, även om så inte är fallet. Intervjupersoner från ett fraktbolag berättar om hur stora partier elektronikprodukter beställs till adresser i exempelvis ett industriområde med en lastkaj.

Telemarketing har en gråzon som utnyttjas

Flera studier konstaterar att det förekommer en problematik med både seriösa och oseriösa telemarketingbolag (se bland annat SOU 2015:77, SOU 2015:61). Det vittnas om otydligheter, bristfällig information och rena felaktigheter i de erbjudanden som även seriösa bolag erbjuder. Flera intervjupersoner beskriver att bristande tillämpning av lagar och etiska regler inom telemarketingbranschen förstärks och utnyttjas av oseriösa och kriminella bolag för att genomföra fakturabedrägerier.

Det finns en pågående diskussion om hur problemen ska hanteras. Post- och telestyrelsen (PTS) har initierat en dialog med de största teleoperatörerna för att verka för en ökad efterlevnad av reglerna. Dessutom finns ett förslag att införa ett skriftlighetskrav i distansavtalslagen (SOU 2015:61). Genom att kräva skriftliga avtal även vid telefonförsäljning skulle avtalssituationen bli tydligare. Dessa avtal föreslås dock enbart gälla privata konsumenter och inte företag. Vissa intervjupersoner inom näringslivet menar att förslaget är önskvärt, medan andra betonar att det skulle försvåra för handeln.[79]

Näringslivets roll som brottsutsatt

Eftersom en hel del av de varor och tjänster som gärningspersonerna är intresserade av finns i näringslivet förekommer företag

[79] Företagare är undantagna den ångerrätt som gäller för privatpersoner, enligt distans- och hemförsäljningslagen (2005:59). Det innebär att en företagare som påstås ha ingått ett avtal inte kan upphäva avtalet genom hänvisning till ångerrätten. Svensk Handel har tillsammans med ett antal branschaktörer tagit fram en särskild överenskommelse vid telefonförsäljning mellan näringsidkare. Enligt den har företagare ångerrätt i sju arbetsdagar.

som brottsoffer för bedrägerier. På ett generellt plan har företag betydligt större resurser än privatpersoner, vilket innebär att i synnerhet storskaliga bedrägerier riktar sig mot näringslivet.

Företag med attraktiva produkter mer utsatta

Det förekommer bedrägerier inom i stort sett alla delar av handeln. Kapitalvaror är särskilt eftertraktade därför att de i allmänhet är enklare att komma över än kontanter, men går att omvandla till kontanter, till skillnad från exempelvis konsumtionsvaror. Elektronik, mobiltelefoner och andra teknikprodukter är exempel på eftertraktade kapitalvaror. De branscher som är särskilt drabbade av bedrägerier hanterar också ofta varor med ett högt andrahandsvärde som snabbt går att sälja vidare.

Sektorer med högre förekomst av annan brottslighet är också särskilt utsatta för bedrägerier. Byggbranschen nämns av flera intervjupersoner som en sårbar bransch. Ekobrottsutredare beskriver att de ser att bedrägerier inom byggbranschen ofta kombineras med andra typer av brott, framför allt skattebrott av olika slag. Orsaker till detta är bland annat att branschen rör sig med stora mängder värdefulla kapitalvaror och att krediter på material är vanligt. Det förekommer också en hög grad av långa entreprenörskedjor inom byggbranschen, vilket är en riskfaktor för bedrägerier liksom för andra typer av brott (se till exempel Brå 2007:27, Brå 2011:7, Rönnblom, Skinnari och Korsell 2015). Skälen är att insynen minskar och att risken ökar för att man får in oseriösa företag längre ner i entreprenadleden.

Gärningspersonernas egen efterfrågan på vissa produkter kan också påverka vilka branscher som väljs ut, vilket en gärningsperson beskriver:

> *Det berodde ju på efterfrågan – vem behövde vad. Jo, en behövde en dubbelsäng. Ja, men då fick det ju bli [specifik möbelaffär], för där visste vi att de var ganska trevliga och lättpratade. En behövde ett guldarmband, ja då blev det [specifik guldsmed]. Så det berodde på efterfrågan, vad som behövdes få fram.*

Fakturabedragare gör i allmänhet sina utskick i stor skala. Till viss del sker utskicken i form av pappersfakturor, vilket innebär kostnader för försändelserna. Det innebär att bedragarna har anledning att försöka undkomma kostnaderna. Det kan exempelvis ske genom medhjälpare på fraktföretagen. Ytterligare en variant är att portokostnaden skjuts över på ett kapat bolag, som senare försätts i konkurs. På så sätt kan skulden förskjutas tillbaka till fraktleverantören. Vaksamheten och kontrollen inom branschen har dock stärkts, menar ansvariga inom fraktkedjan. Det försvårar utnyttjandet av fraktleverantörer, åtminstone inom Sverige.

Decentralisering kan innebära ökad sårbarhet för bedrägeri

Inom decentraliserade branscher som byggbranschen har de enskilda cheferna ofta större mandat att själva göra affärer inom vissa beloppsmässiga ramar. Det förekommer att gärningspersoner känner till beloppsgränserna för enskilda chefers attesträtt och lägger fakturabeloppen strax under dessa, för att försöka undkomma förhöjd kontroll, enligt en intervjuperson i byggbranschen.

Det finns exempel i intervjuerna på hur företag har gjort sig mindre sårbara för fakturabedrägerier. Exempelvis har kedjor inom handeln tagit bort möjligheten för butikschefer att själva teckna större avtal eller göra större inköp från leverantörer. Genom att lyfta mandatnivån högre upp i organisationen har antalet drabbade butiker minskat, menar företrädare för handeln. Det blir svårare för bedragare att ta kontakt med huvudkontoret än med lokala handlare. När inköpen är centraliserade ökar också möjligheten att identifiera bluffbolag och bluffakturor, eftersom företagen får en helhetssyn.

Småföretag kan också vara mer sårbara för fakturabedrägerier, enligt intervjupersoner. Dessa företag har i allmänhet inte samma administrativa resurser för att upptäcka och bestrida bluffakturor, som större bolag har. Intervjupersoner nämner flera näringar, exempelvis jord- och skogsbruk, med en stor andel småföretag som kan bestå av en eller några få personer som äger och arbetar i bolaget. Det innebär i allmänhet en hög arbetsbelastning, vilket ökar risken för att fakturor betalas av misstag, menar intervjupersoner från branschen. I synnerhet äldre personer med en passiv skogs- eller näringsverksamhet uppges vara drabbade.

Företagens sårbarhet för bedräglig försäljning

I denna undersöknings ärendegranskning var över hälften av målsägarna företag vid fakturabedrägerier. Ett annat mått är att vart tredje tillfrågat företag under det senaste året fått en eller flera bluffakturor och vart femte har fått en bedräglig faktura efter en kontakt (SOU 2015:77). Många fall av dessa fakturabedrägerier har inletts med en kontakt med en telefonförsäljare. Företagare som kontaktats av en telefonförsäljare innan en faktura skickas betalar i större utsträckning fakturor jämfört med andra (ibid). Enligt intervjupersoner från näringslivet har telefonförsäljarna för bluffbolagen ofta en hotfull och vilseledande försäljningsstil. I Brås intervjuer och en statlig utredning framkommer att äldre och personer som inte behärskar svenska är särskilt utsatta vid telefonförsäljning (SOU 2015:61).

Anmälningsbenägenheten vid fakturabedrägerier är generellt låg (SOU 2015:77). Att drabbade företag inte alltid gör polisanmälan uppges ha flera orsaker. Det kan handla om att företaget inte insett att det är fråga om en bluffaktura, och därför betalar av misstag (ibid). En intervjuperson som begått fakturabedrägerier beskriver hur man kalkylerar med att företagare betalar av misstag, och därför skickar ut ett stort antal fakturor:

> *Oftast vet de att väldigt många företagare inte är riktigt, att de har koll på – ”jamen, har jag betalt det här för två veckor sen? Men nu har jag fått en faktura till?” Så man betalar. Tänk alltså, om du skickar 100 stycken, 100 företag. Och 10 stycken betalar. Du har ändå gjort pengar!*

I andra fall betalar företagare fakturorna trots medvetenhet om att det är en bedräglig faktura, eftersom det upplevs vara komplicerat att bestrida den. Omkring en femtedel av företagen uppger att de saknar tillräcklig kunskap om hur man bemöter en falsk faktura, och de vet inte heller vart de kan vända sig för att få hjälp (ibid). Företagare tycks vara mer benägna att betala om det handlar om låga belopp. Flera intervjupersoner menar att beloppen ofta ligger på en nivå strax under vad det kostar att anlita en jurist. Vissa gärningspersoner kalkylerar med detta och anpassar fakturabeloppen. Trots att det ofta rör sig om mindre summor kan de bli ekonomiskt kännbara för företag med liten omsättning, enligt företrädare för näringslivet.

Även om det är ovanligt att en bluffaktura verkligen leder till en ansökan om betalningsföreläggande, betalas fakturor av rädsla för att få en betalningsanmärkning eller ett betalningsföreläggande. Om det rör ett aktiebolag får redan en ansökan om betalningsföreläggande som har registrerats hos Kronofogden lämnas till t.ex. ett kreditupplysningsföretag. Det innebär att det finns en reell risk för sänkt kreditvärdighet för företaget. Om bluffbolaget finns med på Svensk Handels varningslista blockeras det dock av kreditupplysningsföretagen, och företaget får ingen anmärkning. Saknas företaget på listan kan företagaren i stället meddela Kronofogden, och ansökan tas bort. Denna process kräver kunskap och tid, vilket inte alla företag har, i synnerhet inte småföretagare, menar intervjupersoner.

Kreditbranschen utsätts för bedrägerier

I kreditbranschen inkluderas kreditgivare och kreditupplysningsbolag. Kreditgivare är en aktör som lånar ut pengar. Det kan röra sig om butiker som erbjuder kreditköp, banker och andra långivare. Dessa drabbas av en hel del bedrägerier.

Kreditupplysningsföretag är en aktör som tillhandahåller information om exempelvis inkomster, skulder och betalningsanmärk-

ningar inför ett kreditköp. Uppgifterna för företag kan också visa styrelseledamöter i bolag och ekonomiska förhållanden. Kreditupplysningsföretagen hämtar bland annat uppgifter från Skatteverket, Kronofogden, Bolagsverket och Statistiska centralbyrån. Enligt lagkrav måste samtliga banker och kreditbolag göra en kreditupplysning av kunden vid en ansökan om kreditköp eller lån. De flesta kreditupplysningar lämnas genom att kreditgivaren har en direktuppkoppling mot kreditupplysningsföretagets register. Om riskerna bedöms vara små godkänns ansökan automatiskt av kreditgivaren, vid högre risker kan fördjupade kontroller krävas.

Kvaliteten på underlagen varierar dock. Några intervjuade gärningspersoner är av uppfattningen att vissa kreditupplysningsbolag tillhandahåller underlag som är alldeles för osäkra. Det förekommer därför att gärningspersoner väljer butiker som anlitar ett kreditupplysningsbolag med lägre kvalitet på upplysningen. En gärningsperson förklarar:

> *Använder de [företag A] är det inte någon idé. Hade jag haft bolag i dag, då hade jag tagit all kreditupplysning via [företag A], inte de här jävla [företag B]. De är för färska än så länge.*

Det förekommer också att de uppgifter som ligger till grund för information från kreditupplysningsbolagen manipuleras. Det handlar exempelvis om felaktiga identitetsuppgifter, inkomster och omsättning, vilket ger en högre kreditvärdighet (se mer nedan om rollen som brottsverktyg, samt kapitel om Identitetsmissbruk).

Möjligheten att kontrollera nya bolag är särskilt begränsad eftersom den information som kreditupplysningsbolagen hämtar från bland andra Bolagsverket är knapphändig. För nystartade företag skulle ytterligare uppgifter behöva inhämtas samt kontroller göras, vilket ofta inte sker, enligt företrädare för näringslivet. I de flesta branscher finns emellertid gränser för hur stora krediter som kan ges till nystartade företag. Kreditgivare kan ha begränsningar i belopp eller i antal varor som kan inhandlas på kredit. Riskerna bedöms i allmänhet större ju yngre ett företag är. Krediter kan också nekas helt till nystartade bolag, vilket förekommer inom vissa branscher.

Intervjupersoner från kreditbranschen noterar att vissa gärningspersoner har kännedom om rutiner och är skickliga på att anpassa upplägg efter kreditkontrollerna. Det förekommer att gärningspersoner tycks känna till hur hög kreditbeviljningsrätt en säljare eller handläggare har. I synnerhet när företag används i upplägget involverar det gärningspersoner som hittat kryphål i system och rutiner, allt för att undvika fördjupade kontroller innan kreditköp medges.

Lån på distans – ökad risk för bedrägerier?

Kreditlånebranschen erbjuder kunder möjligheten att teckna lån på distans, som sms-lån, blancolån eller snabblån. Lån på distans upplevs som mindre riskfyllt av gärningspersonerna, vilket enligt en intervjuperson gör att de söker sig till kreditlånebranschen. En kreditchef inom branschen tycker sig se hur vissa anpassar och utvecklar upplägg i takt med branschens kontrollarbete. Exempelvis har gärningspersoner slutat att söka maxbelopp och ansöker nu om lägre belopp. Detta sker troligen för att försöka undkomma fördjupade kontroller.

Företrädare för näringslivet menar att det finns en naivitet i kreditbranschen inför den brottslighet som existerar, vilket leder till att riskerna underskattas. Andra menar att kontrollen inom kreditlånebranschen trots allt är högre än vid kreditköp inom handeln. En kreditchef säger:

> *Man gör ju inga stora penningaffärer utan att träffa sin kund. Du lånar ju inte 10 miljoner av banken utan att banken ens träffat dig och gått igenom och så. Men däremot, det här med varor och tjänster i form av it-utrustning, bilar, maskiner, såna saker.*

Snabba sms-lån tycks minska

Snabblån via sms har varit en annan variant av kreditbedrägerier, som dock tycks minska under senare år, särskilt efter Sveriges införande av EU:s konsumentkreditdirektiv.[80] Snabblånen har tidigare kunnat tecknas bland vissa mindre aktörer på marknaden utan större säkerhetskrav. Sedan några år tillbaka sker dock en mer noggrann kreditprövningsprocess hos de allra flesta snabblånebolag, och bolagen tillämpar olika metoder för att verifiera kundernas identitet.[81] När sms-lån lanserades 2006 började tjänsten snabbt utnyttjas av bedragare. Det infördes skärpta kontroller och i dag måste kunden ofta använda någon form av e-legitimation, t.ex. BankID, för att registrera ett konto hos låneföretaget. De kommersiella bankerna som ställer ut e-legitimation har dock, enligt uppgift från företrädare för snabblånebranschen, hittills nekat direkt tillgång till sådan licens för bolag som erbjuder snabblån. Dessa bolag har därför varit tvingade att nyttja andra leverantörer av s.k. stark elektronisk identifiering.[82]

Förutsatt att e-legitimation används och tillhör rätt person är det i dag svårt att teckna sms-lån i någon annans namn. Enligt en branschorganisation har bedrägerier i samband med snabblån på

[80] 2008 (2008/48), implementerat genom nya Konsumentkreditlagen 2010/2011.

[81] Att kontrollera kundens identitet är ett krav i linje med lagen om åtgärder mot penningtvätt (2009:62).

[82] I de fall där kunden eller kreditgivaren inte har tillgång till elektronisk identifiering verifieras identiteten på den som ansöker om lånet genom verifierade identitetshandlingar eller i vissa fall personkonto.

senare tid begränsat sig nästan uteslutande till de fall där gärningspersonen är någon närstående som haft tillgång till de annars säkra uppgifterna. Som en representant för kreditbranschen uttrycker det: *Det är i dag svårare att få ett snabblån än att köpa en tv på kredit i en stor elektronikkedja*.

Samtidigt finns det fortfarande en del luckor i snabblånesystemet; även om det inte är vanligt tycks det i vissa fall räcka att man skickar in ett bildmeddelande på en identitetshandling för att lånet ska godkännas – något som framgått i de domar som Brå har granskat. Ett steg mot generellt säkrare lån är ett nytt licenskrav som infördes sommaren 2014[83] och som innebär att samtliga långivare numera måste ha en licens från Finansinspektionen. Finansinspektionens tillsyn gör att alla lån kan granskas, och kreditbolagen kan förlora sin licens om brister upptäcks. Detta har bland annat lett till bättre säkerhetskontroller hos kreditbolagen.

Handeln har kluven inställning till kontroller vid kreditköp

Butiker verkar som kreditgivare genom att erbjuda olika former av avbetalningar av köpet i efterhand. Exempelvis är erbjudanden om att ”få” en mobiltelefon i butiken om man tecknar ett abonnemang en form av kreditköp. Mobilen bekostas genom avgifter kopplade till abonnemanget, och återförsäljarna ersätts av operatören, som verkar som kreditgivare. Vid sådana kreditköp gör handeln identitetskontroller och kreditprövning, som beskrivits ovan. Det förekommer dock att butiker godkänner kreditansökningar trots att kreditupplysningen signalerar om risker som åtminstone borde leda till en manuell kontroll. Till exempel godkänner man krediter trots varningssignaler om att personen eller företaget har många kreditupplysningar på sig under kort tid, enligt intervjupersoner.

Flera gärningspersoner menar också att vissa butiker med kreditgivning är alldeles för dåliga på att göra fördjupade kontroller, i synnerhet när företag genomför köpen. Flera gärningspersoner som begått kreditbedrägerier beskriver att stora delar av handeln har låga kontrollnivåer, vilket gör det möjligt att bara ”gå in och hämta saker”. En gärningsperson beskriver hur denne med ett företag med kreditvärdighet på 50 000 kronor kunde handla på kredit till ett värde av åtskilliga miljoner. En annan gärningsperson berättar:

> *Gud, ja, oj oj oj. Det är så enkelt. Du kan ju föreställa dig hur det känns att kunna gå in på (elektronikkedja) och bara peka på saker och personalen bär ut det i bilen.*

[83] Lagen (2014:275) om viss verksamhet med konsumentkrediter.

Bristande resurser och hög arbetsbelastning beskrivs påverka kontrollnivån negativt, i synnerhet i kombination med en stark säljkultur. Om försäljningssituationen är stressig finns en särskild press på säljaren att genomföra köpen snabbt. Det kan leda till att rutiner inte följs och att man exempelvis litar alltför mycket på köparens uppträdande i en säljsituation, menar intervjupersoner inom näringslivet.

Vissa företag gör fördjupade kontroller

Som tidigare nämnts i detta kapitel ökar intresset för kontroll om bedrägeriförlusterna blir kostsamma. En säkerhetschef beskriver hur man höjde kontrollnivåerna i takt med att bedrägerivolymerna ökade. Fördjupade kontroller av identitetshandlingar infördes bland annat, med följd att kunden fick vänta något längre.

Vissa intervjupersoner beskriver butiker som faktiskt genomför fördjupade manuella kontroller vid höga belopp och vid vissa risksignaler. Andra butiker har skärpt sina kontrollrutiner, exempelvis genom att kräva att en mindre summa dras från ett kontokort vid kreditköp. På så sätt ökar svårigheten för gärningspersonen, eftersom den behöver ha tillgång till både ett falskt kort och en identitetshandling för att kunna utföra ett kreditbedrägeri. Åtgärden minskade bedrägerierna drastiskt men upplevdes också ha negativa konsekvenser för försäljningen, menar ansvariga inom branschen.

En insider kan öka kostnaderna för arbetsgivaren

I flera intervjuer med personer inom näringslivet lyfts problematiken med att drabbas av insiderbrott i företaget. Med insider avses en anställd som hjälper gärningspersoner på utsidan. Medhjälparen kan till exempel vara en försäljare i en butikskedja eller en person på ett kreditgivande bolag. Hjälpen handlar dels om råd om var säkerhetsbristerna finns, dels om att det medges lån eller köp trots att det handlar om bedrägerier. Det senare blir särskilt enkelt att genomföra inom företag med en stark försäljningskultur. Om medhjälparen ertappas med att ha släppt igenom ett bedrägligt köp, hänvisar insidern till att den velat sälja så mycket som möjligt. Insidern kan också skylla på att gärningspersonen hade falska kort- eller identitetsuppgifter, och på så sätt komma undan anklagelser om delaktighet, menar gärningspersoner.

Näringslivets roll som brottsverktyg

Gärningspersonerna kan även använda näringslivet genom att de begår bedrägerier med hjälp av företag. Företagen kan befinna sig i olika faser, som under uppstart av verksamheten, efter år av verksamhet och vid konkurs. Det förekommer att företagen

används för olika typer av bedrägerier, eller i kombination med andra typer av ekonomisk brottslighet som skattebrott, penningtvätt och bokföringsbrott (se till exempel Brå 2016:7, Brå 2015:8, Brå 2015:22, NUC 2015a).

Företag används vid många typer av bedrägerier

Vid vissa bedrägerier är företag en förutsättning, som vid vissa fakturabedrägerier och välfärdsbedrägerier. Vid andra bedrägerityper, ofta olika typer av kreditbedrägerier, möjliggör företaget mer storskaliga bedrägerier samtidigt som den individuella risken för gärningspersonen minskar när han eller hon blir mer dold bakom företaget (se även Brå 2016:7). Detta förstärks ofta genom att målvakter sätts i styrelsen och figurerar i officiella dokument i stället för de egentliga gärningspersonerna. Till detta kommer att företaget kan utgöra en legitim front för att minska upptäcktsrisken eller öka personers benägenhet att betala exempelvis bluffakturor. Exempel finns i materialet på att man väljer ett företagsnamn som liknar ett legitimt företags, för att låna av detta företags ”förtroendekapital”.

Förekomsten av ett företag ger också ökade möjligheter att legitimera och tvätta brottsvinster och kan innebära status för gärningspersonen (Brå 2007:4, Brå 2015:22, Rönnblom, Skinnari och Korsell 2015).

För att genomföra bedrägerier med företag krävs i regel god kunskap om exempelvis företagande och bolagsjuridik. Om organisatörerna skulle sakna den kunskap som krävs använder de medhjälpare med sådan kompetens (se mer i kapitlet om Brottsutsatta och gärningspersoner).

Både aktiebolag och föreningar används

Aktiebolag är en attraktiv organiseringsform av olika skäl. Ett aktiebolag innebär att bolaget kan teckna avtal, ha anställda och äga, samtidigt som ägaren inte blir personligt ansvarig för företagets skulder. Den personliga risken överförs därmed på bolaget.

Polisanställda och säkerhetsansvariga i näringslivet ser en trend i en ökad användning av föreningar och stiftelser i kriminella syften. Insynen och kontrollmöjligheterna i dessa organisationsformer är lägre jämfört med i aktiebolag.

Föreningar tycks också vara attraktiva som brottsverktyg eftersom de kan omsätta stora belopp. Gärningspersonernas främsta intresse av att ha kontroll över en förening är att få tillgång till kontona och via exempelvis bedrägerier och osanna fakturor och annat bokföringsunderlag överföra föreningens pengar till egna konton. En särskild typ är bedrägerier med bostadsrättsförening-

ar som verktyg. Exempel på dessa beskrivs både av två intervjupersoner och i tidigare studier (Rönnblom, Skinnari och Korsell 2015, Brå 2011:7). Gärningspersonerna har genom att ingå eller kapa styrelsen försökt ta lån på bostadsrätter som inte finns i verkligheten. Dessa fiktiva lägenheter har i vissa fall belånats och genererat stora belopp.

Starta upp ett nytt eller köpa ett befintligt företag

Företags attraktivitet som brottsverktyg har skapat en särskild marknad för företag som kan användas för brottsliga syften. Intervjupersoner berättar hur formella och informella bolagsförmedlare startar eller köper upp företag och arbetar upp en god kreditvärdighet på legal eller illegal väg, för att sedan sälja dem vidare som brottsverktyg. Dessa bolagsförmedlare har i allmänhet god bolagskunskap och är specialiserade på att sälja företag i kriminella syften. Bolagsförmedlarna sägs kunna skräddarsy företag som passar ett tänkt brottsupplägg. Genom att gärningspersonen förklarar ett tänkt upplägg kan skickliga förmedlare skaffa fram ett passande bolag. Ett företag kan exempelvis beställas med en viss kreditvärdighet, inom en viss bransch och på en viss ort. I vissa ”paket” ingår målvakt, liksom ett konto och kontakter mot Skatteverket och Bolagsverket. Målvakten är i vissa fall den före detta ägaren som på olika sätt påverkas att sitta kvar i bolaget.

Insider inom olika branscher kan också hjälpa till att förmedla bolag. Bokförare eller revisorer som arbetar med bolag som är nära konkurs kan sälja bolagen med god förtjänst till gärningspersoner.

Enligt flera intervjupersoner är legala annonssidor en vanlig marknadsplats inte bara för legala företag utan även för företag som brottsverktyg (se även Brå 2016:7). En gärningsperson beskriver:

> *Ja, gå in på bolag köpes på [annonssida]. Du kollar där och ser hur många som helst.(…) Så står det ”bolag med hög kreditvärdighet”. Är du seriös behöver du inte ha ett sånt bolag. Det kan du bygga upp själv. Det är bara om du ska fuska med någonting. De sitter bara och säljer bolag för att folk ska ta ut på kredit.*

Köp av företag kan också ske som överlåtelser utan säljarens medvetenhet om syftet med köpet. Det förekommer att gärningspersoner och bolagsförmedlare ger sken av att vara en seriös företagare som vill fortsätta driva ett företag vidare. En intervjuad gärningsperson berättar att man i kontakt med säljaren ofta ljuger om planer och hur företaget ska drivas, för att inte väcka misstankar.

Lätt att starta nytt bolag

Rutinerna för att starta företag har delvis förenklats de senaste åren. Av betydelse för bedrägerierna är att aktiekapitalet för aktiebolag halverades till 50 000 kronor år 2010 och att revisorsplikten för mindre bolag avskaffades år 2011 (Brå 2016:7). Gärningspersoner menar att detta har gjort det enklare att starta ett bolag i kriminella syften.

För att starta ett aktiebolag krävs också en styrelse med en eller flera styrelseledamöter. Styrelseledamöterna får inte vara i konkurs eller ha näringsförbud. Gärningspersoner menar att det är enkelt att starta bolag och registrera styrelsemedlemmar under falskt namn. En anställd på Ekobrottsmyndigheten bekräftar att de ser att falska identitetshandlingar används vid bolagsstarter och att dåliga kopior av körkort eller pass ges in till myndigheterna. En gärningsperson som begått bedrägerier med företag berättar:

> *Vi säger att du går ner på Solvalla camping, där det bor en massa hemlösa. Du har öppnat ett företag och så vill du ha med dig de här personerna i ditt företag, tio stycken säger vi, med namn och adress. De får inte ha några skatteskulder eller något på Kronofogden. Och det är väl inte så svårt, en hemlös har väl inga skulder, de har ju ingen inkomst, de är ju skönstaxerade. Och så ställer du in de här tjugofem personerna, eller tio personerna, på ditt företag, och öppnar ett företag i deras namn.*

Kapa eller tvinga företag att medverka

Enligt intervjupersoner är olika former av illegala övertaganden av bolag mindre vanliga tillvägagångssätt än de legala som beskrivits ovan. De illegala metoderna är generellt mer riskfyllda och osäkra. De mer organiserade gärningspersonerna använder därför ofta legala vägar för att komma över bolag (jfr Brå 2016:7).

En illegal metod är att kapa ett företags identitet, exempelvis genom att kapa en styrelseledamots identitet. Styrelseledamoten kan vara ovetande om identitetsmissbruket tills signaler kommer om att köp gjorts i företagets namn eller att styrelseändringar registrerats hos Bolagsverket.

Överlåtelsen av ett företag fullbordas både vid legala och illegala styrelsebyten genom en ändringsanmälan till Bolagsverket. Styrelseändringar börjar gälla direkt när ändringsanmälan har inkommit till Bolagsverket, och gärningspersonerna har därefter tillträde till att använda företaget. Bolagsverket har en tjänst där ett företag kan få automatiska e-postmeddelanden vid ändringar i företaget. Informationen skickas dock inte ut förrän diarieföring-

en är gjord, vilket i allmänhet tar en vecka. Den tidigare ägarens uppgifter står under denna tid i alla register. Denna tidslucka utnyttjar vissa gärningspersoner för att begå kreditbedrägerier, menar flera intervjupersoner från näringslivet.

Vissa gärningspersoner försöker förlänga denna tidsperiod på olika sätt, så att Bolagsverket måste begära komplettering innan de kan diarieföra styrelsebytet. Det förekommer att gärningspersoner som kapat en styrelsemedlems identitet även kapat e-postadressen, så att ändringsmejlet inte når styrelsen. En gärningsperson menar att skriftlig information borde skickas ut till folkbokföringsadressen med krav på bekräftelse av styrelseändringen innan bolagsändringar träder i kraft.

Det förekommer också att företag övertas under hot eller utpressning. Intervjupersoner från kreditbranschen beskriver hur styrelser genom hot tvingas gå med på en försäljning eller att överlåta styrelseplatser. Ägaren kan också under hot tvingas sälja företaget och sitta kvar i företaget som målvakt.

Gärningspersoner söker företag med eller skapar hög kreditvärdighet

Företag inom i stort sett alla branscher kan användas för att begå bedrägerier, så länge de har god kreditvärdighet, menar gärningspersoner och andra intervjupersoner. I synnerhet är företag inom kapitalintensiva branscher med praxis av stora kreditköp attraktiva som brottsverktyg. Gärningspersoner söker också företag som befinner sig i faser som motiverar stora köp – som uppstart eller expansionsfas.

Den redan nämnda byggbranschen, men även åkeribranschen, är exempel på utsatta branscher. Även grossistbranschen beskrivs av en gärningsperson som attraktiv eftersom man då kan ”köpa in lite av allt” utan att väcka misstankar.

Andra branscher är inkasso och factoring,[84] enligt intervjupersoner från rättsväsendet. Factoringbolag kan användas på olika sätt även i annan brottslig verksamhet, exempelvis för skattebrott, penningtvätt och för att skapa fiktiva inkomster. Inkassobolagen spelar en så viktig roll att de beskrivs separat nedan.

Blåsa upp kreditvärdighet för att öka vinning kräver tålamod

Avancerade och omfattande bedrägerier kräver mer planering, kunskap och organisering från gärningspersonerna. När företaget saknar kreditvärdighet förekommer att gärningspersoner bygger upp en sådan under en kortare eller längre tid innan bedrägeriet

[84] Ett factoringföretag belånar eller köper fakturor. Kunden får, mot en avgift, snabbare in pengar genom att sälja sin fordran till factoringbolaget.

genomförs. Det kan ske på legal, delvis legal eller illegal väg. En metod är att driva viss legal verksamhet i bolaget parallellt med brottsligheten, enligt en ekobrottsutredare.

Flera intervjupersoner från rättsväsendet beskriver hur gärningspersoner ofta bygger upp kreditvärdigheten under lång tid, vilket gör det svårt att upptäcka det kriminella syftet. En gärningsperson som sysslat med kreditbedrägerier förklarar hur planerings- och uppbyggnadsfasen kan vara från några månader upp till flera år för att skapa ett legitimt företag med hög kreditvärdighet:

> *Det här gör du inte över en natt. Utan det här är planering på mellan 3 och 6 månader eller ett år. Det beror på hur länge du vill vänta och hur stort du tänker (…) Jag menar, ska du försöka få ut så mycket pengar som möjligt i kontanter gäller det att du är iskall. Då är det att vänta ut ett år eller så.*

En annan gärningsperson beskriver hur denne tillsammans med medhjälpare köpte företag och drev legal verksamhet inom grossistbranschen i cirka ett år innan bedrägeriet inleddes. Under uppbyggnaden sköttes företagets ekonomi exemplariskt för att skapa en klanderfri legitim fasad. Fakturor betalades i tid och goda kundrelationer skapades. Flera gärningspersoner menar att tålamod, planeringsförmåga och långsiktighet är centrala komponenter om målet är att komma över kontanter och värdefulla kapitalvaror.

Manipulera kreditvärdighet

Manipulerade årsredovisningar är ett sätt att höja kreditvärdigheten. Slopad revisorsplikt för mindre bolag, som gäller sedan 2011, har underlättat möjligheten att manipulera bokslut, enligt gärningspersoner och andra intervjupersoner.[85] Intervjupersoner beskriver hur medhjälpare på kreditbolag, redovisnings-, revisions-, advokat- och bokföringsbyråer samt konkursförvaltare hjälper till att manipulera årsredovisningar och andra dokument.

Ett annat sätt att höja företagets omsättning är att göra fiktiva affärer mellan egna eller medhjälpares bolag. Penningströmmar av till synes legala affärer mellan dessa bolag kan också vara ett led i att tvätta och dölja brottsvinster. En gärningsperson berättar:

> *Första året omsatte de 100 000, nästa år 1 miljon, då blir det en höjning som är rätt stor. Då blir det höga kreditvärdigheter på en gång. Det trixar man med ingående fakturor och grejer. Det är så enkelt, väldigt enkelt.*

Fiktiva anställningar används också för att manipulera kreditvärdighet. En utredare vid Ekobrottsmyndigheten beskriver hur

[85] Bolag med högst tre anställda, en omsättning under tre miljoner och tillgångar till ett värde av högst 1,5 miljoner slipper numera revisor.

gärningspersoner skaffar kontroll över ett antal identiteter, som ges fiktiva anställningar och därefter personnummer och folkbokföringsadresser. Kontrolluppgifter skickas in till Skatteverket, men arbetsgivaravgifter och skatter betalas aldrig. Innan Skatteverket får in uppgifter om inbetalade skatter kan dessa uppgifter användas som underlag för att handla på kredit eller ta kreditlån.

Agera snabbt när kreditbedrägeriet genomförs

När bedrägeriet väl påbörjas har gärningspersonerna en begränsad tid på sig innan bedrägeriet upptäcks. Genomförandet av ett kreditbedrägeri sker därför ofta snabbt, inom ett par dagar eller veckor. Gärningspersonerna vill dels agera innan de obetalda fakturorna uppmärksammas, dels innan varningssignaler om kreditupplysningar och styrelsebyten når företag och kreditgivare. Det finns ofta en noggrann, dokumenterad plan för i vilken ordning varor och kontanter ska hämtas ut.

En strävan efter att likna legitima företag

Gärningspersonerna med företag försöker i varierande utsträckning få dem att likna legitima företag. Några intervjupersoner uttrycker viss oro för hur gärningspersonerna kommer att använda sin företagskunskap i framtiden. Gärningspersoner som tidigare använde bolag för fakturabedrägerier har alltmer övergått till kreditbedrägerier i takt med att medvetenheten om och åtgärderna mot fakturabedrägerier ökat, enligt intervjupersoner. Andra gärningspersoner beskrivs förädla sitt upplägg med företag, genom att utnyttja gråzoner mellan legala och illegala affärer.

Inkassobolag ger legitimitet

Vid exempelvis fakturabedrägerier används inkassoverksamheter – som till och med kan tillhöra gärningspersonerna själva. För att bedriva inkassoverksamhet krävs inget tillstånd för ett företags egna fordringar. Begreppet inkasso är inte heller rättsligt skyddat vilket gör att det kan användas även av oseriösa aktörer (SOU 2015:77). Det innebär att gärningspersonerna kan skaffa kontroll över hela bedrägerikedjan, från fakturautskick till Kronofogden, menar intervjupersoner inom rättsväsendet.

Intervjupersoner berättar att de bedrägliga fakturaföretagen i många fall *hotat* de drabbade med inkassobolag eller Kronofogden, för att skrämma dem att betala. Både Brås intervjupersoner och en tidigare utredning menar, som tidigare nämnts, att det emellertid är relativt ovanligt att fakturabedragarna faktiskt använder Kronofogden eller tingsrätten för att få in pengarna (SOU 2015:77, Brå 2016:7).

Inkassobolag används även för att legitimera företaget. Att snabbt skicka fakturor till Kronofogden kan ge sken av och förstärka bilden av ett seriöst bolag, menar intervjupersoner inom näringslivet.

Erbjudanden i stället för bluffakturor

Flera intervjupersoner från rättsväsendet beskriver hur tillvägagångssättet vid fakturabedrägerier har förändrats mot att i högre grad baseras på ”erbjudanden” med finstilta villkor. De utformas precis så vilseledande att folk går på dem, men inte så vilseledande att det går att fälla i rätten, menar en person från näringslivet. Bedrägeriet kan därför komma att betraktas som en civilrättslig tvist snarare än ett straffrättsligt bedrägeri. Det förekommer att juridiskt kunniga personer involveras för att formulera villkoren. De beskrivs av intervjupersoner från näringslivet som skickliga, med stor juridisk kunskap och förmåga att utnyttja gråzoner, vilket gör det svårt för drabbade personer att bestrida.

Företagen har ofta en hemsida med en till synes seriös vara eller tjänst som erbjuds. Genom det hoppas gärningspersonerna att sannolikheten ökar för att företagen ska tacka ja till erbjudandet, och sedan uppfatta att de ”gjort en dålig affär” snarare än blivit bedragna. Det kan bidra till att man hellre betalar fakturan än bestrider den, menar en säkerhetschef inom näringslivet:

> *De här bolagen är så skickliga och befinner sig i gråzonen. Det kanske inte ens är uppenbart att man blivit lurad. Man tänker mer en civilrättslig tvist. Att man ingått ett dåligt avtal och varit klantig, naiv och sådär... Det finns ett väldigt tydligt upplägg tänker jag, från bolagens sida ... När de är så skickliga på att framställa det hela som ett legitimt bolag.*

Minska risk för upptäckt efter brottet

Efter att bedrägeriet är fullbordat använder gärningspersonerna olika strategier för att minska riskerna för att åka fast. Komplexa bolagsstrukturer används för att försvåra brottsutredningar. Bolagen försätts ofta i konkurs, eller styrelsen byts ut efter kort tid (Brå 2016:7, Brå 2011:7, Brå 2015:22). Nya bolag startas därefter upp under nya namn av samma gärningspersoner. Genom användning av målvaktsbolag, factoringbolag och flera egna bolag blir det svårare att koppla samman transaktioner, bolag och personer. I synnerhet när internationella bolag används blir brottsvinsterna svåra att spåra, menar utredare på Ekobrottsmyndigheten (jfr Brå 2011:7).

De utbetalande myndigheterna och organisationerna

En förutsättning för att bidragsbrott och välfärdsbedrägerier ska komma till rättsväsendets kännedom är att de utbetalande aktörerna upptäcker och anmäler. De utbetalande myndigheternas och organisationernas egen kapacitet att upptäcka mer kvalificerad brottslighet har ökat, men hur kommer det sig och vad får det för effekt?

Utbetalande myndigheter med servicekrav

Flera intervjupersoner och referensgruppsmedlemmar ger uttryck för att de utbetalande myndigheterna och organisationerna har alltför höga servicekrav och att det medför att kontrollerna får stå tillbaka. Fokus ligger på att betala ut ersättning så snabbt som möjligt, inte på att kritiskt granska underlaget. Särskilt poliser och åklagare kan vara kritiska, inte mot enskilda handläggare på de utbetalande myndigheterna – men mot att myndigheterna och organisationerna inte prioriterar frågan. Liknande resonemang finns i flera tidigare rapporter och utredningar (Brå 2015:8, FUT-delegationen 2008, NUC 2015a, jfr Riksrevisionen 2011).

En förklaring till detta är att perspektiven är olika: Rättsväsendet ser facit, när det är hyfsat tydligt att felaktiga utbetalningar har skett och pusslet om hur detta gått till redan lagts av kontrollutredare eller motsvarande på de utbetalande organisationerna. Rättsväsendet ser inte heller alla de ärenden där den sökande har lämnat korrekta uppgifter och inga misstankar uppstått. Mot den bakgrunden kan det vara lätt att vara kritisk. Men hur ser bilden ut från de utbetalande aktörernas horisont?

Kontroll ett relativt nytt område

När man – som i ärendegranskningen – ser ärenden med miljonbelopp i felaktigt utbetalade medel från välfärden är det lätt

att dra slutsatsen att de utbetalande myndigheterna brister i sitt kontrollarbete. För att få lite perspektiv är det dock viktigt att minnas att det är en rätt ny historia att över huvud taget tala om felaktiga utbetalningar och kontrollverksamhet (Korsell, Hagstedt och Skinnari 2008). Denna förändrade syn illustreras inte minst genom en mängd statliga utredningar som utmynnat i förbättrade förutsättningar för kontrollarbete överlag och särskild lagstiftning som bidragsbrottslagen, lagen om underrättelseskyldighet och utökade möjligheter till elektroniskt informationsutbyte (SOU 2006:48, SOU 2008:100, SOU 2009:6, SOU 2011:3, Riksrevisionen 2011, Riksrevisionen 2010, prop. 2007/08:160).

Det är även viktigt att ha i åtanke att de utbetalande aktörerna har mycket olika förutsättningar för sin kontrollverksamhet. En myndighet som ofta lyfts fram som ett gott exempel är Försäkringskassan som sedan mitten av 00-talet haft särskilda öronmärkta kontrollutredare som specialiserat sig på kontrollfrågor. Myndigheten fick till och med särskilda medel för att anställa sådana utredare 2006 och 2007 (Socialdepartementet 2006). När Riksrevisionen 2011 undersökte kontrollarbetet var det enbart Försäkringskassan, CSN och vissa kommuner och arbetslöshetskassor som hade sådana utredare. År 2015 var det vanligare, då fanns en motsvarighet på alla myndigheter, även om det fortfarande varierade mellan kommuner och arbetslöshetskassor (Riksrevisionen 2011, jfr Delegationen mot felaktiga utbetalningar 2007, se Brå 2015:8). Hos vissa myndigheter är kontrollen integrerad i förmånshandläggningen. Syftet är att försöka integrera kontrollperspektivet redan innan utbetalning ägt rum, men risken är uppenbar att kontroller prioriteras ner vid hög arbetsbelastning (Brå 2015:8). Förmånshandläggarna har ett expertstöd i form av specialister, särskilt utsedda kontrollutredare eller bidragsbrottsutredare som kopplas in vid svårare fall eller för att avgöra om polisanmälan ska ske.

I de minsta organisationerna är det enligt referensgruppsmedlemmar svårt att bygga upp kompetens i kontrollfrågor. Det gäller särskilt små kommuner och arbetslöshetskassor. Här finns det i bästa fall en person som ansvarar för utredningar och polisanmälningar, vilket gör det väsentligt svårare att kompetensutveckla sig än inom en större organisation. I en tidigare studie framkom en efterfrågan på att Sveriges kommuner och landsting skulle driva frågan, särskilt för att stötta de mindre kommunerna i kontrollarbetet (Brå 2015:8). Det har även i föreliggande studie framkommit att det saknas vägledning från centralt håll om hur kommunerna ska arbeta när de hittar misstänkta fel. Till detta kommer att misstänkta ärenden kan bli liggande länge till följd av resursbrist, vilket gör det svårt att polisanmäla, eftersom det hunnit gå för lång tid sedan de eventuella brotten begicks.

Fokus på efterkontroll

Kännetecknande för organisationer som endast lägger små resurser på kontroll är att den tenderar att bli reaktiv och händelsestyrd, snarare än strategisk och preventiv. Detta gäller i allra högsta grad de utbetalande myndigheterna och organisationerna. Intervjupersoner i denna och tidigare studier understryker vikten av att genomföra kontroller inför utbetalningar och inte enbart i efterhand när det uppkommit misstankar om felaktigheter (jfr Brå 2015:8, ISF och Brå 2011:12). Några intervjupersoner menar att skadan blir större både för den enskilde och för myndigheten när utbetalningar hunnit rulla på en tid. En gärningsperson berättar att han fick ett återkrav som hann bli stort innan utbetalningarna stoppades. Detta kännbara återkrav blev ett motiv för fortsatt bidragsbrottslighet. Hans bild var dock att myndigheterna med tiden blivit snabbare att upptäcka felaktigheter.

Myndigheter och organisationer med kontrollutredare eller motsvarande har genom dessa en särskild yrkesgrupp som är anställd och utbildad för ändamålet och ser kontroll som något positivt. Deras kontrollarbete sker dock många gånger i samband med eller efter att utbetalning har skett, så det rör sig primärt om efterkontroll. Impulserna[86] uppkommer framför allt på basis av misstankar från förmånshandläggarna, men också från egna urval, tips från allmänheten eller andra myndigheter. De sammanställer misstankarna och genomför de utredningsåtgärder de har mandat att göra. Det kan exempelvis vara att kontrollera uppgifter från den sökande hos andra myndigheter. Vissa använder också sociala medier för att se om en person exempelvis skriver om företagsverksamhet eller om det framgår att personen arbetar svart, parallellt med sitt bidrag (ISF och Brå 2011:12, Brå 2015:8).

Kvalificerade brott fastnar sällan i kontrollen

Slående i ärendegranskningen är att de flesta fall rör tämligen tydliga felaktigheter, som går att upptäcka genom att stämma av olika officiella uppgifter om inkomster och boendeförhållanden. Vissa ärenden är i stort sett frånvarande i granskningen. Det gäller dem som rör svarta inkomster eller helt konstruerade inkomstuppgifter som kvalificerar för arbetslöshetsersättning eller högre bidrag i form av exempelvis sjukpenning eller föräldrapenning. Det vill säga de lite mer kvalificerade brotten.

Tidigare studier innehåller fler sådana exempel, men då har brottet ofta upptäckts av Skatteverket (Brå 2011:7, ISF och Brå 2011:12). I denna studies urval finns enbart ett ärende där den utbetalande myndigheten, Försäkringskassan, lyckats utreda och

[86] Innebär en signal om misstänkt felaktighet.

slå hål på en sökandes felaktiga inkomst. Givet det antalsmässigt begränsade urvalet av granskade ärenden kan kritikern hävda att det är en slump att det ärendet kommer från just Försäkringskassan. Utfallet att Försäkringskassan uppvisar en högre kontrollkompetens vinner dock stöd i att de har fler kontrollutredare och en längre tradition än övriga aktörer av detta arbete (se även ISF och Brå 2011:12, Brå 2015:8).

Konsekvensen av en sådan variation i kontrollkompentens mellan myndigheter och organisationer är att samma brottsliga gärning kan generera en utbetalning hos en aktör utan att det upptäcks, hos en annan generera bidrag och upptäckas och hos en tredje stoppas redan i handläggningen inför den första utbetalningen. Med andra ord ger en organisations kontrollkompetens stora avtryck i vilka ärenden som hamnar på polisens bord.

Går utvecklingen mot preventiv kontroll?

Försäkringskassan, CSN och andra myndigheter som arbetar en del med egna urval har en bas för preventiv kontroll, där man försöker att identifiera riskärenden på ett mycket tidigt stadium. Dessa urval blir alltmer träffsäkra på andelen misstänkta ärenden. Filosofin är att försöka släppa igenom de korrekta ärendena och låta dem få snabb service och utbetalning, medan man fångar upp mer och mer av brottsligheten. Utvecklingen går mot att arbeta mer med riskanalyser och urval där organisationerna försöker närma sig ett mer strategiskt och förebyggande kontrollarbete för att stoppa felaktiga utbetalningar innan de ägt rum.

Bakgrunden till arbetet med urval är erfarenhet om hur brotten går till som fåtts genom utredningar av ärenden, från stickprovskontroller och riktade kontroller av ärenden som uppfyller vissa kriterier. Redan innan dessa urval användes hade CSN genom just riktade kontroller i några ärenden förebyggt felaktiga utbetalningar (Brå 2015:8).

Att skapa träffsäkra urval är dock lättare för vissa förmåner och bidrag än andra. När fusket ser likartat ut, och skiljer sig från legitima bidragstagares uttag blir det lättare att sortera fram. Ju komplexare förmån, desto större är utmaningen för myndigheterna att identifiera adekvata riskindikatorer. Särskilt svårt blir det när man bara har tillgång till viss information att lägga in i databasen, men indikatorerna på brott dyker upp i något annat system, genom en annan myndighets kontroller. Ett troligt sådant exempel är vissa företagarstöd, där ansökan om ersättningen och handlingar som lämnas in till Arbetsförmedlingen i sig inte föranleder extra kontroller, men som tillsammans med uppgifter från Skatteverket skulle kunna föranleda brottsmisstankar.

Utbetalande myndigheter behöver hjälp från kontrollmyndigheter

Utmaningen med att upptäcka bidragsbrott och andra välfärdsbedrägerier ligger inte främst i brottens komplexitet utan i de utbetalande aktörernas uppdrag. Jämfört med de typiska brottsbalksbedrägerierna är bidragsbrotten knappast komplexa, svårutredda eller utmanande. Inte minst eftersom gärningspersonen är känd och den drabbade myndigheten eller organisationen kunnat utreda en hel del på egen hand. Jämfört med andra storskaliga ekobrott är inte ens de mest organiserade bidragsbrotten särskilt välorganiserade. Det är också känt i vilket bolag brotten begås, eftersom det är det bolaget som tar emot ersättningen. Det finns ett visst inslag av målvakter, men jämfört med storskaliga skattebrott eller kreditbedrägerier är organisationsnivån låg.

Det har ändå visat sig vara svårt för utbetalande myndigheter och organisationer att upptäcka och utreda brotten. En stor svårighet är att de sällan har all information som de behöver, utan är beroende av (icke-offentliga) uppgifter från andra aktörer.

Kommunerna har en särställning, och lagstiftningen ser annorlunda ut än för övriga utbetalande myndigheter och organisationer. Begränsningar bland annat i lagen om underrättelseskyldighet gör att kommunerna – som fysiskt träffar sina klienter och får betydligt större kunskap om dem än andra utbetalande aktörer – inte får lämna information till andra aktörer om misstänkta bidragsbrott (se vidare Brå 2015:8). Däremot får de ta emot impulser om bidragsbrott där de är målsägare enligt lagen om underrättelseskyldighet. Med andra ord är vissa namngivna andra myndigheter skyldiga att rapportera när de misstänker fusk med exempelvis kommunernas ekonomiska bistånd.

Arbetsförmedlingen och länsstyrelserna befinner sig i en ännu sämre sits. Företagarstöden och lönegarantin riktas inte till enskilda för personligt ändamål, och brott mot dessa faller därför inte inom ramen för bidragsbrottslagen och lagen om underrättelseskyldighet. Detta innebär att andra myndigheter kan upptäcka deras brott, men inte får rapportera misstankarna. Det framgår både i denna och tidigare studier (se Brå 2015:8, SOU 2008:74, SOU 2014:16). Det handlar i stället om bedrägerier enligt brottsbalken. Referensgruppen bekräftar dock att dessa brott är mycket få i förhållande till de ”vanliga” bedrägeriernas stora volymer.

Eftersom personer som begår brott mot företagarstöd och lönegaranti ofta fuskar med andra bidrag samt skatter och avgifter vore Arbetsförmedlingen och länsstyrelserna hjälpta av att tydligare definieras som utbetalande myndigheter (jfr Brå 2015:8). Detta skulle kunna leda till att Skatteverket enligt lagen

om underrättelseskyldighet vore skyldigt att underrätta dem om misstänkta felaktigheter. Ett sätt att lösa detta sekretessproblem och lättare få uppgifter från andra myndigheter har varit att Arbetsförmedlingen, och även vissa länsstyrelser, gått in i den myndighetsgemensamma satsningen mot organiserad brottslighet (SOU 2014:16, Brå 2015:8).[87]

Både utredare och målsägare

En central fråga som diskuterats av intervjupersoner och referensgruppsmedlemmar är hur man ska förhålla sig till att den utbetalande myndigheten både har sakkunskapen om förmånerna och är målsägare vid bidragsbrott och andra välfärdsbedrägerier. Till skillnad från bedrägerier mot privatpersoner är det alltså målsägaren själv som utreder händelsen, gör en preliminär uppsåtsbedömning och polisanmäler om man tror att det rör sig om ett brott och inte en oavsiktlig felaktighet.

I vissa fall innehåller polisanmälan en flera sidor lång utredning som visar brottstillfällena, belopp per utbetalning och totalsumma. I den mån den sökande skickat in brev eller i samtal lämnat väsentlig information kan detta finnas med i den utbetalande myndighetens eller organisationens egen utredning. Vissa intervjupersoner menar att rättsväsendet borde utnyttja detta mer i den fortsatta utredningen, andra är tydliga med att det från och med en anmälan är en fråga för rättsväsendet. En åklagare berättar:

> *De lämnar in en polisanmälan och tycker att det får väl polisen utreda. Men hallå, hallå – vem är det som kan regleringen kring det? Det är ju ni! Ni måste ju kunna beskriva på vilket sätt det är rätt och på vilket sätt det är fel. Vi har haft halv sjukersättning och jobbat 25 procent ... Okej? Hur funkar de där reglerna? Det får ni förklara i så fall. Där har Försäkringskassan blivit mycket, mycket bättre. De levererar ju mer eller mindre nästan färdiga utredningar.*

Andra intervjupersoner menar att de behöver de utbetalande myndigheternas kunskap, men det är svårt att involvera dem i utredningen, eftersom de trots allt är målsägare och därför en part i målet. Givet de bitvis komplexa regelverken ökar effektiviteten om det enkelt går att ställa frågor om dessa regelverk. En tidigare studie visar att några myndigheter, däribland CSN, lagt resurser på att konstruera en färdig bilaga som beskriver regelverken – för att underlätta för polis och åklagare (Brå 2015:8).

[87] Det är en satsning som inleddes 2009 där en rad myndigheter samverkar för att bekämpa grov organiserad brottslighet. I satsningen ingår följande myndigheter: Arbetsförmedlingen, Ekobrottsmyndigheten, Försäkringskassan, Kriminalvården, Kronofogdemyndigheten, Kustbevakningen, Migrationsverket, Polismyndigheten, Skatteverket, Säkerhetspolisen, Tullverket och Åklagarmyndigheten.

En målsägare med egna sanktionsmöjligheter

En tydlig skillnad mellan målsägare vid bidragsbrott och andra välfärdsbedrägerier respektive företag och privatpersoner som drabbas av bedrägerier är att de förstnämnda har egna sanktionsmöjligheter. Vid sidan av att göra en polisanmälan har alla utbetalande myndigheter och organisationer möjlighet att återkräva det felaktigt utbetalade beloppet. Denna återkravsprocess är ofta skild från utredningen om huruvida det rör sig om ett bidragsbrott, bedrägeri eller om det var ett ouppsåtligt misstag. De större myndigheterna har särskilda återkravshandläggare.

Till detta kommer att arbetslöshetskassorna har ytterligare sanktionsmöjligheter. De är medlemsorganisationer, och skiljer sig därför något från övriga utbetalande aktörer. Arbetslöshetskassornas särskilda sanktioner heter ”frånkännande” och ”uteslutning”. Vid ett frånkännande får medlemmen ingen ersättning i ett visst antal ersättningsdagar. Uteslutning innebär att man utesluts ur den aktuella arbetslöshetskassan. Det kan bli aktuellt om man aktivt lämnat felaktiga eller vilseledande uppgifter eller underlåtit att upplysa om ändrade förhållanden som påverkar rätten till ersättning.

Denna sanktionsmöjlighet gör att de utbetalande myndigheterna och organisationerna inte blir fullt så beroende av rättsväsendet som andra målsägare. De kan utdela egna sanktioner och i vissa fall får de också tillbaka felaktigt utbetalda medel. Detta, tillsammans med intervjuer och tidigare studier, talar för att de knappast polisanmäler för mycket. Skälet till att ärenden ändå läggs ner av polis och åklagare tycks oftare vara att det inkommer ny information i förhör eller att det av andra skäl är svårt att styrka och bevisa uppsåtet och gärningen.

Rapporten fortsätter nu med en analys av vad som händer när dessa – och andra bedrägerianmälningar – hanteras av rättsväsendet.

Rättsväsendets arbete

Tidigare i rapporten presenterades översiktliga redovisningar av personuppklaringsandelar och nedläggningsorsaker för de mest vanligt förekommande kategorierna av bedrägerier i Brås urval av anmälda bedrägeribrott. Detta kapitel börjar med en kort sammanfattning av resultaten avseende skillnader i personuppklaring mellan de olika typerna av bedrägerier, och därefter ligger fokus på att sätta dessa resultat i en bredare kontext, med inriktning på de strukturella förutsättningarna som påverkar rättsväsendets möjligheter att utreda och lagföra de polisanmälda bedrägeribrotten.

Stor variation mellan olika bedrägeribrott i förutsättningar för personuppklaring

Något förenklat kan det konstateras att det finns tre centrala förutsättningar som måste föreligga för att brott ska personuppklaras:

- Det måste finnas en misstänkt person som identifierats.
- Det måste finnas tillräckligt med bevisning för att knyta gärningspersonen till brottstillfället.
- Det måste finnas tillräckligt med bevisning för att styrka ett brottsligt uppsåt (eller motsvarande, t.ex. grov oaktsamhet).

Tidigare i rapporten visades att personuppklaringen är mycket högre för vissa typer av bedrägerier än andra. När det gäller brottsbalksbedrägerierna (se tabell 23) kan de stora skillnaderna i personuppklaringen mellan olika typer av anmälda bedrägerier i första hand hänvisas till de möjligheter som finns för polisen att identifiera misstänkta personer och i andra hand till möjligheter att knyta gärningspersonen till de enskilda brottstillfällena och att styrka uppsåt. När det däremot gäller bidragsbrott är gärningspersonen typiskt sett redan känd och utmaningen ligger i att bevisa uppsåt (alternativt grov oaktsamhet).

Tabell 23. Sammanfattande redovisning av skillnader i personuppklaring i Brås urval av brottsbalksbedrägerier.

	Anmälda brott		Andel personuppklarade till slutet 2014	Mediantid från inskrivnings-datum till uppklarings-/ nedläggningsbeslut	
	N	%	%	Uppklarade	Nedlagda
Annonsbedrägerier	62	16	27	280	22
Fakturabedrägerier	49	12	14	358	81
Kortbedrägerier	87	22	2	209	2
Kreditbedrägerier	68	17	6	182	5
Övrigt telefon- och internetbedrägeri	62	16	0	-	1
*Andra bedrägeri-ärenden**	72	18	3	26	4
Totalt	**400**	**100**	**8**	**273**	**4**

* Övrig bedräglig försäljning, övriga bedrägliga köp/lån/uttag, butiksbedrägeri, annat bedrägeri mot BrB 9 kap.

Bättre förutsättningar för uppklaring vid annons- och fakturabedrägerier

Den kategori av brottsbalksbedrägerier som kännetecknas av bäst möjligheter i alla tre avseenden är annonsbedrägerier. Det beror inte minst på att gärningspersonerna ofta använder sitt eget bankkonto vid brotten, vilket ger bra möjligheter att både spåra gärningspersonen och att sedan knyta den misstänkte till de enskilda brottstillfällena. Vidare kan brottsserierna enkelt samordnas med hjälp av kontonumret, vilket enligt intervjupersonerna gör det relativt enkelt att styrka uppsåt genom att visa på orimligheten i de typer av invändningar som gärningspersoner typiskt sett använder sig av i dessa ärenden.

Även fakturabedrägerier kännetecknas av relativt sett goda möjligheter till personuppklaring. Fakturorna innehåller information om ett bankkonto som pengar ska betalas till, de begås ofta i mycket stor omfattning och de kan samordnas med hjälp av antingen kontouppgifter eller det organisationsnummer som framgår av fakturorna. De svårigheter som enligt intervjupersonerna uppstår vid utredningar av fakturabedrägerier handlar i stället om att utredningarna blir mycket omfattande, bland annat på grund av det stora antalet målsägare. Juridiskt sett kan det dessutom bli svåra avvägningar om hur man framgångsrikt ska driva målen i domstol.

Sämre förutsättningar vid utredningar av kort- och övriga telefon- och internetbedrägerier

De kategorier av brottsbalksbedrägerier där personuppklaringen är lägre – kortbedrägerier, kreditbedrägerier och övriga tele-

fon- och internetbedrägerier – och som relativt ofta läggs ner av polisen med motiveringen att brottet inte går att utreda, kännetecknas av helt andra förutsättningar för personuppklaring. Här är det relativt sällan som man når fram till den första av de tre förutsättningar som nämns ovan, det vill säga att identifiera en misstänkt gärningsperson.

Vid kort- och kreditbedrägerier finns i vissa fall en känd misstänkt person redan vid anmälningstillfället, till exempel om gärningspersonen är en bekant till anmälaren eller om anmälan görs av en butik eller ett utlämningsställe där brottet har upptäckts vid en kontroll av ett misstänkt kort eller identitetshandling. Men oftast är gärningspersonens identitet okänd. I dessa typer av ärenden finns det sällan någon möjlighet att följa pengar till ett bankkonto som kan knytas till gärningspersonen. Vidare tycks de åtgärder som är möjliga för polisen att vidta för att identifiera misstänkta personer, framför allt i form av försök att säkra bildbevisning från övervakningskameror, sällan ge resultat. Det beror bland annat på att många butiker inte sparar övervakningsbilder i mer än några dagar.

Vid de olika typer av brott som ingår i kategorin övriga telefon- och internetbedrägerier, finns ibland bearbetningsbara spår i form av exempelvis en banköverföring. Samtidigt har större delen av dessa brott anmälts utan att det skett en överföring, och i den mån det finns bearbetningsbara spår i dessa ärenden leder de oftast utomlands. Enligt litteraturen begås dessa bedrägerier ofta av kriminella grupperingar som utnyttjar tekniska möjligheter att försvåra de brottsbekämpande myndigheternas eventuella spårningsförsök.

Svårigheter vid bidragsbrotten avser framför allt bevisproblem

När det gäller brott mot bidragsbrottslagen, är de första två förutsättningar som nämnts oftast uppfyllda redan vid anmälningstillfället, och personuppklaringen är relativt hög jämfört med de flesta typerna av brottsbalksbedrägerier. De motiveringar som anges av polis och åklagare vid nedläggning handlar oftast om svårigheter med att styrka brottet, och kanske framför allt att den misstänkte haft ett brottsligt uppsåt (alternativt varit grovt oaktsam). Här tycks det ofta handla om skiljaktigheter i uppsåtsbedömningen mellan utredare hos den utbetalande myndigheten och poliser eller åklagare. Ett önskemål som framfördes av en representant för de utbetalande myndigheterna var att polisen skulle ta mer hjälp av utredarna vid de utbetalande myndigheterna för att lära sig hur myndighetsutredarnas underlag skulle kunna användas för att styrka uppsåt eller ett grovt oaktsamt handlande (jfr Brå 2008:6, Brå 2015:8).

En strukturell obalans mellan brottsvolymen och utredningsresurser

Brås redovisning av bedrägeriutvecklingen enligt befintlig statistik visar att det är ett mycket stort antal bedrägeribrott som anmäls till polisen samt att volymen av anmälda brott har ökat markant sedan 2008. År 2014 anmäldes över 144 000 bedrägeribrott och över 10 000 brott mot bidragsbrottslagen. Sammantaget ökade antalet anmälda brottsbalksbedrägerier och bidragsbrott med över 50 procent under perioden 2008–2014. Under samma period ökade antalet anmälningar som ledde till personuppklaring med 20 procent. Samtidigt tyder de statistiska källorna på att de kategorier av anmälningar som ökat mest till stor del avser svårutredda bedrägerityper – kortbedrägerier och internetbedrägerier.

Ökade, men alltjämt otillräckliga, utredningsresurser i förhållande till brottsvolymen

Under perioden 2008–2014 ökade den totala resurstiden som enligt polisens verksamhetsberättelser lagts ner på utredning och lagföring av bedrägeribrotten med drygt 40 procent.[88] Enligt intervjupersoner både inom och utanför rättsväsendet finns emellertid fortfarande en stor obalans mellan de anmälda bedrägeribrottens volym och de resurser som finns tillgängliga för att utreda och lagföra dessa brott. Ett mycket tydligt tema i Brås intervjuer med poliser och åklagare var ett önskemål om att bedrägerirotlarna skulle få de resurstillskott som krävs för att bättre kunna hantera de stora brottsvolymer som löpande anmäls till rättsväsendet.

En viktig effekt av de bristande utredningsresurserna är att handläggningstider för bedrägeriutredningar kan bli långa,[89] vilket bland annat har uppmärksammats av JO vid flera tillfällen. År 2010 riktade exempelvis JO skarp kritik mot polisen i Stockholm på grund av att ett stort antal bearbetningsbara bedrägeriärenden hade legat i balans en längre tid utan att några utredningsåtgärder hade vidtagits (JO 2011). Flera av intervjupersonerna nämnde också stora balanser hos bedrägerirotlarna som ett problem. En biverkan av pressen på polisen att hålla ner handläggnings-

[88] Rikspolisstyrelsen 2011 (s. 247), 2012b (s. 229), 2015 (s. 169). Resurstiden redovisas för kategorin Bedrägeribrott m.m., som inkluderar dels brott mot bidragsbrottslagen, dels brott mot 9 kap. 1–10 § brottsbalken (Rikspolisstyrelsen 2010, s. 82). Redovisningskategorin är därmed bredare än de bedrägeribrott som ingått i Brås kartläggning.

[89] Polisens årsredovisningar för perioden 2008–2014 visar att medelgenomströmningstiderna för bearbetade bedrägeriärenden varje år har legat högre än motsvarande genomströmningstider för de andra redovisade brottstyperna, med undantag under de flesta år för de ekonomiska brott som handläggs av Ekobrottsmyndigheten.

tiderna, i kombination med de bristfälliga utredningsresurserna, blir dessutom en ökad press att snabbt lägga ner de anmälningar där man bedömer att de sannolikt inte kommer leda till åtal.

Resursläget skapar både arbetsmiljöproblem och frustration

Obalansen mellan brottsvolymen och de tillgängliga utredningsresurserna har flera negativa effekter på rättsväsendets arbete med att utreda och lagföra bedrägeribrott. Det skapar inte minst allvarliga arbetsmiljöproblem. Bland intervjupersonerna var det några såväl inom som utanför rättsväsendet som beskrev både förundersökningsledare hos polisen och åklagare som hade ”gått in i väggen” och blivit långtidssjukskrivna som resultat av en för tung arbetsbelastning. En åklagare menade att det i en del större bedrägeriutredningar behövs två förundersökningsledare för att klara av arbetsbelastningen på ett hållbart sätt (jfr Åklagarmyndigheten 2015).

Bland intervjupersonerna var det bedrägeriutredare inom polisen som uttryckte en frustration över att få ägna mycket tid åt relativt enkla mål, framför allt annonsbedrägerier, för att det är dessa som ger utslag i uppklaringsstatistiken, ”lättplockade poäng” som en polis uttryckte saken. Både intervjuade poliser och åklagare uttryckte en frustration över de resurser som bedrägeriutredare får lägga ner på att utreda mindre allvarliga bidragsbrott.

> *Vi vill inte åt en massa mammor som har glömt vård av barn, och en arbetslös som inte vet hur han ska fylla i a-kassans blanketter och så vidare. Det är inte dem vi söker, utan vi söker de här som systematiskt utnyttjar vårt välfärdssystem, att bedra staten på pengar, det är där de stora pengarna ligger. De här andra brotten, de är bara en belastning för oss.*

Det fanns också en frustration över att det så sällan finns resurser för åtgärder som skulle ge möjlighet att komma åt huvudgärningspersoner som använder sig av målvakter eller medhjälpare, till exempel för att hämta ut varor som köpts på kredit eller med stulna kortuppgifter.

Snabb nedläggning av särskilda brottskategorier kan resultera i kunskapsstagnation

Som kan uttydas av resultaten av Brås granskning av nedläggningarna bland bedrägeribrott innebär den press som finns på polisen att snabbt lägga ner anmälningar som inte anses kunna leda till lagföring en risk att rättsväsendets utredningsresurser framför allt riktas mot en mindre del av den anmälda bedrägeribrottsligheten, där det relativt enkelt går att identifiera en misstänkt

person. I förlängningen kan det innebära att kunskaperna inom polisen och åklagarväsendet om vissa typer av bedrägeribrott, samt om hur dessa ska utredas framgångsrikt, blir allt bättre, medan det inte blir någon utveckling när det gäller andra typer av bedrägeribrott.

En sådan trend kan i längden bli problematisk, inte minst då det sker en ständig utveckling i de modus som används vid bedrägeribrott. De intervjuade brottsutredarna och åklagarna menar att utredningen av nya typer av brottslighet är en lärande process, där man får lära av andras eller egna erfarenheter och misstag.

Fler omfattande och komplexa utredningar som slukar resurser

Kriminalstatistiken visar att ökningen i antalet personuppklarade bedrägeribrott är fördelad över ett minskande antal lagföringar. Utöver den ökning i volymen av anmälda bedrägerier som rättsväsendet har att hantera, tyder detta förhållande på att det också skett en ökning i andelen större utredningar som avser ett stort antal bedrägeritillfällen. Denna utveckling är sannolikt kopplad till förbättringar som skett i polisens samordning av bedrägeribrott, vilket är en positiv utveckling som lyftes fram av flera av intervjupersonerna, inom både rättsväsendet och näringslivet. Det framgår också av en inspektion av polismyndigheternas handläggning av bedrägeriärenden som genomfördes av Rikspolisstyrelsen år 2011 (Rikspolisstyrelsen 2012a). Enligt flera intervjupersoner har möjligheterna till en bra samordning av bedrägeriärenden förbättrats ytterligare genom polisens sammanslagning till en myndighet, bland annat tack vare att poliser i hela landet nu har tillgång till samma, gemensamma datoriserade utredningssystem (DurTvå). Samtidigt menar intervjupersoner att en del stora bedrägeriutredningar, till exempel vid fakturabedrägerier, har inletts som en del i satsningen mot den grova organiserade brottsligheten.

En konsekvens av denna i grunden positiva utveckling är emellertid en ökande andel bedrägeriutredningar som avser en omfattande och ofta även komplex brottslighet, som kräver stora utredningsresurser. Fakturabedrägeriutredningar kan exempelvis avse flera tusen brottsmisstankar och ett stort antal målsägande. Särskilt i mål som avser fakturabedrägerier efter telefonkontakter kan det också finnas många misstänkta gärningspersoner, bland annat i form av telefonförsäljare. Den bevisning som krävs för att kunna knyta rätt gärningsperson till de olika brottstillfällena blir mycket omfattande.

Enligt intervjuade åklagare kan utredningar av både kreditbedrägerier och kortbedrägerier också bli mycket omfattande, framför

allt när det handlar om systematiska och organiserade kriminella verksamheter. Där kan det dels förekomma ett flertal gärningspersoner, dels kan brottsligheten ske i flera led. Det kan handla om att skaffa fram stulna kortuppgifter eller köpa ett kreditvärdigt bolag, inköp av stora mängder varor och slutligen vidareförsäljning av dessa varor, till exempel via annonssidor på internet. Som framgår av en del av domarna i Brås granskning krävs en insamling och bearbetning av stora mängder data från flera olika källor för att kunna knyta gärningspersonerna dels till varandra, dels till de olika brottstyperna och brottstillfällena som ingår i förundersökningen.

Även bland bedrägeribrotten mot välfärden förekommer exempel på utredningar som blir mycket omfattande och resurskrävande, framför allt i form av stora assistansbedrägerimål.

Förundersökningsbegränsning kan inte alltid användas som det var tänkt

Enligt Riksåklagarens riktlinjer (Åklagarmyndigheten 2008) är det främsta syftet med tillämpningen av rättegångsbalkens bestämmelser om förundersökningsbegränsning att öka effektiviteten i brottsbekämpningen genom att koncentrera utredningsresurser till de uppgifter som är mest angelägna. Genom att avstå från att lägga resurser där insatserna inte skulle ha någon betydande effekt på påföljden vill man skapa förutsättningar för att i stället ta hand om andra, mer angelägna brott (ibid.). Teoretiskt sett kan möjligheten att tillämpa reglerna om förundersökningsbegränsning anses som särskilt användbara i stora bedrägeriutredningar. I dessa fall handlar det om en uttalad seriebrottslighet, där de utredningsresurser som kan slukas om man ”utreder allt” blir nära intill oändliga, men där de enskilda brotten i brottsserien får mindre effekt på påföljden ju längre brottsserien är.[90]

Intervjuade åklagare har varit överens om att möjligheten att använda förundersökningsbegränsning vid bedrägeribrottslighet tillämpas olika av olika åklagare. Enligt intervjupersonerna finns det en del åklagare som ”åtalar på allt” medan andra är mer angelägna om att endast utreda de brottstillfällen som behövs för att vid åtal uppnå vad som bedöms vara en lämplig påföljd.

Det var samtidigt flera åklagare som lyfte fram att det är svåra bedömningar som måste göras vid beslut om att förundersökningsbegränsa brottsmisstankar under större bedrägeriutredning-

[90] Det beror på att det i svensk påföljdspraxis tillämpas en så kallad straffrabatt vid upprepad brottslighet. I praktiken innebär det att domstolen utgår från straffvärdet för det allvarligaste brottet i domen och därefter lägger till en procentandel av straffvärdet för de övriga brotten enligt en fallande skala (jfr SOU 2013:85, s. 82f.)

ar. Bland annat menade man att det kan vara viktigt att kunna påvisa den faktiska omfattningen av brottsligheten i domstolen. Åklagare menade vidare att man inte får tappa bort målsägandeperspektivet samt att det kan vara svårt att ”välja bort” vissa målsägande i större mål, bland annat om det framgår att gärningspersonerna medvetet har riktat in sig på särskilt sårbara grupper, till exempel äldre personer. Andra menade att man i utredningar som avser många brottstillfällen från början inte kan veta vilka av dessa brottstillfällen som man kommer att kunna knyta gärningspersoner till och hitta tillräckligt med bevisning för att styrka det i domstolen. Det innebär att ett för tidigt beslut att förundersökningsbegränsa vissa brott kan äventyra möjligheterna att skapa ett tillräckligt bra bevisningsunderlag för att över huvud taget väcka åtal.

> *När jag börjar med de här 400 brotten så vet jag inte vilka jag kan jobba med. Om jag redan då säger, ”Äh, men vi jobbar med de 10”. Då vet inte jag om jag kan bevisa dem till slut.*

Samtidigt menade åklagare att man också måste ta hänsyn till de utredningsresurser som finns att tillgå inom polisen, bland annat då det pressade arbetsläget innebär att man från polisens håll gärna vill att åklagare ska avgränsa de utredningsinsatser som krävs i större bedrägeriutredningar. Överlag kan slutsatsen dras att arbetet med komplexa bedrägeriutredningar ställer stora krav på förundersökningsledaren att veta hur man bäst ska avgränsa förundersökningen i det enskilda fallet (jfr även Åklagarmyndigheten 2015).

Kopplingar till utlandet försvårar bedrägeriutredningar

En annan faktor som försvårar bedrägeriutredningar är de gränsöverskridande aspekterna av den här typen av brottslighet. De motiveringar som anges av polisen vid nedläggning visar att relativt många brott har setts som icke utredningsbara på grund av att de har begåtts utomlands. Ahola (2013) menar att det inte är ovanligt att bedragare använder sig av banker i flera olika länder, samt att pengarna studsas mellan ett flertal bankkonton innan de till slut hämtas ut. Att följa pengarna utomlands handlar därmed om en mycket tidskrävande process, med successiva förfrågningar till flera utländska banker, som dessutom till slut ofta endast leder till banken där en målvakt redan hunnit hämta ut pengarna i kontanter (ibid., jfr även Moore m.fl. 2009).

Mot bakgrund av det knappa resursläget, och den press som finns på polis och åklagare att snabbt avsluta ärenden som inte kommer att leda till åtal, är det inte orimligt att utredningar snabbt läggs ner när de enda spår som finns är t.ex. uppgifter om ett utländskt kontonummer till vilket pengar har skickats via

Western Union. Det kan handla om ett ”vän i nöd”-mejlbedrägeri eller uppgifter om en transaktion som har initierats i ett annat land (som exempelvis är fallet vid många av de polisanmälda kortbedrägerierna).

Att polisen inte följer spår som leder utomlands för att försöka identifiera okända gärningspersoner betyder däremot inte att bedrägeribrott med gränsöverskridande inslag alltid läggs ner av rättsväsendet. Det framgår av de granskade domarna att gränsöverskridande bedrägeribrott, som ofta avser långa brottsserier och betydande belopp, blir både åtalade och lagförda i svenska domstolar. I domarna finns flera exempel på gränsöverskridande bedrägeriverksamheter som lett till lagföring, som avser såväl annonsbedrägerier som kortbedrägerier och även fakturabedrägerier.

Det är också flera intervjuade åklagare som har beskrivit att man ofta får göra en bedömning avseende om det är möjligt och rimligt att begära in uppgifter från utländska banker för att kunna följa bedrägerirelaterade gränsöverskridande penningströmmar. En åklagare menade att man kan få uppgifter från en utländsk bank, till exempel med hjälp av finanspolisen, men att denna information i första hand bara får status som så kallade upprättelseuppgifter. För att kunna föra in uppgifterna i en förundersökning måste man sedan göra en begäran om internationell rättslig hjälp. Enligt åklagare är processen kring att begära rättslig hjälp tidskrävande, och utredningarna bromsas upp och fördröjs ytterligare.

Begränsade it-resurser och underutvecklade ärendehanteringssystem bromsar

Det finns flera domar i Brås material där det framgår att brottsutredningen har krävt omfattande it-forensiska undersökningar av datorer och mobiltelefoner. Tidigare Brå-rapporter (Brå 2013:14, Brå 2015:6) om andra typer av brott har uppmärksammat hur både poliser och åklagare upplever att en kapacitetsbrist hos polisens it-forensiska funktioner innebär långa väntetider för att få tillbaka resultat från den här typen av undersökningar, vilket leder till att utredningar drar ut på tiden. Problemet har också uppmärksammats av Rikspolisstyrelsen i en inspektion av förmågan att handlägga it-brott vid fem olika polismyndigheter (Rikspolisstyrelsen 2014). Samma problem har lyfts fram i intervjuer med åklagare även i den här studien.

Ett annat problem enligt intervjupersonerna är att de ärendehanteringssystem som används av polisen och Åklagarmyndigheten inte är utformade för att kunna hantera stora utredningar på ett effektivt sätt. Det innebär att även de rent administrativa åtgär-

der som krävs för att korrekt redovisa anmälda brott, brottsmisstankar och misstankebeslut, som bland annat används som underlag till den offentliga kriminalstatistiken, blir både tidsödande och resurskrävande. En åklagare beskrev till exempel en större bedrägeriutredning, där man hade fått låna in en administratör som fick sitta i en månad bara för att hinna registrera samtliga brottsmisstankar i ärendet.

Kompetensförsörjning

Överlag visar Brås genomgång av de polisanmälda bedrägerierna en stor spridning av olika modus samt att utredning av bedrägeribrottsligheten kräver en bredd och varierad sammansättning av olika kompetenser. Flera av Brås intervjupersoner har också pekat på olika kompetensförsörjningsproblem som negativt påverkar rättsväsendets förmåga att utreda och lagföra bedrägeribrott. När det gäller bidragsbrotten har det exempelvis uppmärksammats i flera olika sammanhang att det finns mycket som talar för att dessa bör utredas av personer som är specialister på området samt att vissa utredare och åklagare anses ha för lite kunskap för att hantera de mer avancerade bidragsbrottsärendena på ett effektivt sätt (Brå 2008:6, Åklagarmyndigheten 2015).

Tidigare Brå-studier (t.ex. Brå 2015:6) har uppmärksammat att både polis och åklagare upplever att it-kompetensen hos rättsväsendets olika aktörer generellt sett är bristfällig, bland annat när det gäller brott som sker via internet, samt att det behövs utbildningssatsningar för att höja denna kompetens. Bland intervjuade poliser och åklagare i denna studie var det framför allt enskilda åklagare som menade att poliser och åklagare skulle behöva mer utbildning avseende bedrägerier som begås via internet. Bland intervjupersonerna från näringslivet nämndes att man märkt en mer generell bristfällig it-kompetens under kontakter med polisen.

Intervjuade åklagare menade också att det åtminstone på vissa bedrägerirotlar är en stor andel unga utredare som måste läras upp och som behöver mycket detaljerade utredningsdirektiv för att veta hur de ska gå tillväga med olika aspekter av en utredning. Detta har också i Brås intervjuer kopplats till en uppfattning att utredningsverksamheten inom polisen har låg status jämfört med andra delar av det polisiära uppdraget samt att detta kan påverka både kompetens- och ambitionsnivån hos polisens bedrägeriutredningsverksamhet. Utredningsverksamhetens låga status skulle därmed ha karaktären av ett strukturellt problem, som sannolikt endast kan hanteras på längre sikt, till exempel genom strategiska förändringar i polisens kompetensförsörjning.

Detta avspeglades också i att Brås intervjupersoner, när de diskuterade behovet av att utöka antalet utredare som arbetar med be-

drägeriutredningar, ofta lade till att det inte nödvändigtvis skulle handla om fler poliser, utan snarare om fler civilutredare med rätt kompetens för uppdraget.

> *Fler poliser. De är underbemannade. De är alldeles för få. Det behövs fler utredare. Utredare som verkligen vill arbeta med ... Just när det gäller bedrägerier behöver det inte nödvändigtvis vara poliser ska jag tillägga.*

Bland annat nämndes ett behov av flera revisorer, tillgångsutredare,[91] personer med kompetensen att analysera olika typer av teknisk bevisning och även av personer med juridisk utbildning. Samtidigt nämndes att det är svårt att hålla kvar duktiga civilutredare inom polisen, delvis på grund av löneläget, delvis på grund av avsaknaden av karriärvägar för civilanställda inom polisorganisationen.

Ny satsning: Polisens NBC

Nationellt bedrägericenter (NBC) startade sin verksamhet i mars 2014 i syfte att göra brottsbekämpningen både mer effektiv och strukturerad (NBC 2014a, Rikspolisstyrelsen 2015). Enligt kontakter med NBC har centrets *polisoperativa* verksamhet koncentrerat sig på att utveckla nationell brottssamordning i bedrägeriutredningar. Det handlar om att samordna utifrån brottsmodus, med fokus på ärenden där det saknas en känd gärningsperson. Varje månad genomförs videokonferenser med kontaktpersoner som utsetts vid landets alla före detta polismyndigheter och nuvarande polisregioner; målet är att skapa en gemensam nationell lägesbild som underlättar operativa prioriteringar.

En viktig utveckling som nämnts av flera av Brås intervjupersoner är NBC:s arbete med att skapa ett nationellt samordningsregister över bankkontonummer. Registret, som fortfarande är under utveckling, innebär att kontoförfrågningar till bankerna numera samordnas centralt, till skillnad från tidigare, då flera förfrågningar om samma kontonummer kunde ställas till banker av bedrägeriutredare i olika delar av landet. Registret innebär både förkortade handläggningstider och förbättrade möjligheter att identifiera bedrägerier med nationell förgrening. NBC har också upprättat en särskild databas i samverkan med underrättelseenheten vid polisens nationella operativa avdelning (NOA) för att effektivisera arbetet med underrättelseinformation. Som också nämnts tidigare i rapporten utgör NBC en viktig samordnande

[91] Enligt intervjupersoner kan tillgångsutredare bland annat genomföra analyser av komplexa transaktionsmönster avseende överföringar mellan olika bankkonton samt koppla dessa mönster till övrig information i utredningen. Redovisningarna underlättar för både förundersökningsledare och domstolar att ta ställning till vilka slutsatser som kan dras med utgångspunkt i transaktionerna.

kontaktpunkt i förhållande till polisens it-brottscentrum vid olika typer av mer organiserade internetrelaterade bedrägeriverksamheter, till exempel angrepp med skadlig kod.

Varje månad sprider NBC, inom rättsväsendet men även externt, korta beskrivningar av aktuell lägesbild på bedrägeriområdet, och tre gånger om året publiceras fördjupande rapporter (se t.ex. NBC 2014a, 2015a, b). Publikationerna bygger även på en kontinuerlig omvärldsbevakning som NBC genomför för att få kunskap om vilket arbete mot bedrägerier som pågår i andra länder.

När det gäller den *brottspreventiva* delen av verksamheten har centret etablerat kontakt med sju brottspreventiva funktioner i respektive polisregion. Syftet är att skapa gemensamma brottspreventiva strategier. Enligt NBC har månatliga videokonferenser lett till en identifiering av ett antal prioriterade områden, som stämmer väl överens med de stora bedrägerityperna som trätt fram i Brås genomgång av de polisanmälda brotten (jfr NBC 2015b):

- kreditbedrägerier via identitetsintrång
- internetköp med stulna kortuppgifter (CNP)
- bedrägerier mot äldre
- fakturabedrägerier
- annonsbedrägerier.

Det pågår även ett flertal metodutvecklingsprojekt vid NBC, bland annat ett samarbete med flertalet aktörer för att skapa en ny rutin för att dela elektroniska kontoutdrag mellan bankerna och rättsväsendet. En annan målsättning är att förbättra rutiner kring inhämtning av övervakningsfilm.

En av de satsningar som NBC själv anser som viktigast är dock att *sprida information* för att öka medvetenheten hos allmänheten och hos viktiga samhällsaktörer. Det sker genom regelbundna mediaframträdanden, föreläsningar och en egen Facebooksida ”Polisen bedrägeri”.

Bedrägeriproblemet kan inte lagföras bort

En viktig slutsats av Brås genomgång av förutsättningarna för rättsväsendets arbete med att utreda de anmälda bedrägeribrotten är att problemen med bedrägeribrottslighet inte kan lösas enbart genom rättsväsendets utrednings- och lagföringsverksamhet. Brottsvolymen är helt enkelt för stor. De viktigaste insatserna för att minska skadan av bedrägeribrottsligheten måste därför riktas mot det förebyggande arbetet i samhället i stort. Detta var också ett återkommande tema under möten med representanter för myndigheter och organisationer vid Brås studiebesök i Storbritannien.

Del 4. Slutsatser, utvecklingsområden och åtgärdsförslag

I denna avslutande del sammanfattas och diskuteras först studiens övergripande slutsatser. Det kommer att framgå vilka utvecklingsområden som är de mest angelägna när det gäller att motverka bedrägeribrottslighet samt bidragsbrott. Därefter presenteras en rad förslag på åtgärder för att förebygga dessa brott, stoppa de brott som redan pågår och förbättra utredningsarbetet gällande brott som redan ägt rum.

Sammanfattande diskussion och slutsatser

Omfattande, heterogent och dynamiskt brottsområde

Få brottsområden präglas av en sådan uppsjö av olika tillvägagångsätt som bedrägeribrottsligheten. Det motsvaras av en stor bredd när det gäller gärningspersoner. Hela skalan finns från personer som har ett akut behov av snabba pengar – exempelvis till följd av skulder och missbruk – till personer med goda kunskaper om företagande, teknik och juridik, som begår storskaliga och välplanerade bedrägerier. Den senare kategorin gärningspersoner har också kapacitet att utveckla sina brottsupplägg och dra nytta av teknisk utveckling och kryphål i regelverk. Det gör det svårare för rättsväsendet att styrka brott.

Förutom att bedrägeribrottsligheten är heterogen och föränderlig når den ut i många samhällssektorer; den drabbar privatpersoner liksom företag och myndigheter.

Utifrån ett urval av polisanmälda ärenden har fem huvudkategorier identifierats gällande bedrägerier enligt BrB 9 kap. Den enskilt största kategorin bland dessa brottsbalksbedrägerier är *kortbedrägerier*, där gärningspersonen använder ett stulet eller skimmat kort för bedrägliga köp eller uttag, alternativt gör köp med elektroniska kortuppgifter – vanligtvis på internet. En nästan lika stor kategori består av *kreditbedrägerier*, som typiskt sett innebär bedrägliga köp eller lån i annans namn. Här används även företag som brottsverktyg. Företag används som regel även i samband med *fakturabedrägerier*, där rena bluffakturor skickas ut till mottagarna, alternativt föregås utskicket av någon form av kontakt (t.ex. telefonförsäljning). Ytterligare en kategori består av *annonsbedrägerier*, där bedragaren genom en annonssida på internet vilseleder en köpare att betala för en vara som sedan inte skickas. En femte, till innehåll inte lika enhetlig kategori har kallats för *övriga telefon- och internetbedrägerier* och innefat-

tar brott där bedragaren, ofta genom sociala medier eller mejl, vilseleder en annan person genom att utnyttja dennes goda vilja (”vän i nöd” eller ”romansbedrägerier”). Här ingår även olika ofta tekniskt avancerade brott där bedragaren använder skadlig kod eller nätfiske för att komma åt känsliga uppgifter. Inte sällan utgör dessa gärningar ett led i annan bedrägeribrottslighet.

Det finns också en sjätte kategori som består av *bidragsbrott och andra välfärdsbedrägerier.* Bidragsbrott täcks inte av brottsbalken utan regleras sedan 2007 enligt en särskild lag och kategorins innehåll är relativt homogent och avgränsat.

Vad väntar i framtiden: bedrägerier med kort, sociala medier och osanna identiteter

Beskrivningen ovan baserar sig på Brås granskning av ärenden anmälda till polisen under våren 2013. De övergripande kategorierna av olika bedrägerityper som togs fram har, enligt intervjupersonerna, inte förändrats i grunden, men mycket tyder på att det bara under den senaste tiden har skett en del skiftningar, och den snabba utvecklingen mot ständigt nya modus lär fortsätta. Experter förutspår att sociala medier kommer att spela en allt viktigare roll i bedragarnas försök att vilseleda andra personer för egen vinning (NBC 2015a[92]). *Annonsbedrägerier* kan, enligt Brås intervjupersoner, delvis ha förflyttats från traditionella annonssidor som Blocket och Tradera till sociala medier (Instagram, Facebook m.fl.).

Det som här benämns *övriga telefon- och internetbedrägerier* omfattar diverse mer tekniskt avancerade upplägg. Sociala medier gör det möjligt för bedragarna att kartlägga en persons vanor och nätverk och utnyttja denna information exempelvis vid mer riktade nätfiskeattacker. Fler bedrägerier kommer också, enligt en prognos (ibid.), att koncentrera sig till mobila plattformer, då allt fler av våra kontakter och transaktioner äger rum där.

Det andra stora problemområdet, även det internetrelaterat, är bedrägerier med elektroniska kortuppgifter. Enligt uppgifter från NBC, baserade på centrets omvärldsbevakning, finns det många indikationer på att just dessa *kortbedrägerier* är den snabbast växande kategorin. Enligt uppgifter från polisen och bankerna har flera stora dataintrång ägt rum under de senaste åren, där mängder av kortuppgifter hamnat i fel händer och använts för bedrägliga köp. Dessa bedrägerier har ofta förgreningar utomlands.

[92] http://www.cnbc.com/2015/12/10/five-fraud-predictions-for-2016-paypal-exec-commentary.html.

När det gäller anmälda *fakturabedrägerier* har utvecklingen varit en annan. Anmälningarna har först minskat något för att sedan öka igen under 2015. Sannolikt speglar dock uppgifterna främst rättsväsendets stötvisa hantering av stora fakturabedrägerihärvor, snarare än en trend i den faktiska brottsligheten. Samtidigt är det ett faktum att näringslivet har satsat stora resurser på att motverka dessa bedrägerier. Uppgifter i denna studie tyder på att detta i kombination med rättsväsendets framgång i vissa ärenden har påverkat brottsligheten och fått vissa gärningspersoner att i stället skicka sina fakturor utomlands.

Det finns också indikationer på att en del gärningspersoner övergått från fakturabedrägerier till *kreditbedrägerier*. Vid båda dessa typer används ofta företag som verktyg, vilket kräver en del erfarenhet och kunskap. Dessa bedrägerier sker inte sällan med hjälp av identitetsstöld, och enligt flera källor har sådana modus ökat kraftigt. Att bedragare använder sig av osanna identiteter identifieras som ytterligare ett område där ökningar är att vänta. Det kan nästan talas om parallella utvecklingstrender, då det å ena sidan utvecklas åtgärder mot säkrare identifiering, samtidigt som ny teknik används för att underlätta snabba köp där i princip ingen identifiering krävs (t.ex. kontaktlösa betalkort).

Bedrägerier kan inte enbart lagföras bort

De stora volymerna av bedrägerier, i kombination med att många delar av samhället påverkas, ställer mycket höga krav på rättsväsendet. Polisens utredningsresurser räcker inte till för att utreda alla bedrägerier som anmäls, utan resultaten talar för att vissa typer av anmälningar snabbt sållas bort för att få resurser att utreda de ärenden som har framgångspotential. Ett primärt mål för det brottsbekämpande arbetet måste vara att minska själva inflödet av bedrägerianmälningar genom förebyggande insatser. För att åstadkomma detta behöver flera berörda samhällsfunktioner – näringslivet, den finansiella sektorn, olika myndigheter m.fl. – göras delaktiga i det förebyggande arbetet.

Brå har inom ramen för uppdraget besökt England, som ligger ett steg före Sverige när det gäller insatser på bedrägeriområdet. Studiebesöket visade tydligt att samma slutsatser har dragits på Home Office, City of London Police, Cifas och Cipfa:[93] med de mångfacetterade bedrägerierna krävs ett betydligt mer utvecklat förebyggande arbete. Företag och privatpersoner måste ha verktyg för att kunna skydda sig själva från identitetsmissbruk och därpå följande bedrägerier. Men det är också viktigt att lägga

[93] Home office är Storbritanniens inrikesdepartement, Cifas är en näringslivsorganisation och Cipfa en organisation som bekämpar bedrägerier mot stat och kommun, samt mot hälso-, utbildnings- och välgörenhetssektorn.

ihop de bilder som olika aktörer har av brottsligheten – för att förstå utvecklingen och ligga i framkant.

Snabb kundservice versus kontroll och säkerhet

När det gäller näringslivet visar intervjuerna ett starkt tema: en upplevd konflikt mellan hög försäljning och effektiva säkerhetsåtgärder. Inom myndigheterna och organisationerna som tillhör välfärdssystemen tycks det finnas en motsvarighet till detta genom en konflikt mellan god service och kontroll.

Som redan nämnts kan det skönjas parallella utvecklingstrender när det gäller säker handel. Det finns en insikt om att god kundkännedom är viktig, liksom en strävan efter att införa effektiva säkerhetsåtgärder för att undvika bedrägerier. Vinstfrågan är dock central för de flesta företag, och den dominerande målsättningen är att göra transaktionerna enkla och snabba. Representanter för branschorganisationer inom handeln och finanssektorn menar att de i sin budget vanligtvis kalkylerar med förluster för bedrägerier. Många har egna bevakningssystem med hjälp av vilka ett stort antal bedrägerier kan stoppas i tid. När det inte lyckas ersätts kunder för eventuell förlust, men näringslivet håller ofta låg profil i bedrägerisammanhang för att skydda sitt varumärke. Vissa har på sina håll upplevt ett samband mellan ökad säkerhet och minskad försäljning.

Att kunna identifiera sig i samband med en transaktion, antingen elektroniskt eller i ett fysiskt möte, är en central fråga när det gäller att bekämpa bedrägerier. I dag kräver det oftast några extra steg, och enligt flera av de intervjuade kan närmast varje sekund vara avgörande för konsumentens val av säljsida.

En ökad säkerhet behöver dock inte nödvändigtvis betyda minskad service och försäljning. Som tidigare beskrivits testas nya tekniska lösningar redan, och skulle biometriska data användas i större utsträckning kan det innebära både säkra och smidiga processer. Framför allt behöver man öka medvetenheten hos företagen om deras sociala och etiska ansvar – något som diskuteras mer nedan. Samma sak gäller på de utbetalande myndigheterna, där parollen ”rätt utbetalning till rätt person” måste få prioritet framför en snabb utbetalning.

Inte enbart ekonomiska förluster

Även om bedrägeribrotten enligt lagen definieras utifrån ekonomisk vinning respektive skador är det uppenbart att dessa brott drabbar mer än enbart enskildas, företagens och statens

ekonomi. En person vars identitet har blivit stulen och använd i bedrägliga transaktioner behöver i dag exempelvis spendera åtskilliga timmar för att spärra sin identitet för kreditköp. Att bli utsatt för ett bedrägeri på sociala medier genom att någon utger sig för att vara en nära vän eller en potentiell kärlekspartner påverkar utan tvekan både den enskildes välmående, och i förlängningen riskerar även samhällets grundläggande tillitsstrukturer att ta skada. Enskildas tillit till företag, statens myndigheter och själva skattesystemet äventyras när förluster genom bedrägerier inte uppmärksammas och tas på allvar av de ytterst ansvariga. Självklart kan detta ha en (om än svårligen mätbar) negativ effekt också på handeln. Dessutom kan brottsvinsterna från bedrägerier används till att finansiera nya brott.

I ett internationellt perspektiv talas det om så kallad *corporate social responsibility* (CSR), eller ansvarsfullt företagande.[94] Med det menas att företagen har ett samhällsansvar som sträcker sig utöver det rent ekonomiska och även omfattar ett socialt och miljömässigt perspektiv. Innehållet i begreppet har med tiden vidgats och utifrån CSR:s principer diskuteras i dag även vikten av företagens ansvar att bekämpa bedrägerier och annan ekonomisk brottslighet. Med tanke på alla konsekvenser av bedrägerier, i kombination med att företag i vissa fall används som verktyg, är näringslivets ansvar uppenbart.

Många gråzoner och svåra gränsdragningar

En annan slutsats är att bedrägeribrottsligheten präglas av många gråzoner mellan det legala och det illegala. Som redan nämnts använder bedragare ofta legala företag för bedräglig verksamhet, exempelvis genom att ta över sådana företag med falska identiteter. Problemet med aggressiv telefonförsäljning, som framför allt äldre personer blir vilseledda med, utgör en annan gråzon. Här är det inte alltid självklart att avgöra om gärningen är ett brott eller under vilken lagstiftning händelsen annars ska hanteras (t.ex. civilrätt och marknadsrätt). Även lån mellan släkt och bekanta kan i vissa fall motsvara ett brottsbalksbedrägeri, medan de i andra fall kan resultera i en civilrättslig tvist.

Ett relaterat problem är att bidragsbrott sedan 2007 regleras enligt en särskild lag, men att en del närliggande bedrägerier mot välfärden fortfarande hanteras enligt kap. 9 brottsbalken. Något förenklat handlar det om förmåner som riktar sig till företag (exempelvis företagarstöd från Arbetsförmedlingen). Vissa assistansbedrägerier har dock varit svåra att placera i bidragsbrottslagen eller kap. 9 brottsbalken. Det är inte alltid enkelt att avgöra var gränsen går, och enligt intervjuade poliser och åklagare kräver

[94] http://ec.europa.eu/growth/industry/corporate-social-responsibility/

just denna del av tillämpningen en del klargöranden. Samtidigt ligger det i bedrägeribrottslighetens natur att avgränsningarna är svåra att göra, vilket visar på att gråzoner förekommer även inom själva brottsområdet.

Internetbruket gör att en stor del av brottsligheten inte heller kan avgränsas geografiskt. Starka internationella förgreningar är ett vanligt inslag; det har framkommit att många bedrägerier kan spåras utomlands, och dessa omständigheter påverkar möjligheter att klara upp brotten. Även på en nationell nivå kräver utredningar av dessa brott mer samordning än många andra brottstyper.

Förebyggande och brottsbekämpande förslag

På basis av undersökningens resultat ska nu förebyggande och brottsbekämpande förslag beskrivas. Det är långt ifrån en fullständig genomgång, eftersom aktörerna som bedriver förebyggande insatser mot bedrägerier är många. Här lyfts de åtgärder som är mest centrala i förhållande till vad som framkommit i denna kartläggning.

Brå har tagit intryck av modellen gällande situationell brottsprevention (Clarke 1997). Genom situationell brottsprevention försöker man förändra en situation så att bedrägerier framstår som svårare att begå. Kartläggningen har visat att bedrägeribrottslighetens nutida omfattning och karaktär är starkt förknippad med teknikutvecklingen (datorer, internet, elektroniska betalningssystem m.m.) och är en följd av ändrade samhälleliga rutinaktiviteter. Med rutinaktiviteter menas ”återkommande och vanligt förekommande aktiviteter som människor utför för att tillgodose sina behov” (Cohen och Felson 1979). Det som kallas för tillfällesstrukturen för brott har alltså påtagligt förändrats. Därför har vi fokuserat på åtgärder som primärt är inriktade på potentiellt kriminogena situationer snarare än på brottsbenägna individer.

Modellen inriktades till en början mot att försvåra stölder, inbrott och andra brott i den fysiska miljön. Med tiden har den dock börjat användas även mot brottslighet som kännetecknas av en högre komplexitet och avsaknad av en tydlig fysisk brottsplats. Det handlar om både ekonomisk och organiserad brottslighet (Lehtola och Paksula 2000, Bullock, Clarke och Tilley 2010, Korsell och Nilsson 2003, Brå 2007:4, Brå 2007:7, Brå 2007:23, Brå 2012:12). Därför har den bäring även på bedrägerier.

Enligt denna modell förebyggs brott genom fem principer:

- Öka den upplevda svårigheten att begå brott.
- Öka den upplevda risken med att begå brott.
- Minska den upplevda vinningen av brott.

- Minska risken för provokation.
- Motverka bortförklaringar som underlättar brott.

Det är framför allt de tre första principerna i modellen som appliceras i detta avsnitt om åtgärdsförslag. Nedan beskrivs Brås åtgärdsförslag i tre olika avsnitt; dels åtgärder som syftar till att förebygga bedrägerier, dels förslag på hur olika aktörer kan stoppa pågående bedrägerier och slutligen hur utredningar av dessa brott kan förbättras.

Förebygga bedrägerier

Ett av rapportens viktigaste resultat är att bedrägerierna är av sådana volymer att de inte enbart kan utredas bort, och trots särskilda satsningar inom rättsväsendet behöver flera aktörer ta sitt ansvar. Det gäller alltså att förebygga brotten, vilket inte minst kan ske genom att de potentiellt utsatta blir mer vaksamma och medvetna om hur bedrägerier kan gå till. Även näringslivet och myndigheter utanför rättsväsendet har en central roll när det gäller att motverka bedrägeribrott.

Förbättra kunskapen om hur man skyddar sig mot bedrägerier

Som tidigare nämnts är bedrägerier ett mycket föränderligt område, och att informera om nya bedrägeriupplägg bör därför vara en central åtgärd för att minska denna brottslighet. Information till potentiella utsatta, både enskilda och företag, är ett viktigt verktyg överlag. Det kan vara en särskilt viktig åtgärd när det gäller bedrägerier som begås av mindre rationella gärningspersoner som inte reflekterar över upptäcktsrisken.

Genom att öka kunskapen om hur bedragare agerar och hur normala transaktioner och affärer ser ut minskar man rimligtvis risken för fullbordade bedrägerier. Potentiella brottsoffer kan exempelvis informeras om att vara försiktiga med att öppna mejl från okända adresser, om hur man bestrider bluffakturor eller att vara mer restriktiva vid hantering av sina person- eller kontouppgifter och information om sig själva på sociala medier.

Behovet av ett samlat grepp konstaterades efter en stor ökning av bedrägeribrotten under de senaste åren, varför polisens Nationella bedrägericenter (NBC) öppnades under våren 2014. En stor del av centrets arbete består i att informera allmänheten om vilka bedrägerier som sker och hur enskilda kan skydda sig. NBC har också kontakt med näringslivet, myndigheter och bankväsendet för att påverka bedrägeribrott som inte enbart riktas mot privatpersoner utan även företag och den offentliga sektorn.

Handeln har exempelvis byggt upp varningslistor under senare år, där information om företag med tveksam verksamhet finns sammanställd. Detta är rimligen ett viktigt verktyg för att förebygga exempelvis fakturabedrägerier eller andra bolagsrelaterade brott. Ytterligare exempel kommer från näringslivet, där företagarorganisationer sprider lathundar, goda exempel och försöker öka kunskapen om bedrägerimodus. En statlig utredning (SOU 2015:77) betonar Konsumentverkets upplysningstjänst som en naturlig informationskälla gällande bl.a. fakturabedrägerier.

Det finns med andra ord gott om exempel på aktörer som försöker sprida information om nya bedrägeriformer. En risk med de många aktörerna är dock att informationen blir oöverskådlig för den enskilde. Det vore en klar fördel om dessa initiativ kunde samordnas och det avsattes särskilda resurser för att skapa en gemensam plattform som sammanställer den senaste informationen och exempelvis länkar till viktiga aktörers hemsidor.

Identitetsfrågan behöver ses över

Säker ursprungsidentifiering

I kapitlet om identitetsmissbruk framgår att det finns problem dels med falska identiteter, dels med att verkliga personers identiteter utnyttjas för bedrägerier. En av de viktigaste viktigaste åtgärderna i identitetsfrågan är att garantera säker ursprungsidentifiering. Det har också lyfts i en rad rapporter (Skatteverket 2014) och skrivelser från näringslivet till regeringen.[95]

När personer registreras hos Migrationsverket eller Skatteverket bör det finnas starka ambitioner att skapa en ytterst säker koppling mellan en person och en identitet, det vill säga minimera risken för multipla identiteter. Trots medvetenheten om problemet med identitetsmissbruk saknar myndigheterna verktyg för att motverka det. Det skulle krävas regeländringar för att exempelvis Skatteverket – när de upptäcker falska identitetshandlingar – ska få ta dem i beslag. Exempel finns på att myndigheter behövt lämna tillbaka falska identitetshandlingar trots starka misstankar.

Vid misstanke om felaktiga identitetshandlingar sker det ibland en polisanmälan från den upptäckande myndigheten. De saknar dock anmälningsplikt och upplever, enligt intervjuer, osäkerhet om lagstöd. Det kan därför finnas ett behov av att förtydliga eller skapa lagstöd. Förslaget om att kriminalisera olovlig identitetsanvändning (bilaga 5) träffar inte bruket av helt falska identiteter, som inte innebär ett intrång i en existerande persons identitet. I detta fall är åtgärder riktade mot en säkrare ursprungsidentifiering en mer angelägen strategi.

[95] T.ex. Svenska Bankföreningen 2015-06-22, KRONAN Säkerhet AB, 2015-04-18.

Biometriska data

Biometriska data har av de intervjuade beskrivits som den mest effektiva metoden för att både garantera säker ursprungsidentifiering och förbättra identitetskontroller.[96] Även om frågan kan ses som kontroversiell ur integritetssynpunkt, har biometrisk identifiering redan börjat användas i ett stort antal länder, och i vissa sammanhang även i Sverige (pass, mobiltelefoni m.m.). Den globala trenden gällande identifieringstekniken tycks gå mot en ökad användning av biometriska data och fler möjligheter bör med fördel utforskas även i Sverige.

Biometriska data kan användas både för att få säkrare identitetshandlingar men även vid exempelvis kortbetalningar,[97] något som troligtvis kan minska antalet bedrägerier. Användning av liknande teknik är både säkrare ur identitetssynpunkt och snabbare och smidigare för kunden som inte behöver memorera sin kod – ett exempel på att säkerhetsåtgärder inte nödvändigtvis behöver bromsa upp ekonomiska transaktioner.

Behov av en central ansvarig aktör i identitetsfrågan

Som framgår av kapitlet om Identitetsmissbruk finns ett 15-tal godkända identitetshandlingar i Sverige. Det försvårar identitetskontroller, särskilt inom handeln och på utlämningsställen. Vissa handlingar är också lättare att förfalska än andra.

Flera berörda aktörer framför önskemål om färre identitetshandlingar och en myndighet som får ansvaret i identitetsfrågan. Svenska Bankföreningen har till regeringen (Ju2015/05176/L4) föreslagit att staten bör ta på sig ansvaret för en nationell gemensam utfärdandeprocess av svenska identitetshandlingar, och då i samtliga faser: genom krav på ansökningsprocess genom personlig inställelse, bakgrundskontroll av den sökande, tillverkningsprocess av kortet, utlämningsprocess med personlig inställelse och möjlighet att verifiera äkthet av utgivna identitetshandlingar genom sina myndigheter. En sådan åtgärd skulle alltså vara riktad mot att både säkra den tidigare nämnda ursprungsidentifieringen och att underlätta framtida kontroller. Enligt flera intervjuade är ansvarsfrågan grundläggande när det kommer till identitetsmissbruk och en central ansvarig aktör är därför önskvärd.

Förändrad roll för folkbokföringen

Förekomsten av dubbla och felaktiga identiteter genererar inte enbart bedrägerier utan försvårar också brottsutredningar. En

[96] Biometri är den teknik som gör det möjligt att bearbeta en persons fysiska särdrag, exempelvis dennes fingeravtryck, ansikte eller ögon, till en unik digital profil (SOU 2007:100).

[97] I Norge används exempelvis redan kontaktlösa kort i kombination med fingeravtryck (se kapitlet Identitetsmissbruk).

tidigare studie beskriver problemen med det rådande systemet där felaktiga personnummer till följd av spårbarhetskrav ligger kvar (Brå 2015:8). Det finns en uppenbar risk att en myndighet eller kreditprövningsaktör som stämmer av uppgifter uppfattar identiteten som korrekt när den finns registrerad hos Skatteverkets folkbokföring.

Eftersom många bedrägerier möjliggörs av felaktiga folkbokföringar är det viktigt att säkerställa att uppgifterna i databasen är av hög kvalitet. Folkbokföringen har av tradition sett sig som en registrerande verksamhet och har små resurser och få möjligheter att genomföra kontroller. Brå har i andra sammanhang föreslagit att folkbokföringen får en mer granskande och utredande roll. För detta krävs ytterligare verktyg, exempelvis en möjlighet att ge sig ut och besöka ”misstänkta” adresser (jfr SOU 2008:74, Brå 2015:8). Eftersom besök på fältet är resurskrävande är det viktigt att verktygen används vid tämligen konkreta misstankar om fel. Det kan exempelvis handla om att åka ut och dokumentera att en på pappret orimlig folkbokföring är felaktig – t.ex. visa att det är en industrilokal eller att ytan är för liten för ett hushåll för alla som är folkbokförda där.

Säkrare utlämning av personuppgifter

En annan viktig åtgärd, som också berör folkbokföringen, gäller rutinerna kring utlämning av personuppgifter. Många intervjupersoner menar att det är alldeles för enkelt i Sverige att få tag på sådana uppgifter gällande en annan person. De intervjuade menar att en mer restriktiv syn på utlämning av personuppgifter skulle förhindra en stor del av identitetsmissbruk och att detta inte kräver någon ändring i grundlagen, utan en ändring av tillämpliga sekretessbestämmelser. En översyn av rutiner kring hantering av personnummer och hur dessa regleras bör alltså, mot bakgrund av ökande antal identitetsstölder, vara aktuell.

En ökad sekretess kring hantering av personnummer skulle självklart innebära att sedan länge etablerade rutiner behöver förändras. Den tekniska utvecklingen framskrider dock med hög hastighet, med nya möjligheter men också ny sårbarhet. Det är därför viktigt att samhällets olika funktioner anpassas till nya trender och garanterar identitetsskydd utifrån de nya förutsättningarna.

Näringslivets ansvar

Som klarlagts har näringslivet en mycket viktig roll i hantering av bedrägerifrågan, då företag kan fungera som både verktyg och möjliggörare för många bedragare. Vilja till förebyggande åtgärder borde även motiveras av att näringslivet lider stora förluster orsakade av bedrägeribrott.

Säkra kortbetalningar – en av de stora utmaningarna
Bedrägerier med stulna kort eller kortuppgifter utgör ett särskilt problemområde, präglat av motstridiga utvecklingstrender mot både större säkerhet och transaktioner som inte kräver en identifiering. Kortbedrägerier, i synnerhet utan det fysiska kortet (CNP), har enligt alla befintliga källor ökat markant under den senaste tiden, och är svårast att förebygga.

Intervjuade representanter för rättsväsendet menar att e-handeln och bankväsendet behöver ta ett större ansvar på området, förslagsvis genom att kräva identifiering med e-legitimationer vid köp. Sådana säkra internetbetalningar behandlas i ett reviderat EU-direktiv (PSD2) som publicerades i slutet av 2015 (se bilaga 6).[98] Syftet är att utöka kraven på så kallad stark kundautentisering som går ut på identifiering med hjälp av en kombination av flera faktorer, däribland biometriska data. De intervjuade menar dock att även om direktivet innebär en större säkerhet generellt så driver den samtidigt på den fortsatta avregleringen av betalmarknaden, med nya aktörer som direkt kan få tillgång till person- och kontouppgifter. Kunderna slipper då exempelvis att registrera sina kontouppgifter vid varje köp, vilket kan utgöra nya risker.

De större bankerna möjliggör att kunderna själva lägger en spärr på sina kontokort för internetköp eller köp utomlands (s.k. geoblocking). Kunden kan då via en bank-app tillfälligt öppna kontokortet enbart vid önskat köp. Lösningen har dock en del begränsningar; förutom att inte alla banker i dag erbjuder tjänsten har vissa utländska företag en spärr på kontokortet; det omöjliggör betalningar via autogiro när det gäller en rad omtyckta tjänster (t.ex. Spotify eller Netflix). Om dessa rutiner utvecklas kan de få en viktig förebyggande effekt både inom och utanför Sverige.

Låt rätt aktör ta ansvaret vid bedrägerier
Inte minst vid olika kort- och kreditbedrägerier kan det ekonomiska ansvaret för ett fullbordat bedrägeri landa på flera olika aktörer. Som framgår av kapitlet om Näringslivets roller kan det handla om en privatperson, kortutgivaren, inlösaren, utlämningsstället, fraktleverantören eller kreditgivaren. I praktiken innebär det att banker och kortutgivare får ta det ekonomiska ansvaret för många bedrägerier, förutsatt att övriga aktörer har följt sina säkerhetsrutiner. En risk med ett sådant system är att få aktörer är motiverade att utveckla sitt säkerhetsarbete och kunden till att minimera det personliga risktagandet. Utlämningsställen och

[98] Europaparlamentets och rådets direktiv (EU) 2015/2366. Medlemsstaterna har till den 13 januari 2018 på sig att anta och offentliggöra de bestämmelser som är nödvändiga för att följa direktivet. (Europeiska unionens officiella tidning, L 337/35. 2015/12/23).

säljare inom handeln behöver exempelvis få fler incitament att genomföra noggranna kontroller.

Ytterligare en risk med att näringslivet delar på ansvaret och inte redovisar sina kostnader till följd av bedrägerier, är att konsumenterna inte ser att de också drabbas. Det sker främst genom ökade kostnader för varor och tjänster, som täcker upp för bedrägeriförlusterna. Information om det kan öka viljan att använda säkrare betalningslösningar – även om det tar några sekunder längre tid – och viljan att skydda sina kortuppgifter bättre.

Att stoppa brott i början av fraktkedjan: Känn din kund!

Brås granskning visar att tre fjärdedelar av polisanmälda bedrägerier innehåller ett modus som kan kopplas till någon form av köp- eller säljprocess. Nyckeln till att förebygga många bedrägerier är, enligt intervjupersoner, att ha god kundkännedom.

Goda exempel kommer från de stora kreditprövnings- och betalaktörerna som har utvecklat sina kontroller. Tack vare att de har stora betalningsflöden har de helt andra möjligheter än ett litet företag inom handeln att skilja på normala transaktioner och misstänkta bedrägerier. Det innebär väsentligt större möjligheter att lära känna sin kund. Vissa aktörer styr över risktransaktioner till andra betalnings- och leveranssätt. Exempel på risktransaktioner är höga belopp, ovanligt köpmönster för aktuell kund eller att köpet gäller vissa typer av varor som är attraktiva för bedragare. Följden blir att den aktuelle kunden inte kan välja fakturabetalning utan måste betala direkt med kort, eller att varan skickas med avisering till folkbokföringsadressen via brev i stället för med sms till uppgivet mobilnummer. Detta är åtgärder som fler aktörer skulle kunna använda.

Samtidigt visar denna undersökning att intresset riktas mer mot kontroller i ett senare skede, främst när beställda varor lämnas ut. Att stoppa bedrägerier så tidigt som möjligt, redan vid beställningen, bör vara angeläget, men diskuteras sällan. Satsningar på säker e-handel bör utgöra en större del av det förebyggande arbetet mot bedrägerier i fraktkedjan, både genom exempelvis ökad e-legitimering och genom att utveckla riskprofileringen.

Intervjupersoner inom näringslivet uttrycker behov av ett större utbyte med varandra, för att uppdatera sina riskprofiler och bättre identifiera bedrägerier. Detta är särskilt angeläget eftersom potentiella kunder kan drabbas om deras identiteter missbrukas i bedrägerier. Här sätter dock sekretessbestämmelser, konkurrensfrågor och integritetsskydd gränser. Samtidigt riskerar det att bli en konkurrensfråga eftersom de större aktörerna har helt andra möjligheter att göra goda kreditprövningar än de små – enbart eftersom de har mer egen data om köptransaktioner. Hur kredit-

branschen och handeln ska kunna arbeta mot bedrägerier på ett mer ändamålsenligt sätt är därför en fråga som lagstiftningsmässigt bör ses över. Exempelvis i England har näringslivet genom organisationen Cifas helt andra möjligheter att dela information i just detta syfte.

Kontroller före utbetalningar av lån och bidrag

Kreditbedrägerier och välfärdsbedrägerier har en sak gemensamt. De upptäcks ofta först en tid efter att betalningen ägt rum, och det är då svårt att återkräva pengarna. De större kredit- och långivarna försöker att helt stoppa bedrägliga affärer. Exempel på sådana åtgärder är att göra grundliga identitetskontroller genom att ställa frågor till personen, inte enbart titta på handlingarna.

Samma utmaning möter de utbetalande myndigheterna och organisationerna. En brist bland de utbetalande aktörerna är att fokus – särskilt bland de polisanmälda brotten – ligger på fall där bidrag redan betalats ut felaktigt. Kontrollerna sker alltså primärt i efterhand. Intervjupersoner och tidigare studier betonar vikten av kontroller före utbetalning, eller i vart fall innan skadan hunnit bli alltför stor. Det kräver dock att förmånshandläggarna ges kunskap och tid att upptäcka felaktigheter. Till detta kommer ett mer strukturerat kontrollarbete, med urvalsprofiler, riskanalyser och mönstersökningar. Flera myndigheter arbetar i den riktningen, men det är framför allt de större utbetalande myndigheterna som har tillräckliga resurser och datamängd.

Behovet av kontroller före utbetalning är särskilt stort när förmånen riktar sig till företag. Här talar intervjuerna för att förmånshandläggaren bör ställa frågor som: Vem äger företaget och vad har denne för relation till den anställde som ska ha bidrag? Finns ekonomiskt utrymme i bolagen för (de höga) lönerna? Är bolaget nystartat? Matchar omsättningen antalet anställda? Finns en reell verksamhet? Hur ser företaget ut i Skatteverkets register?

Branschsamverkan i säkerhetsfrågor

Viss samverkan och utbyte av information sker redan inom näringslivet. Flera av bedrägerier berörda branscher har forum eller branschorganisationer där säkerhetsansvariga träffas. Samtliga intervjupersoner som ingår i något sådant sammanhang betonar vikten av dessa möten, inte minst för att snabbt identifiera nya brottstrender och modus.

Genom att konkurrenter enas om en standard i säkerhetsfrågor blir det ingen konkurrensfråga och därmed lättare att få även den mest försäljningsinriktade företagsledningen att intressera sig för säkerhet. Det beskrivs som avgörande för att företagen ska vidta åtgärderna. Branscher som inte har några samverkansforum och

företag som inte ingår i en branschorganisation har å sin sida mycket att vinna på att inleda samarbeten eller kopiera säkerhetslösningar. I annat fall finns en risk att de drabbas hårdare av brottsligheten, eftersom de kan uppfattas som lättare måltavlor. Intervjuerna med gärningspersonerna talar också för att det snabbt sprider sig vilka företag som ligger efter med säkerhetsarbetet.

Myndigheternas förebyggande insatser

Olika myndigheter har också stor potential att förebygga bedrägerier. Det har redan tydligt framkommit när det gäller hanteringen av identitetsfrågor. Här presenteras ytterligare några förslag gällande både rättsväsendets och andra myndigheters arbete.

Behov av regelförenklingar

Ärendegranskningen innehåller ett par exempel där det av nedläggningsskälen framgår att polis och åklagare tycker att de utbetalande myndigheterna och organisationernas regelverk är krångligt. Även andra studier framhåller att regelförenklingar är nödvändiga (SOU 2008:74, Brå 2015:8). Vissa förmåner är gamla och utformades för en annan tid med fastanställningar hos samma arbetsgivare och offentliga aktörer snarare än privata företag inom välfärdssektorn. Idag är det inte helt lätt för den sökande att få in sin situation i regelverkens mallar, enligt vad som framgår i några ärenden. När regelverken består av vissa med varandra överlappande bidrag är det inte alltid självklart vilket bidrag den sökande egentligen ska ha. Det faktum att vissa bidrag överlappar varandra gör också behoven av informationsutbyte särskilt stora.

Om de oavsiktliga felen är många tar det resurser från ärenden med välfärdsbedrägerier. När de oavsiktliga felen minimeras blir det också enklare att skilja brotten från bristfällig handläggning och otydliga och dåligt pålästa sökande. Därför bör utbetalande aktörer, deras departement och statliga utredningar i ämnet sträva efter att identifiera överlappningar och glapp i regelverk och föreslå regelförenklingar.

Tillgångsinriktad brottsbekämpning

Som framgår av kapitlet om Brottsutsatta och gärningspersoner är vissa bedrägerier mycket lönsamma. Att minska lönsamheten blir därför en central förebyggande åtgärd. Även om gärningspersonen blir gripen och lagförd är intrycket att det sällan görs stora beslag av pengar. Det är därför viktigt att arbeta med tillgångsinriktad brottsbekämpning för att få tag i så mycket av brottspengarna som möjligt. En framkomlig väg som lyfts av några intervjupersoner är att använda penningtvättslagstiftningen. Eftersom sådana brottsutredningar bygger på att följa transaktio-

ner kommer man närmare pengarna. Dessutom kan Finanspolisens kompetens om penningtvätt utnyttjas. Ytterligare ett motiv är att det går att få tillbaka målsägandes pengar, när man följer transaktion för transaktion och säkrar pengarna innan de lämnat ”kontovärlden” och försvunnit.

Nyckeln till att bedriva tillgångsinriktad brottsbekämpning är att parallellt med utredningen arbeta med tillgångsutredare eller revisorer som har kompetens att följa penningströmmarna. Hur detta kan gå till förklaras närmare i rapporten *Gå på pengarna*, där praktiker förklarar hur man arbetar tillgångsinriktat i underrättelse- och utredningsarbete (se Brå 2014:10).

Försvåra att använda företag som brottsverktyg

Som framgår inte minst av kapitlet Näringslivets roller används företag för att begå storskaliga bedrägerier. Det är angeläget att försvåra denna användning. (För en bredare analys av detta problem och fler förslag se Brå 2016:7).

För att förebygga kapning av bolag och att bolag bildas enbart för att användas för brott föreslås att Bolagsverket får en mer granskande roll och inte i första hand är en registrerande myndighet (Brå 2016:7, jfr Brå 2015:22). Det är också viktigt att Bolagsverket och andra relevanta aktörer, som Skatteverket, Ekobrottsmyndigheten, polisen och branschorganisationer tar fram checklistor på varningsindikatorer. Detta för att företagen som används som brottsverktyg ska identifieras innan bedrägerierna blir för omfattande.

Även myndigheter som arbetar med tillsyn och kontroll spelar en viktig roll för att stänga ute bedrägliga företag. Redan nu sker en granskning innan assistansföretag får tillstånd att bedriva verksamhet. Hur sådan vandelsprövning och andra administrativa åtgärder kan användas för att förebygga brott utvecklas i en annan rapport (se Brå 2015:15).

Nya brottskoder för att bättre följa utvecklingen

Brås resultat bekräftar det som aktörer inom rättsväsendet lyfter som ett problem, nämligen att de brottskoder som används i kriminalstatistiken inte ger en användbar bild av utvecklingen av anmälda bedrägeribrott. När det gäller brottskoden ”bedrägeri med hjälp av internet” ingår exempelvis både bedrägerityper som är relativt enkla att klara upp (annonsbedrägerier) och bedrägerier som är mycket svårare att utreda (kreditbedrägerier, kortbedrägerier, övriga telefon- och internetbedrägerier). Den aktuella indelningen av brottskoderna innebär därmed att det blir svårt att överblicka de typer av bedrägeribrott där utredningsinsatser fungerar bra och de typer där det kan behövas utvecklingsåtgärder. Mer ändamålsenliga brottskoder skulle dels ge rättsväsendets

aktörer möjlighet att lättare följa utvecklingen i anmälningsstatistiken, dels ge möjlighet att följa utvecklingen av polisens och åklagarnas utredningsprestationer. Det skulle ge bättre underlag för att identifiera områden som kan behöva prioriteras. Samtidigt måste behovet av nya brottskoder vägas mot vissa nackdelar, exempelvis ett avbrott i tidsserierna över de anmälda bedrägeribrotten.[99] En översyn av bedrägeribrottskoderna skulle rimligen ske i ett nära samarbete mellan Brå, som har ansvar för den officiella kriminalstatistiken, och Polisens Nationella bedrägericenter.

Hämta uppgifter från säkraste källan

Service och kontroll uppfattas ofta som oförenliga processer. I själva verket kan de kombineras. Det blir som allra tydligast när myndigheter får hämta uppgifter från säkraste källan, direkt från arbetsgivaren, läkaren eller banken i stället för att förlita sig på uppgifter som går via den sökande.

Arbetslöshetskassorna har, för att underlätta för arbetsgivare och sökande, infört en arbetsgivarportal (www.arbetsgivarintyg.nu). Syftet är att minska oavsiktliga fel och underlätta för arbetsgivaren att fylla i intyget – genom att denne får stöd av webbverktyget. Av intresse för denna rapport är att det samtidigt försvårar för den sökande att själv förfalska arbetsgivarintyg. Försäkringskassan har ett liknande system som omfattar en hög andel läkare och läkarintyg. Sådana system som bygger på en form av e-legitimation visar vilka uppgifter som kommer direkt från intygsgivaren.

Eftersom vissa intyg är ytterst osäkra finns ett intresse bland utbetalande myndigheter och organisationer att få del av kontouppgifter från banker (Brå 2015:8, jfr SOU 2008:74). I stället för en oklar hyresavi går det då att genom överföringar se exakt vad personen har betalat i hyra. Försäkringskassan har möjlighet att direkt från banken hämta kontoutdrag för bostadsbidrag och bostadstillägg. Eftersom även vissa arbetsgivarintyg uppfattas som osäkra finns ett behov av att även få uppgifter från banker om löneutbetalningars storlek.[100] Banksekretessen är stark och det finns goda skäl för det. Lagstiftaren bör dock prioritera så att det verkligen är de mest centrala uppgifterna som får hämtas direkt från banken.

[99] Vidare är det planerat att avveckla det nuvarande systemet med brottskoder i samband med det så kallade RIF-arbetet (Rättsväsendets informationsförsörjning) – ett pågående arbete som syftar till att med stöd av it utveckla ett förbättrat informationsutbyte i brottmålshanteringen. Se vidare http://www.bra.se/bra/brott-och-statistik/statistik/rif---battre-informationsutbyte-i-rattskedjan.html

[100] Ytterligare ett sätt att komma närmare dessa betalningar är att införa inkomst på individnivå per månad, s.k. månadsuppgift (se vidare Brå 2015:8).

Överväg direktåtkomst av fler uppgifter för de utbetalande myndigheterna

Som framgått av kapitlet om Utbetalande myndigheter och organisationer söker vissa som ett led i en mer effektiv kontrollverksamhet riskbaserade urval och försöker samköra uppgifter med varandra, i den mån regelverken tillåter. Vilka myndigheter som får hämta vilka uppgifter är dock något slumpmässigt (se vidare Brå 2015:8). Det finns därför ett behov av en översyn av databas- och registerlagstiftningar med ett samlat grepp för välfärdssystemets olika myndigheter och organisationer. Där bör det också övervägas att utvidga direktåtkomst till fler förmånssystem hos fler myndigheter och organisationer.

Stoppa pågående bedrägerier

Rapporten visar att många bedrägerier sker systematiskt och i organiserade former. Det genererar stora mängder målsägare, liksom – vid välfärdsbedrägerier – många felaktiga utbetalningar. Därför är en central brottsbekämpande strategi att försöka identifiera dessa brott när de pågår och stoppa dem så tidigt som möjligt.

Att underlätta identitetsspärr

Ett problem som beskrivits i flera intervjuer är de konsekvenser som stulna identiteter innebär för den drabbade. Personen behöver spärra sin identitet för kreditköp, vilket är en tidskrävande process som innebär många samtal till olika aktörer. Det pågår för närvarande ett projekt på UC AB (f.d. Upplysningscentralen) som syftar till att skapa en samordningsfunktion så att de som drabbas av identitetsstöld enbart ska behöva ringa ett samtal.

Alternativa lösningar till identitetsspärr kan också övervägas, som inte innebär samma begränsning för den som utsatts för identitetsstöld. I Storbritannien har personer som fått sin id-handling stulen eller identitetsuppgifter kapade en möjlighet att kontakta en organisation (Cifas) för att markeras med en varningsflagg. Denna varningsflagg innebär att om någon söker exempelvis ett lån i en persons namn hämtas uppgiften att denne har en varningsflagg. Det innebär att kreditinstitutet kontaktar personen genom de kontaktuppgifter denne lämnat till Cifas, och inte dem som angetts på låneansökan. Handläggningstiden kan fördröjas med någon arbetsdag, men det förekommer att bedrägerier genom detta system förhindras, samtidigt som ingreppet i den enskildes vardag blir betydligt mindre än med det svenska spärrsystemet. Det vore värt att utreda frågan om en liknande lösning i Sverige.

Arbeta mer underrättelsebaserat mot bedrägerier

Ett problem som lyfts fram i intervjuer med såväl företrädare för rättsväsendet som näringslivet är att komma åt de mest aktiva gärningspersonerna. Som framgått av ärendegranskningen kan en del seriebedragare stå för ett stort antal brottsmisstankar. Den bilden bekräftas även av flera intervjupersoner. När det handlar om organiserade bedrägerier lyckas man ofta i bästa fall avlägsna målvakter och medhjälpare ett tag, medan vissa huvudmän är svåra att identifiera och utreda.

När det gäller brottsbekämpning finns en väsentlig skillnad mellan bedrägerier och andra ekobrott. Vid exempelvis skattebrott har Skatteverket och Ekobrottsmyndigheten ansvar, två myndigheter som har egna resurser att driva underrättelseverksamhet mot just denna brottstyp. Det ger ett betydligt bättre underlag för att kartlägga och förstå vilka gärningspersoner som är mest aktiva. Något liknande saknas på bedrägeriområdet.

Om företag används ligger ärendet nära Ekobrottsmyndighetens område. Även Skatteverket kan identifiera liknande brottsupplägg. Polismyndigheten har vid sidan av en mängd mer prioriterade brott också bedrägeribrotten, men inte om ingången blir bokföringsbrott och skattebrott. Åklagarmyndigheten har samma problem som polisen. De utbetalande myndigheterna kan vara drabbade, men har svårt att utreda, särskilt de mest kvalificerade brotten. Näringslivet kan se mönster i sin utsatthet, men har också svårt att agera och utreda vilka som ligger bakom brotten. Några företrädare för näringslivet ger också uttryck för att de gärna skulle lämna data till polisen. Detta för att en aktör skulle få en helhetsbild och bättre kunna analysera brottsligheten. Som framgår av rapporten pågår ett samarbete mellan NBC och NOA inom polisen för att effektivisera polisens eget arbete med underrättelseinformation gällande bedrägeribrott. Sådana insatser behöver förstärkas och systematiseras.

En inspirationskälla kan vara Storbritannien där man infört att alla polisanmälningar kommer in via ett särskilt anmälningssystem för bedrägeribrott, Action Fraud. I detta enorma flöde av uppgifter bearbetas data även i de fall en utredning inte inleds. Det skapas alltså en form av underrättelsedatabas med uppgifter så att det går att analysera flödet av misstänkta bedrägerier. Samma databas innehåller också vissa uppgifter från näringslivet, som lämnas över av organisationen Cifas.

Ett särskilt argument för att arbeta mer underrättelsebaserat med bedrägerier rör de ärenden där företag används. Brottsvinsterna finns under en tid i bolaget men tas sedan ut. Här gäller det för myndigheterna att identifiera bolagen innan pengarna är borta

tillsammans med organisatörerna och enbart målvakten – som inte kan svara på några frågor – är kvar.

Agera även mot interna bedrägerier

Många av de intervjuade säkerhetsansvariga inom näringslivet berör också insider-temat, det vill säga bedrägerier där gärningspersonen eller medhjälparen är en anställd inom företaget. Av intervjuerna framgår att olika företag och organisationer har olika syn på interna brott. Vissa menar att de polisanmäler allt och att sådana brott särskilt ska beivras. Andra menar att det ibland tystas ner och löses ”smidigt” genom att personen säger upp sig. Ett problem med denna strategi är att samma person kan fortsätta sin brottslighet hos en ny arbetsgivare (Brå 2014:4). Interna brott kan exempelvis ligga bakom en del kortbedrägerier och fakturabedrägerier.

Det är därför viktigt att företag och organisationer prioriterar de interna brotten. Sådana rutiner bör vara en självklar del av de tidigare nämnda CSR-principerna gällande företagsetik. Det handlar både om förtroendet för organisationen – att man tar brott på allvar – och att de interna brotten ofta kan röra mycket stora belopp, högre än vid de externa bedrägerierna.

Öka informationsutbytet mellan myndigheterna

Denna undersökning visar att det finns en efterfrågan på ett mer effektivt sätt att utbyta information vid misstanke om identitetsmissbruk. Ett problem som lyfts av intervjupersoner samt en myndighetsgemensam kartläggning (NUC 2015a) är att det krävs samsyn mellan myndigheterna. Ett hinder är att sekretessreglerna tolkas olika av myndigheterna. Ett exempel på lösning finns vid välfärdsbedrägerierna, i form av lagen om underrättelseskyldighet.

Använd och utvidga lagen om underrättelseskyldighet

Vid bidragsbrott gäller lagen om underrättelseskyldighet (SFS 2008:206). Den rör dock enbart ekonomiska bidrag till *enskilda* och träffar därför inte företagens välfärdsbrott. Brå föreslår att lagen om underrättelseskyldighet utvidgas till att omfatta alla bidrag i välfärdssystemet. Brå har tidigare framfört att man bör överväga att ha samma regler för socialtjänsten som för övriga utbetalande verksamheter (se vidare Brå 2015:8). Av särskilt stor betydelse är att inkludera stöden till företagare (jfr SOU 2008:74, SOU 2014:16, Riksrevisionen 2011). Även lönegarantin bör omfattas av lagen.

Genom att tydliggöra regelverket kan Skatteverket och andra myndigheter som upptäcker välfärdsbrott begångna av företag lättare lämna denna information till den utbetalande myndigheten eller organisationen. Detta utan att behöva göra särskilda överväganden genom den generalklausul som finns i 10 kap. 2 § offentlighets- och sekretesslagen (2009:400). Det skulle kunna innebära fler impulser[101] och göra det tydligare att alla välfärdens bidrag har samma skydd.

Dessutom skulle lagen kunna användas i större uträckning (Brå 2015:8). De utbildningsinsatser som genomfördes när lagen om underrättelseskyldighet var ny fick antalet impulser att öka kraftigt (Brå 2015:8). Det finns återigen ett behov av sådana utbildningsinsatser. Handläggarna behöver få tydliggjort vilka möjligheter som finns att lämna impulser. Utmaningen är att beskriva exempel som är relevanta och uppkommer i deras arbete och vilken information de i sådana situationer får lämna vidare. Inte minst de utbetalande myndigheternas jurister, och för kommunernas del Sveriges kommuner och landsting, kan här hjälpa till att formulera exempel.

Förbättra utredningarna av bedrägerier

Att förebygga och stoppa pågående bedrägerier är utan tvekan de åtgärder som behöver prioriteras och resursförstärkas. Hur stora ambitioner man än har på dessa områden kommer dock brotten i viss utsträckning alltid att äga rum och kommer att behöva hanteras av rättsväsendet. Nedan presenteras förslag på hur rättsväsendet kan förbättra brottsutredningarna.

Bättre polisanmälningar från utbetalande myndigheter

Att kvaliteten varierar mellan polisanmälningar från olika utbetalande myndigheter och organisationer är tydligt av Brås genomgång. I ett ärende antecknar polisen att de inte förstår hur den utbetalande organisationen har räknat. I andra fall har man en tydlig mall som beskriver gärningen och varför man misstänker uppsåt. Utbetalningarna finns i tydliga tabeller. För att få en högre och jämnare kvalitet på polisanmälningarna bedriver NBC i skrivande stund ett metodstödsarbete. För närvarande pågår försöksverksamhet med Försäkringskassan i Stockholms län om att höja kvaliteten och att skicka anmälningarna till polisen via e-post. Försöket kommer att utvärderas under första kvartalet 2016.

[101] Det vill säga en signal om misstänkt felaktighet.

Utöka polisens samordning för att förbättra utredningar

Flera intervjupersoner från både näringslivet och rättsväsendet betonar att det har skett stora förbättringar i polisens samordning av bedrägeriärenden, samt att en polismyndighet och ett nationellt utredningssystem (DurTvå) kommer att bidra med ytterligare möjligheter till förbättringar. Bakgrunden är att personer som begår systematiska bedrägerier sällan begränsar sig till en fysisk plats, vilket blir särskilt tydligt vid de många internetrelaterade bedrägerierna. Tidigare kunde gärningspersonerna dölja sig i flödet av alla bedrägerianmälningar, men med dagens system kan polisen söka efter ärenden som rör en specifik misstänkt gärningsperson och ett specifikt bankkonto som tagit emot överföringar. Det ger möjligheter att koppla ihop ärenden och se systematiken. Dessutom kan grövre brottsrubriceringar bli aktuella när helheten syns och kan utredas. Att förbättra samordningen har också varit ett av syftena med att skapa NBC.

Brå ser det som viktigt att inte släppa frågan om samordning, utan att den snarare bör intensifieras nu när möjligheterna blivit större.

Identifiera åtgärder som kan effektivisera hanteringen av stora utredningar

Vissa bedrägerier resulterar i stora mål som är mycket krävande för rättsväsendet att hantera. Enligt granskningen gäller det särskilt fakturabedrägerier, assistansbedrägerier och vissa kortbedrägeriärenden. Samma problematik finns i kreditbedrägerierna, även om systematiken inte blir fullt lika tydlig i de ärenden som granskats av Brå.

Vid fakturabedrägerier skulle införandet av brottet grovt fordringsbedrägeri enligt Egendomsskyddsutredningens förslag innebära stora effektiviseringsvinster för rättsväsendets hantering av dessa mål. Det handlar om ett förslag att kriminalisera betalningsuppmaningar som i vilseledande syfte riktas till en vidare krets och som avser betydande värden. Brottet skulle vara fullbordat redan då gärningspersonen avsänt eller på annat sätt förmedlat meddelanden till mottagarna, utan något krav på att de mottagit meddelandena. Detta skulle bland annat innebära att man inte längre behövde styrka ett vilseledande enligt bedrägeribestämmelsen i förhållande till var och en av dem som utsatts för ett storskaligt fakturabedrägeri.[102]

Vidare har vissa åtgärder för att effektivisera handläggning av stora utredningar föreslagits av exempelvis Åklagarmyndigheten

[102] Se vidare bilaga 1. I skrivande stund bereds förslaget i regeringskansliet.

(2015). Exemplet de studerat är assistansbedrägerier, men det har bäring på stora bedrägerimål generellt. Det handlar exempelvis om att bedriva förundersökningen koncentrerat, med tillräcklig resurssättning och rätt kompetenser. Myndigheten lyfter även att utredningsgrupper som får vara intakta, är fredade från andra ärenden och har byggt upp erfarenhet visat sig vara mer effektiva, vilket kortar utredningstiden avsevärt. Det är viktigt att identifiera ytterligare åtgärder som kan effektivisera rättsväsendets hantering av stora utredningar. Här kan nämnas att Brå har fått i uppdrag att analysera utvecklingen av förundersökningars och brottmåls omfång och komplexitet under de senaste tio åren. Karaktären hos särskilt stora mål ska kartläggas och en bedömning ska göras av vad som ligger bakom utvecklingen.

Se över kompetenssammansättningen hos polisens bedrägeriutredare

Resultaten visar på en utbredd uppfattning att det finns en brist på vissa viktiga kompetenser inom polisens bedrägeriutredningsverksamhet. Det handlar dels om personer med specialkompetens avseende välfärdsbedrägerier, dels om kompetenser som behövs vid analyser av olika typer av bevisningsunderlag som är centrala inom ramen för bedrägeriutredningar. Enligt Brås intervjupersoner handlar det bland annat om revisorer, tillgångsutredare och utredare med särskild juridisk kompetens. Överlag tyder resultaten på att det kan finnas behov av att se över den sammansättning av kompetenser som finns inom polisens bedrägeriutredningsverksamhet.

Utöka rättsväsendets kapacitet vid utredning av it-relaterad brottslighet

Både tidigare Brå-studier och andra granskningar har visat på brister i rättsväsendets förmåga att hantera it-relaterad brottslighet (Brå 2013:14, 2015:6, Rikspolisstyrelsen 2014, Riksrevisionen 2015). Det handlar dels om kunskapsbrister genom hela rättskedjan, dels brister i polisens kapacitet vid it-undersökningar och framtagning av olika typer av teknisk bevisning. I den här studien betonades särskilt att kapacitetsbristen hos polisens it-forensiska funktioner bromsar utredningar och utgör ett särskilt hinder för en mer effektiv hantering av stora bedrägeriutredningar. Det finns därför anledning för Brå att återigen lyfta behovet av att se över kapaciteten genom bemanning av it-forensiker för att effektivisera handläggningen av dessa brott. Här kan också nämnas att Brå för närvarande arbetar med ett regeringsuppdrag där utvecklingen av förekomsten av it-relaterade inslag i de polisanmälda brotten i olika brottskategorier analyseras, i relation till

utvecklingen hos polisen av resurser ägnade åt att bistå utredningar med it-relaterat stöd och forensiska it-undersökningar.

Öka rättsväsendets kunskap om vissa utredningsmetoder

Kapitlet om Rättsväsendets arbete i denna rapport har illustrerat hur ärenden med vissa bedrägerimodus ofta läggs ner av rättsväsendet. Skälet är att det är svårt att identifiera en gärningsperson och att det rör sig om många mindre bedrägerier. För gärningspersonen kan dock dessa mycket väl omsätta stora belopp. Givet det stora inflödet av ärenden måste polisen mycket snabbt ta ställning till vilka ärenden som går att utreda vidare och vilka som ska läggas ner. En klar risk är att modus som anses vara svårutredda slentrianmässigt läggs ner. Dessutom byggs det aldrig upp någon kompetens om hur dessa brott går till och vilka utredningsmöjligheter som trots allt finns. Det vore därför angeläget att i ett metodutvecklingsprojekt titta närmare på ett antal av dessa till synes svårutredda ärenden och se om det går att nå längre i utredningarna.

Analysen visar också att det finns särskilda utmaningar vid utredningar av gränsöverskridande bedrägerier. En tidigare rapport visar att kunskapen om de möjligheter som finns på det internationella planet är låg (Brå 2014:10, kap. 8). Samverkan mellan olika svenska myndigheter kan också förbättra möjligheten att snabbare få internationell hjälp när det gäller brottsutbyte och information.[103]

Metodutveckling: kort- och kreditbedrägerier

Brås resultat tyder på att det skett en positiv utveckling i rättsväsendets förmåga att samordna, utreda och lagföra bedrägerier där bankkonton ger ett säkert spår som kan följas (framför allt annonsbedrägerier och fakturabedrägerier). Även när det gäller kategorin övriga telefon- och internetbedrägerier visar Brås intervjuer att det på senare tid skett en positiv utveckling i hur dessa anmälningar hanteras. När det gäller kort- och kreditbedrägerier tyder däremot Brås intervjuer på att dessa hanteras på i stort sett samma sätt i dag som år 2013 (året för Brås urval av ärenden), med många snabba nedläggningar. Metodutvecklingsinsatser som kan bidra med nya möjligheter för att identifiera gärningspersonerna vid kort- och kreditbedrägerier samt knyta gärningspersonerna till brottstillfällen kan därmed anses som angelägna.

[103] För mer information om vilka myndigheter som har vilka möjligheter, läs kapitel 8 i Brå-rapporten *Gå på pengarna*, Brå 2014:10.

Öka rättsväsendets kompetens att utreda bedrägerier med företag

Vissa gärningspersoner använder företag för sina bedrägerier, vilket typiskt sett ger större volym i brottsligheten. Det ställer också särskilda krav på rättsväsendet. Genom bolagskonstruktioner kan det vara särskilt svårt att utreda *vilka* som ligger bakom bedrägerierna. De personer som syns är framför allt medhjälpare och målvakter. Att förstå sådana strukturer är en relativt ovanlig uppgift för polisen. Däremot har Skatteverket och Ekobrottsmyndigheten större erfarenhet av att kartlägga företag som används för brott. Problemet är, återigen, att bedrägerier inte ingår i deras primära ansvarsområde. Här tyder intervjuerna på att det finns ett behov av kunskapsutbyte myndigheterna emellan om hur man utreder ekonomisk brottslighet som begås med hjälp av företag (se vidare rubriken Tillgångsinriktad brottsbekämpning).

Ytterligare aktörer kommer med i bilden när företaget har utbetalningar från välfärden. För några år sedan utvecklade Försäkringskassan, Skatteverket och polisen sitt utredningsarbete mot assistansbedrägerier genom några stora utredningar (ISF och Brå 2011:12). Skatteverket granskade företagens bokföring etc., polisen utförde spaning. Dessutom har Försäkringskassan möjlighet att göra besök i brukarens hem och notera vilka assistenter som arbetar där. Inspektionen för vård och omsorg, IVO, får göra oannonserade besök, vilket kan vara nyttigt för att dokumentera när en anordnare inte driver en reell verksamhet. Av särskilt intresse vid sådana besök i anordnarens lokaler är exempelvis tecken på felaktiga tidrapporter (se vidare Brå 2015:8).

Liknande behov av samverkan finns inte minst vid misstänkta bedrägerier mot Arbetsförmedlingens företagarstöd (se vidare Brå 2015:8). Arbetsförmedlingen fattar beslut och har kunskap om stöden, Skatteverket har kunskap om företagen. Beroende på granskningsobjekt kan även andra utbetalande myndigheter ingå. Polisen behöver deras kunskap om systemen för att genomföra spaning och utredning av de misstänkta brotten.

Referenser

Ablan, L., Libicki, M. och Galay, A. (2014). *Markets for cybercrime tools and stolen data*. Santa Monica: RAND corporation, National Security Research Division.

Ahola, M. (2013). *Bedrägeri. Introduktion och handledning för brottsutredare*. Stockholm: Norstedts Juridik.

Anderson, R. m.fl. (2013). Measuring the cost of cybercrime. I: Böhme, R. (red.), *The economics of information security and privacy*. Berlin: Springer.

Arvidsson, N. (2009). *Framtidens betalsystem. En studie av förnyelse av det svenska betalsystemet*. Stockholm: Kungliga tekniska högskolan.

Aquilina, J., Casey, E. och Malin, C. (2008). *Malware forensics: Investigating and analyzing malicious code*. Burlington, MA: Syngress.

Bhargav, A. (2015). *PCI compliance. The definitive guide*. Boca Raton, FL: CRC Press.

Bradbury, D. (2014). Testing the defences of bulletproof hosting companies. *Network security*, 2014(6), s. 8–12.

Brenner, S. (2012). *Cybercrime and the law. Challenges, issues and outcomes*. Boston: Northeastern University Press.

Brottsförebyggande rådet, Brå (2005). *När olyckan inte är framme. Bedrägerier mot allmän och privat försäkring*. Rapport 2005:10. Stockholm: Brottsförebyggande rådet.

Brottsförebyggande rådet, Brå (2007). *Vart tog alla pengarna vägen? En studie av narkotikabrottslighetens ekonomihantering*. Rapport 2007:4. Stockholm: Brottsförebyggande rådet.

Brottsförebyggande rådet, Brå (2007). *Narkotikadistributörer – En studie av grossisterna*. Rapport 2007:7. Stockholm: Brottsförebyggande rådet.

Brottsförebyggande rådet, Brå (2007). *Fusk med a-kassa. Motiv, omfattning och åtgärder.* Rapport 2007:23. Stockholm: Brottsförebyggande rådet.

Brottsförebyggande rådet, Brå (2007). *Organiserat svartarbete i byggbranschen*. Rapport 2007:27. Stockholm: Brottsförebyggande rådet.

Brottsförebyggande rådet, Brå (2008). *Samverkan mot bidragsbedrägerier. Exemplet Västmanland och Skåne*. Rapport 2008:6. Stockholm: Brottsförebyggande rådet.

Brottsförebyggande rådet, Brå (2011). *Penningtvätt. Rapportering och hantering av misstänkta transaktioner*. Rapport 2011:4. Stockholm: Brottsförebyggande rådet.

Brottsförebyggande rådet, Brå (2011). *Storskaliga skattebrott – En kartläggning av skattebrottslingens kostnader*. Rapport 2011:7. Stockholm: Brottsförebyggande rådet.

Brottsförebyggande rådet, Brå (2012). *Otillåten påverkan mot företag. En undersökning om utpressning*. Rapport 2012:12. Stockholm: Brottsförebyggande rådet.

Brottsförebyggande rådet, Brå (2012a). *Användning av brottskoder. En kvalitetsstudie inom kriminalstatistiken*. Kvalitetsstudie 1. Stockholm: Brottsförebyggande rådet.

Brottsförebyggande rådet, Brå (2013). *Bestämmelsen om kontakt med barn i sexuellt syfte. En uppföljning av tillämpningen av lagen från polisanmälningar till domar*. Rapport 2013:14. Stockholm: Brottsförebyggande rådet.

Brottsförebyggande rådet, Brå (2014). *Korruption i Myndighetssverige. Otillåten påverkan mot insider*. Rapport 2014:4. Stockholm: Brottsförebyggande rådet.

Brottsförebyggande rådet, Brå (2014). *Gå på pengarna – Antologi om tillgångsinriktad brottsbekämpning*. Rapport 2014:10. Stockholm: Brottsförebyggande rådet.

Brottsförebyggande rådet, Brå (2015). *Polisanmälda hot och kränkningar mot enskilda personer via internet*. Rapport 2015:6. Stockholm: Brottsförebyggande rådet.

Brottsförebyggande rådet, Brå (2015). *Intyget som dörröppnare till välfärdssystemet. En rapport om välfärdsbrott med felaktiga intyg*. Rapport 2015:8. Stockholm: Brottsförebyggande rådet.

Brottsförebyggande rådet, Brå (2015). *Administrativa åtgärder mot ekonomisk och organiserad brottslighet. Del 1: Tillstånd att bedriva verksamhet*. Rapport 2015:15. Stockholm: Brottsförebyggande rådet.

Brottsförebyggande rådet, Brå (2015). *Matchfixning. Manipulation av matcher och spelmarknad*. Rapport 2015:18. Stockholm: Brottsförebyggande rådet.

Brottsförebyggande rådet, Brå (2015). *Penningtvätt och annan penninghantering. Kriminella, svarta och grumliga pengar i legal ekonomi.* Rapport 2015:22. Stockholm: Brottsförebyggande rådet.

Brottsförebyggande rådet, Brå (2016). *Nationella trygghetsundersökningen 2015. Om utsatthet otrygghet och förtroende*. Rapport 2016:1. Stockholm: Brottsförebyggande rådet.

Brottsförebyggande rådet, Brå (2016). *Kriminell infiltration av företag*. Rapport 2016:7. Stockholm: Brottsförebyggande rådet.

Buchanan, T. och Whitty, M. (2014). The online dating romance scam: Causes and consequences of victimhood. *Psychology, crime and law* 20, s. 261–283.

Buescher, A., Leder, F. och Seibert, J. (2011). Banksafe information stealer detection inside the web browser. I: Sommer, R., Balzarotti, D. och Maier, G. (red.), *Recent advances in intrusion detection*. Berlin: Springer.

Bullock, K., Clarke, R. V. och Tilley, N. (red.) (2010). *Situational Prevention of Organised Crimes*. Portland: Willan Publishing.

Chua, C., Wareham, J. och Robey, D. (2007). The role of online trading communities in managing internet auction fraud. *MIS Quarterly* 31, s. 759–781.

Clarke, R. C. (red.) (1997). *Situational crime prevention. Successful case studies*. 2:a upplagan. New York: Criminal Justice Press.

Clough, J. (2015). *Principles of cybercrime*. Cambridge: Cambridge University Press.

Cohen, L.E. och Felson, M. (1979). Social change and crime rate trends: A routine activities approach. *American Sociological Review* 44, s. 588–608.

Department for Work and Pensions (2011). *Fraud and error in financial, welfare and revenue services: A systematic map of the empirical research evidence with particular reference to notification of changers of circumstances*. Sheffield: DWP.

Dibs (2015). *Svensk e-handel*. Dibs årliga rapport om e-handel, mobil handel och betalningar. www.svensk-e-handel.se

Ds 2015:12. *Missbruk av svenska pass. Omfattning och åtgärdsförslag*. Stockholm: Justitiedepartmentet.

Dunham, K. m.fl. (2009). *Mobile malware attacks and defense*. Burlington, MA: Syngress Publishing.

El-Din, R.S., Cairns, P. och Clark, J. (2015). The human factor in mobile phishing. I: Dawson, M. och Omar, M. (red.), *New threats and countermeasures in digital crime and cyber terrorism*. Hershey PA: Information Science Reference.

Engdahl, O. (2010). *Bortom girigheten. Ekonomisk brottslighet i bank- och finansbranschen*. Finland: Boréa.

Europol (2014). *The internet organised crime threat assessment (iOCTA)*. The Hague: European cybercrime centre, Europol.

Finansinspektionen (2009). *Kontobedrägerier*. Rapport 2009:13. Stockholm: Finansinspektionen.

FUT-delegationen (2007). *Orsaker till felaktiga utbetalningar av ekonomiskt bistånd från kommunerna*. Rapport 2. Stockholm: Fritzes.

FUT-delegationen (2008). *Hur tryggar vi trygghetssystemen? Kontroller och kontrollmetoder*. Rapport 9. Stockholm: Fritzes.

Gill, M. (2005). *Learning from fraudsters*. London: Protiviti.

Gill, M. (2007). *Learning from fraudsters. Reinforcing the message*. London: Protiviti.

Gillespie, A. (2016). *Cybercrime. Key issues and debates*. New York: Routledge.

Goldberg, D. och Larsson, L. (2013). *It-säkerhet för privatpersoner – en introduktion*. Stockholm: Stiftelsen för internetinfrastruktur.

Goldberg, D och Larsson, L. (2014). *Korthuset. Hur tjuvarna flyttade ut på nätet och varför din bank lät det hända*. Norstedts.

Gounev, P. (2012). 4 Organised crime, corruption and the private sector. I: Gounev, P. och Ruggiero, V. (red.) *Corruption and organized crime in Europe. Illegal partnerships*. London: Routledge. s. 32–54.

Grant, N. och Shaw, J. (2014). *Unified communications forensics*. Waltham, MA: Syngress.

ISF och Brå (2011). *Bidragsbrott och skattebrott. Välfärdens dubbla kriminalitet*. Rapport 2011:12. Stockholm: Inspektionen för socialförsäkringen och Brottsförebyggande rådet.

JO (2011). *Justitieombudsmännens ämbetsberättelse*. Redogörelse 2010/2011: JO1.

Johnson, B. och Larsson, P. (2011). Ryktet om bidragsfusk hotar trygghetssystemen. *DN debatt,* 24/6-2011.

Kang, A. m.fl. (2013). Security considerations for smart phone smishing attacks. I: Jeong, H. -Y. m.fl. (red.), *Advances in computer science and its applications*. Berlin: Springer.

Kaushik, A. (2013). *Sailing safe in cyberspace. Protect your identity and data*. New Delhi: Sage.

Kharraz, A. m.fl. (2015). Cutting the Gordian knot: A look under the hood of ransomware attacks. I: Almgren m.fl. (red.), *Detection of intrusions and malware, and vulnerability assessment. 12th International Conference, DIMVA, Milan, Italy, July 9-10, 2015*. Proceedings. Cham: Springer.

Kirwan, G. och Power, A. (2013). *Cybercrime. The psychology of online offenders*. Cambridge: Cambridge University Press.

Korsell, L., Hagstedt, J. och Skinnari, J. (2008). Från kelgrisar till styvbarn. *Nordisk Tidsskrift for Kriminalvidenskab*. April, 2008–95. Årgång Nr. 1, s. 21–38.

Korsell, L. och Nilsson, M. (2003). *Att förebygga fel och fusk. Metoder för reglering och kontroll*. Stockholm: Norstedts juridik.

Korsell, L., Skinnari, J. och Vesterhav, D. (2009). *Organiserad brottslighet i Sverige*. Malmö: Liber.

Kronqvist, S. (2013). *Brott och digitala bevis. En handledning*. Stockholm: Nordstedts juridik.

Lehtola, M. och Paksula, K. (2000). *Situational crime prevention of ecomomic crime*. Helsinki: National council for crime prevention.

Levi, M. (2008). *The phantom capitalists. The organization and control of long-firm fraud*. Revised edition. Aldershot, Hampshire: Ashgate.

Levi, M. m.fl. (2015a). *The implications of economic cybercrime for policing*. Research report, City of London Corporation. London: City of London Corporation.

Levi, M. m.fl. (2015b). *The implications of economic cybercrime for policing. Technical Annex*. Research report, City of London Corporation. London: City of London Corporation.

Luiijf, E. (2012). Understanding cyber threats and vulnerabilities. I: Lopez, J. m.fl. (red.), *Critical infrastructure protection. Information infrastructure models, analysis and defense*. Berlin: Springer.

Maras, H.-E. (2015). *Computer forensics. Cybercriminals, laws and evidence*. Burlington, MA: Jones & Bartlett.

Mitic, S. (2009). *Stopping identity theft. 10 easy steps to security*. Berkeley, CA: Nolo.

Montague, D. (2011). *Essentials of online payment security and fraud prevention*. Hoboken, New Jersey: John Wiley and Sons.

Moore, T., Clayton, R. och Andersson, R. (2009). The economics of online crime. *Journal of economic perspectives* 23:3, s. 3–20.

NBC (2014a). *Nationell lägesbild Bedrägerier.* Stockholm: Nationellt bedrägericenter. Polismyndigheten.

NBC (2014b): *Sammanfattning gällande lagförslag om identitetsintrång*. PM. Nationellt Bedrägericenter. Polismyndigheten.

NBC (2015a). *Intressant just nu om bedrägerier.* December 2015. Stockholm: Nationellt bedrägericenter. Polismyndigheten.

NBC (2015b). *Lägesbild bedrägerier 2015*. Stockholm: Nationellt bedrägericenter. Polismyndigheten.

NFC (2015): *Det fysiska ID-kortet – problem och möjligheter.* Seminarium om ID-stölder, Stockholm 2015-03-10. Helene Andersson, Dokumentanalysgruppen, Nationellt Forensiskt Centrum. Polismyndigheten.

NUC (2015a). *Lägesbild av den grova organiserade brottsligheten 2016-2017*. Stockholm: Nationella underrättelsecentret/ Polismyndigheten.

NUC (2015b). *Identitetsrelaterad brottslighet*. Öppen version. Stockholm: Nationella underrättelsecentret. Polismyndigheten.

Prop. 2005/06:1. *Budgetpropositionen för 2006*. Stockholm: Finansdepartementet.

Prop. 2006/07:80. *Bidragsbrottslag*. Stockholm: Finansdepartementet.

Prop. 2007/08:160. *Utökat elektroniskt informationsutbyte*. Stockholm: Finansdepartementet.

Rikspolisstyrelsen (2010). *Polisens årsredovisning 2009*. Stockholm: Rikspolisstyrelsen.

Rikspolisstyrelsen (2011). *Polisens årsredovisning 2010*. Stockholm: Rikspolisstyrelsen.

Rikspolisstyrelsen (2012a). *Polismyndigheternas handläggning av bedrägeriärenden. En uppföljande inspektion*. Inspektionsrapport 2011:9. Stockholm: Rikspolisstyrelsen, Enheten för Inspektionsverksamhet.

Rikspolisstyrelsen (2012b). *Polisens årsredovisning 2011*. Stockholm: Rikspolisstyrelsen.

Rikspolisstyrelsen (2014). *Inspektion av polismyndigheternas förmåga att handlägga IT-brott*. Tillsynsrapport 2014:2. Stockholm: Rikspolisstyrelsen.

Rikspolisstyrelsen (2015). *Polisens årsredovisning 2014*. Stockholm: Rikspolisstyrelsen.

Riksrevisionen (2010). *Informationsutbyte mellan myndigheter med ansvar för trygghetssystem*. RiR 2010:18. Stockholm: Riksrevisionen.

Riksrevisionen (2011). *Vad blev det av de misstänkta bidragsbrotten?* RiR 2011:20. Stockholm: Riksrevisionen.

Riksrevisionen (2015). *It-relaterad brottslighet – polis och åklagare kan bli effektivare*. RIR 2015:21. Stockholm: Riksrevisionen.

ROCIC (2014). *Credit card crime*. ROCIC special research report. Nashville: Regional Organized Crime Information Center.

Rönnblom, H., Skinnari, J. och Korsell, L. (2015). ”6. Sweden.” I: Savona, E., och Berlusconi, G. (red.), *Organised Crime Infiltration of Legitimate Businesses in Europe: A Pilot Project in Five European Countries. Final report of Project ARIEL*. Milan: Transcrime.

Savona, E., och Berlusconi, G. (red.), (2015). *Organised Crime Infiltration of Legitimate Businesses in Europe: A Pilot Project in Five European Countries. Final report of Project ARIEL*. Milan: Transcrime.

Simha, A. (2013). Advance fee fraud. I: Salinger, L. (red.). *White collar and corporate crime*. Thousands Oaks CA: Sage.

Skatteverket (2014): *Identitetsrelaterad brottslighet inom folkbokföringen*, del 1-3. Stockholm: Skatteverket.

Socialdepartementet (2006). *Regleringsbrev för budgetåret 2006 avseende Försäkringskassan*. Ändringsbeslut 2006-06-21. S2006/5107/SK. Stockholm: Socialdepartementet.

SOU (1970). *Körkort och körkortsregistrering*. Betänkande av körkortsutredningen. SOU 1970:26. Stockholm: Statens offentliga utredningar.

SOU (1994). *Personnummer – integritet och effektivitet*. Betänkande av Personnummerutredningen. SOU 1994:63. Stockholm: Statens offentliga utredningar.

SOU (2006). *Bidragsbrott*. SOU 2006:48. Stockholm: Statens offentliga utredningar.

SOU (2007). *ID-kort för folkbokförda i Sverige*. Betänkande från id-kortutredningen. SOU 2007:100. Stockholm: Statens offentliga utredningar.

SOU (2008). *Rätt och riktigt. Åtgärder mot felaktiga utbetalningar från välfärdssystemen*. SOU 2008:74. Betänkande av Delegationen mot felaktiga utbetalningar. Stockholm: Statens offentliga utredningar.

SOU (2008). *Bidragsspärr*. SOU 2008:100. Stockholm: Statens offentliga utredningar.

SOU (2009). *Återkrav inom välfärdssystemen – förslag till lagstiftning*. SOU 2009:6. Stockholm: Statens offentliga utredningar.

SOU (2011). *Sanktionsavgifter på trygghetsområdet*. SOU 2011:3. Betänkande av Utredningen om ett administrativt sanktionssystem inom trygghetssystemen. Stockholm: Fritzes.

SOU (2012). *Åtgärder mot fusk och felaktigheter med assistansersättning*. SOU 2012:6. Stockholm: Statens offentliga utredningar.

SOU (2013). *Starkt straffrättsligt skydd för egendom*. Betänkande av Egendomsskyddsutredningen. SOU 2013:85. Stockholm: Statens offentliga utredningar.

SOU (2014). *Det ska vara lätt att göra rätt*. Betänkande av utredningen om åtgärder mot felaktiga utbetalningar inom den arbetsmarknadspolitiska verksamheten. SOU 2014:16. Stockholm: Fritzes.

SOU (2015). *Ett stärkt konsumentskydd vid telefonförsäljning*. SOU 2015:61. Stockholm: Statens offentliga utredningar.

SOU (2015). *Fakturabedrägerier*. Betänkande av utredningen om åtgärder mot fakturabedrägerier. SOU 2015:77. Stockholm: Statens offentliga utredningar.

Statskontoret (2009). *Sagt men inte gjort – en granskning av Arbetsförmedlingens arbete för att förhindra felaktiga utbetalningar*. 2009:13. Stockholm: Statskontoret.

Svenska stöldskyddsföreningen (2013): *Kartläggning av allmänhetens kunskap, inställning och attityder kring ID-kapning*. Demoskop.

Tak, G. och Ojha, G. (2012). Awareness based approach against e-mail attacks. I: Meghantathan, N. m.fl. (red.), *Advances in computing and information technology*. Berlin: Springer.

Turban m.fl. (2015). *Electronic commerce. A managerial and social networks perspective*. New York: Springer.

Watson, G., Mason, A. och Ackroyd, R. (2014). *Social engineering penetration testing. Executing social engineering pen tests, assessments and defence*. Oxford: Syngress.

Whitty, M. och Buchanan, T. (2016). The online dating romance scam: The psychological impact on victims – both financial and non-financial. *Criminology and Criminal Justice* (under tryckning).

Youngblood, J. (2015). *A comprehensive look at fraud identification and prevention*. Boca Raton: CRC Press.

UC AB (2015): *Det var länge sen tjuvar använde såna här*. UC:s årliga enkät till bedrägerispärrade. Stockholm: UC AB

Åklagarmyndigheten (2008). *Förundersökningsbegränsning och åtalsunderlåtelse*. Riksåklagarens riktlinjer, RåR 2008:2.

Åklagarmyndigheten (2013). *Bidragsbrottslagen*. RättsPM 2013:4. Stockholm: Åklagarmyndighetens utvecklingscentrum.

Åklagarmyndigheten (2015). *Bedrägeri och bidragsbrott med assistansersättning. Probleminventering och rekommendationer.* RättsPM 2015:5. Åklagarmyndigheten: Utvecklingscentrum Stockholm.

Bilaga 1

Angränsande statliga utredningar

Egendomsskyddsutredningen

År 2012 fick en särskild utredare i uppdrag att undersöka behovet av att stärka det straffrättsliga skyddet för egendom. Bland annat skulle utredaren ta ställning till om inslaget av systematiken i vissa former av brott, exempelvis bluffakturor, bör få större betydelse för brottsrubriceringen av förmögenhetsbrotten. Uppdraget slutredovisades i december 2013 (SOU 2013: 85).

Av särskilt intresse för Brås uppdrag är att utredningens betänkande beskriver bedrägerier med hjälp av bluffakturor som ett stort samhälleligt problem. Vidare konstateras att den lagtekniska utformningen av bedrägeribrottet inte är avpassad för omfattande systematiska bedrägeriförfaranden, som organiserade fakturabedrägeriverksamheter. Det beror bland annat på att bedrägeribrottets utformning ställer höga krav på brottsutredningen att bevisa att det skett ett vilseledande i förhållande till varje målsägare. Det innebär att varje målsägare måste förhöras om varje enskild faktura och i förekommande fall om skälet till att hon eller han har betalat fakturan. Det kräver mycket omfattande utredningsresurser, och i praktiken innebär det att en stor del av de systematiska bedrägeribrotten förblir obeivrade, vilket bland annat innebär en risk att rättssystemets trovärdighet sätts i fara.

Förslag om en ny straffbestämmelse – grovt fordringsbedrägeri

Utredningen drog slutsatsen att en ny straffbestämmelse behövdes, som tar sikte på systematiskt bedrägeri med bluffakturor. Det nya brottet skulle bara finnas i grov form och skulle benämnas *grovt fordringsbedrägeri*, med en straffskala på fängelse i lägst sex månader och högst sex år.

Straffansvaret skulle omfatta betalningsuppmaningar och liknande meddelanden, såväl muntliga som skriftliga, som i vilse-

ledande syfte riktas till en vidare krets av mottagare och som avser betydande värden. Enligt utredningen bör 50 mottagare anses som en vidare krets, samtidigt som det skulle överlämnas till rättstillämpningen att avgöra om detta rekvisit i det enskilda fallet kan vara uppfyllt även vid ett mindre antal mottagare. Som undre gräns för vad som skulle betraktas som ett betydande värde angavs ca fem prisbasbelopp.

Brottet skulle vara fullbordat redan då gärningspersonen avsänt eller på annat sätt förmedlat meddelanden till mottagarna, utan något krav på att mottagarna mottagit meddelandena. Enligt utredningen skulle det innebära en förenkling av brottsutredningarna, då de brottsbekämpande myndigheterna inte längre skulle behöva förhöra samtliga mottagare för att kontrollera om de tagit del av meddelanden med betalningsuppmaningar och blivit vilseledda. Utredningen föreslog vidare att både förberedelse och försök till det nya brottet skulle bli straffbart.

Förslag om kriminalisering av identitetsintrång
Av intresse för Brås uppdrag är att utredningen också presenterade ett förslag om att kriminalisera olovlig användning av annans identitetsuppgifter. Utredningen konstaterar att det skett en ökning och att i princip vem som helst i dag kan drabbas av brott genom att deras identitet används olovligen och att det kan leda till långtgående konsekvenser för de drabbade. Det nya brottet skulle benämnas *identitetsintrång* och föreslås omfatta sådana uppgifter som kan användas för att identifiera en levande fysisk person, exempelvis personnummer, samordningsnummer, namn och adress.

Mot bakgrund av utredningens slutsatser har regeringen i en lagrådsremiss (2016-02-11) lämnat ett förslag om att kriminalisera *olovlig identitetsanvändning*. För mer detaljer, se bilaga 5.

Utredningen om åtgärder mot fakturabedrägerier

I september 2015 publicerade Utredningen om åtgärder mot fakturabedrägerier sitt betänkande (SOU 2015:77). Utredningens kartläggning visar att fakturabedrägerier förekommer i stor omfattning, och de som utsätts är både privatpersoner, företag, statliga förvaltningsmyndigheter och kommun och landsting. Staten och företagen drabbas dock mest – både av rena bluffakturor och av fakturabedrägerier där någon kontakt initialt ägt

rum.[104] En majoritet av de personer och organisationer som tar emot bedrägliga fakturor betalar inte. Trots det visade utredningens grova skattning att personer bakom fakturabedrägerier under det gångna året kan ha gjort vinster motsvarande från omkring en halv miljard och upp till över en miljard kronor.

Många betalar av andra skäl än att de blivit vilseledda
Utredningens kartläggning visade att betalning i många fall sker på grund av en överdriven rädsla för betalningsanmärkningar. Andra skäl var att man bedömer att det är enklare och mer ekonomiskt än att bestrida fakturan eller att man bedömer sina chanser att få rätt vid en rättslig prövning som små. Samtidigt visade kartläggningen att det enda som den som utsatts behöver göra i regel är att bestrida fakturan. De avtalsrättsliga regler som finns i dag ger, enligt utredningen, ett tillräckligt gott skydd för att personer som drabbas av fakturabedrägerier ska kunna undgå betalningsskyldighet vid en eventuell domstolsprövning.

Information till konsumenter och företagare en central åtgärd
Det mest effektiva sättet att motverka fakturabedrägerier är alltså att förmå dem som utsätts för fakturorna att hävda sina rättigheter enligt de regler som finns och att vägra betala. Enligt utredningen framstår Konsumentverkets upplysningstjänst som en naturlig kanal för att nå ut med information till konsumenter, medan Tillväxtverket anses vara den bäst lämpade myndigheten för att ansvara för information till företagen. Vidare föreslogs att även polisen ska ges i uppdrag att tillhandahålla relevant information till konsumenter eller näringsidkare som drabbats av fakturabedrägerier.

Ytterligare förslag från utredningen var att det borde ställas högre krav på försäljarens bevisning vid civilrättsliga mål som rör marknadsföring via telefonförsäljning samt att reglerna om ansvar för motpartens rättegångskostnader i förenklade tvistemål bör ändras för att göra det mer ekonomiskt rationellt att bestrida ogrundade fakturor i stället för att betala för att slippa en eventuell rättegång.

Utredningen lämnade också synpunkten att det vore en god idé att ge Bolagsverket ett tydligare brottsförebyggande uppdrag och

[104] När det gäller bluffakturor var det exempelvis 20 procent av de tillfrågade privatpersonerna som uppgav att de mottagit en eller flera bluffakturor under det senaste året. Detta kan jämföras med 34 procent av företagen, 36 procent av de statliga förvaltningsmyndigheterna och endast 8 procent av kommunerna. Motsvarande andelar som uppgett ett de utsatts för fakturabedrägerier efter kontakt var 12 procent (bland privatpersoner), 21 procent (bland företag), 26 procent (bland statliga förvaltningsmyndigheter) och 8 procent (bland kommunerna).

en möjlighet att vägra registrering vid misstanke om att ett bolag kan komma att användas i brottsligt syfte.

Nytillsatt Utredning om organiserad ekonomisk brottslighet mot välfärden

Den 24 september 2015 tillsattes en utredning om organiserad och systematisk ekonomisk brottslighet mot välfärden (Ju 2015:10). Utredaren ska bland annat kartlägga fenomenet, identifiera riskfaktorer i de utsatta välfärdssystemens regelverk, organisation, rutiner och tillämpning samt föreslå åtgärder för att förebygga och förhindra brotten. I detta ligger att även studera om informationsutbytet mellan berörda myndigheter fungerar. De föreslagna åtgärderna ska även syfta till att effektivisera de brottsbekämpande myndigheternas förutsättningar att utreda och beivra organiserad och systematisk ekonomisk brottslighet mot välfärden. I uppdraget ingår att utarbeta nödvändiga lagförslag. Uppdraget ska redovisas senast den 2 maj 2017.

Bilaga 2

Kodning av rättsväsendets nedläggningar av bedrägeriärenden

De olika koder som används av polisen och åklagarna vid nedläggning av brott är ibland svårgenomskådliga. När en utredning till exempel läggs ner av polisen med en hänvisning till att det inte längre finns anledning att fullfölja förundersökningen kan det bero på flera olika saker. För att förenkla redovisningen av rättsväsendets nedläggning av bedrägeribrotten har Brå därför kodat materialet utifrån en kombination av dels var i utredningsprocessen ärendet har lagts ner (utan att inleda förundersökning, efter att ha inlett förundersökning, utan att en misstänkt person har identifierats eller efter att en misstänkt person har identifierats), dels utifrån de nedläggningsgrunder och skriftliga motiveringar som angetts vid nedläggningsbeslutet. Nedan redovisas de kategorier av nedläggningar som används i rapportens redovisningar.

Dubbelanmält: Ärendet har lagts ner med en hänvisning till att brottet har dubbelanmälts.

Ej brott: I denna kategori finns dels ärenden som har lagts ner utan att inleda förundersökning med en hänvisning till att det anmälda förfarandet inte är brottsligt, dels ärenden där man efter att ha inlett förundersökning har dragit slutsatsen att det saknas anledning att anta att det skett ett brott som hör under allmänt åtal.

Preskriberat: Ärendet har lagts ner med en hänvisning till att brottet är preskriberat.

Anmälan inte längre aktuell: I dessa ärenden har en förundersökning inletts. I vissa fall har anmälan sedan dragits tillbaka av anmälaren, till exempel då det visat sig att det skett ett missförstånd

eller en förväxling. I vissa fall har polisen lagt ner ärendet med en hänvisning till att det inte längre finns anledning att fullfölja förundersökningen, samtidigt som det framgår att det beror på att den situation som föranledde anmälan har löst sig. Det kan finnas olika anledningar till detta, som exemplifieras i den löpande texten där det är aktuellt.

Ej utredningsbart: Här finns framför allt ärenden som har lagts ner utan att inleda förundersökning. Den vanligaste motivering som anges i materialet i dessa ärenden är ”brottet går uppenbart inte att utreda”. Här finns också några anmälningar där en förundersökning först har inletts, men sedan har lagts ner inom ett fåtal dagar med motiveringen att brottet inte går att utreda.

Spanings-/bevisproblem (ingen misstänkt identifierad): Förundersökning har inletts, men ärendet har lagts ner utan att en misstänkt person har identifierats. Här är ”ej spaningsresultat” den vanligaste nedläggningsmotivering som framgår av materialet. Här finns också flera anmälningar där motiveringen till nedläggningen varit att det inte finns förutsättning att styrka brott mot viss person, att vidare utredning ej förväntas styrka skälig misstanke eller att fortsatt förundersökning inte förväntas leda till att brott kan styrkas.

Bevisproblem (misstänkt identifierad): Förundersökning har inletts och nedläggningen har skett först efter att man har identifierat en person som kan misstänkas för brottet (denna person har dock inte nödvändigtvis registrerats som skäligen misstänkt för brottet i misstankeregistret). Här är hänvisningar till olika typer av bevisproblem de vanligaste nedläggningsmotiveringarna i de granskade ärendena. Det handlar bland annat om att brott inte kan styrkas, att det inte går att bevisa att den eller de som varit misstänkta har gjort sig skyldiga till brott, att det inte går att bevisa de objektiva förutsättningarna för att förfarandet ska vara brottsligt eller att det inte går att bevisa brottsligt uppsåt.

Förundersökningsbegränsning: En misstänkt person har identifierats men ärendet har lagts ner genom ett beslut om så kallad förundersökningsbegränsning. I de granskade ärendena har den misstänkte gärningspersonen i dessa fall oftast antingen redan blivit dömd för brott eller kommer att åtalas för annan brottslighet. I dessa situationer innebär beslutet att den misstänkte redan fått respektive kommer att få en påföljd som anses tillräcklig för att omfatta även den aktuella brottsligheten.

Misstänkt lämnat landet: Här har man identifierat en misstänkt person, men denna finns inte längre i Sverige.

Ärendet fortfarande öppet i slutet av 2014: Här framgår av Brås registerutdrag att en person har registrerats som skäligen miss-

tänkt för brottet, samt att brottet fortfarande var under utredning i slutet av 2014, vilket är studiens sista uppföljningsdatum i misstankeregistret.

Oklart: I denna kategori finns ett fåtal ärenden där det framgår av Brås material att en förundersökning har inletts, men ingen skäligen misstänkt har registrerats i misstankeregistret och det saknas annan information om huruvida en misstänkt person har identifierats på grund av att material inte har skickats till Brå av polisen.

Bilaga 3

Brås typologi och befintliga brottskoder

Kvaliteten i polisens brottskoder gällande brottsbalksbedrägerier har diskuterats i tidigare avsnitt, och var en del av motiveringen till att i Brås kartläggning söka skapa en mer adekvat kategorisering. I tabell 1B redovisas hur de fem huvudkategorierna som identifierats i ärendegranskningen korresponderar med dessa brottskoder. En del av skillnaden (förutom att kategorierna har delvis olika innehåll) förklaras av att Brå har haft all information tillgänglig som finns i förundersökningar, medan polisen tillämpar sina brottskoder vid anmälningstillfället, då många omständigheter kring brotten inte är klarlagda.

Det framgår att majoriteten av det som Brå beskriver som *annonsbedrägerier* kodas av polisen som bedrägeri med hjälp av internet, men ofta även som övrigt bedrägeri. Några annonsbedrägeriärenden var även kodade som datorbedrägeri.

Beträffande *fakturabedrägerier* är diskrepansen mellan Brås kategori och polisens kodning liten, då det finns en relativt tydlig brottskod för detta modus. Majoriteten av ärenden har därför registrerats under brottskoden fakturabedrägeri. Några ärenden kodades dock som övrigt bedrägeri respektive automatmissbruk.

Även bedrägerier med hjälp av kontokort har en särskild brottskod i polisens statistik; innehållet i denna är dock avgränsat på ett annat sätt än *kortbedrägerier* enligt Brå. En stor andel (30 procent) av Brås kortbedrägerier kodas visserligen av polisen som just bedrägeri med kontokort, men majoriteten, två ärenden av fem, kodas som datorbedrägeri (vilket ofta är korrekt med tanke på instruktioner till polisen). En relativt betydande del kodas vidare som automatmissbruk respektive övrigt bedrägeri, medan två ärenden hade brottskoden med hjälp av internet.

När det kommer till ärenden som Brå valt att beskriva som *kreditbedrägerier*, kodas två tredjedelar av dessa enligt brottsko-

den övrigt bedrägeri, men en del också som bedrägeri med hjälp av internet. Några ärenden hade brottskoden datorbedrägeri respektive bedrägeri med kontokort. Kreditbedrägeriärenden kan tillhöra de mest komplexa och är därmed svåra att placera under en specifik brottskod.

Kreditbedrägerierna är en av de kategorier som är mest splittrade över flertalet av polisens brottskoder. Detsamma gäller dock även ärenden som Brå samlat under benämningen *övriga telefon- och internetbedrägerier*. Kategorin är, som redovisats ovan, mycket heterogen, och många av dessa ärenden rör försöksbrott. Majoriteten kodas av polisen som bedrägeri med hjälp av internet samt datorbedrägeri (ungefär lika stora andelar), men relativt många ärenden registrerades som övrigt bedrägeri.

Internet och datorer

En del i regeringens uppdrag till Brå är att särskilt belysa vilka typer av bedrägerier som begåtts med hjälp av datorer och internet. Om vi i stället för som ovan utgår från de brottskoder som finns för dessa två brottskategorier, så observeras i tabellen att en stor andel av de ärenden som av polisen registrerats som *datorbedrägerier* är dels Brås kortbedrägerier, dels de olika bedrägerityper som ingår i kategorin övriga telefon- och internetbedrägerier. Den sistnämnda kategorin är också framträdande bland de ärenden som polisen registrerat under brottskoden för bedrägeri *med hjälp av internet*. Närmare hälften av de ärenden som registrerats under denna brottskod avser däremot annonsbedrägerier. Cirka en av tio av de anmälningar som registrerats under en av dessa två brottskoder avser kreditbedrägerier.

Tabell 1B. Fördelning av ärenden i Brås granskning enligt polisens brottskoder respektive Brås typologi. Absoluta tal.

Brottskod	Annons-bedrägeri	Faktura-bedrägeri	Annan bedräglig försäljning	Kort-bedrägeri	Kredit-bedrägeri	Annat bedrägligt köp/lån/uttag	Övrigt telefon- och internet-bedrägeri	Butiks-bedrägeri	Övrigt bedrägeri enl. BrB 9 kap.	Totalt
Datorbedrägeri (0901)	5	0	6	36	6	0	21	0	1	75
Automatmiss-bruk (0902	0	2	0	12	0	0	0	1	1	16
Snyltning (0903)	0	0	0	0	1	9	0	0	0	10
Med kontokort (0904)	0	0	0	26	3	0	1	0	0	30
Mot funktions-nedsatt (0905)	0	0	0	0	0	0	0	0	3	3
Övrigt bedrägeri (0906)	14	6	10	11	43	8	15	8	17	132
Fakturabedrä-geri (0912)	1	41	0	0	2	0	0	0	0	44
Med hjälp av internet (0913)	42	0	4	2	13	1	25	0	0	87
Annat checkbe-drägeri (0922)	0	0	0	0	0	0	0	0	2	2
Mot försäkrings-bolag (0929)	0	0	0	0	0	0	0	0	1	1
Totalt	**62**	**49**	**20**	**87**	**68**	**18**	**62**	**9**	**25**	**400**

Bilaga 4

Tidigare skattningar av förekomst och utveckling av identitetsmissbruk

Både inom rättsväsendet och inom näringslivet har det genomförts kartläggningar för att uppskatta omfattningen av olovlig användning av andras identiteter. De olika sätten att definiera, avgränsa och därmed benämna fenomenet gör att dessa inte är direkt jämförbara, men samtliga bidrar med relevant information. Sammantaget tyder mycket på att bedrägerier med hjälp av identitetsmissbruk har ökat i antal, drabbar både enskilda, näringslivet och välfärdssystemet samt omsätter stora belopp. Inte sällan finns det kopplingar till organiserad brottslighet.

Stöldskyddsföreningen

Stöldskyddsföreningen genomförde i samarbete med Demoskop under hösten 2013 intervjuer (telefonrekryterad webbpanel) med ett urval bestående av 1 105 personer 25–74 år gamla (Svenska stöldskyddsföreningen 2013). Syftet var att kartlägga omfattningen av identitetskapningar. Resultaten visade att antalet kreditupplysningar som tas på enskilda är högre för yngre personer och män. Tre av fyra kontrollerar sedan vem som tagit upplysningen och om det var befogat.

Enbart 7 procent (9 procent män och 5 procent kvinnor) ansåg sig vara väl informerade om identitetskapning. Andelen som ansåg sig som välinformerad var högre bland höginkomsttagare (16 procent).

Bara 2 procent uppgav att de någon gång blivit utsatta för en identitetskapning. Andelen är densamma för både kvinnor och män, men något högre bland höginkomsttagare (3 procent). Vidare har 6 procent blivit utsatta för försök till identitetskapning.

Kunskapen om hur man kan skydda sig mot identitetskapning visade sig vara relativt låg: cirka en fjärdedel hade mycket eller ganska hög kunskap samtidigt som kunskapsnivån var klart högre bland män och höginkomsttagare. Knappt två av fem uppgav sig vara mycket eller ganska oroliga för att bli utsatta för en identitetskapning. Nästan hälften, 4 av 10, är rädda att lämna ut sitt personnummer och ännu fler, 53 procent, hade avstått från köp eller medlemskap på grund av krav på att lämna sådana uppgifter. Enbart 14 procent visste vad som krävdes för att spärra sitt personnummer. Majoriteten, 6 av 10, påstod sig beredda att i ett förebyggande syfte spärra sitt personnummer för kreditupplysning och öppna det enbart vid behov.

Skatteverket

Skatteverket har i ett antal rapporter uppmärksammat problemet med identitetsrelaterad brottslighet med folkbokföringen som brottsverktyg (Skatteverket 2014). I rapporterna identifieras ett antal indikatorer på att en person är involverad i sådan brottslighet. En är exempelvis att identitetens födelseort ligger i ett tredjeland och inte är en ort i landet för medborgarskapet. En annan indikator är att en person startar företag inom ett år från invandringstillfället, är folkbokförd ”c/o” eller är eller varit engagerad i ett bolag där det förekommer oklara identiteter. Ytterligare exempel är att personen har eller har haft särskild postadress där det förekommer oklara identiteter.

Skatteverket framför en rad förbättringsförslag, bland annat att införa en ny kontrollgrupp på folkbokföringen, åtgärder vid falska identiteter, registrering av passnummer (och eventuellt även arbetsgivaren) i folkbokföringsdatabasen och kriminalisering av att låta någon folkbokföra sig felaktigt på en adress.

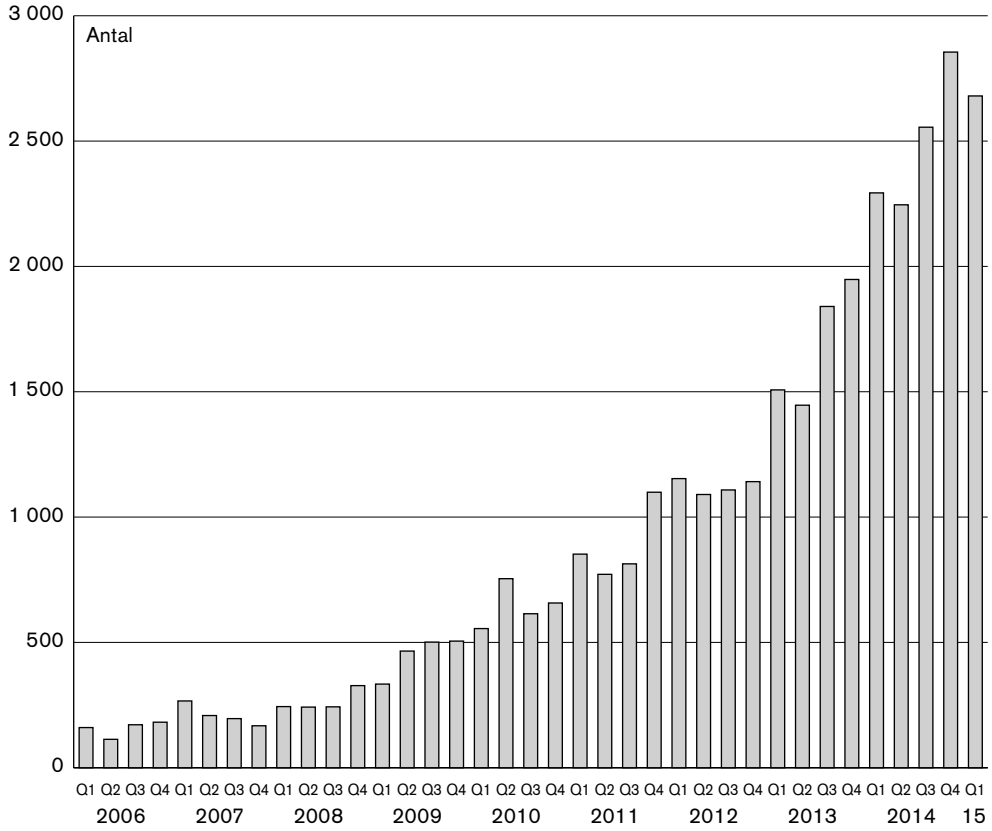
UC AB (tidigare Upplysningscentralen)

UC AB är Sveriges i särklass största kreditupplysningsföretag. Det är därför framför allt dit som den vars identitet blivit stulen ska vända sig för att spärra sitt personnummer för kreditköp. I flera år i rad har UC AB genomfört en kartläggning av dessa bedrägerispärrar. Den senaste (UC AB 2015) visade att antalet spärrar ökade med hela 385 procent mellan första kvartalet 2010 och motsvarande period 2015. Under första kvartalet 2015 registrerades 2 675 bedrägerispärrar. Det innebär att om man skattar antalet spärrar som kommer att ha registrerats vid 2015 års slut – förutsatt att det kan bortses från ytterligare ökning – kan det uppgå i minst 10 700 bedrägerispärrar det året (Brås skattning).

År 2014 begärdes 7 626 identitetsspärrar hos UC AB. Bedrägerier med kapade identiteter omsatte enligt UC AB:s bedömning

3,7 miljarder kronor under 2014, vilket är en ökning med 37 procent sedan 2013.

Figur 1B. Bedrägerispärrar enligt UC AB:s årliga kartläggning.



Källa: UC AB

En del av UC AB:s kartläggning består av en enkät till personer som spärrat sin identitet.[105] Svarsfrekvensen är låg, men här sammanfattas ändå de viktigaste resultaten. I enkäten ställs frågor om olika omständigheter kring kapningen. Resultaten för år 2014 visar att snittbeloppet vid ett bedrägeri med hjälp av identitetskapning är 54 000 kronor, och även detta innebär en ökning sedan 2013 (40 000 kronor). Största problemet med identitetskapning uppges finnas inom internethandel (ökning med 17 procent mellan 2014 och 2015), vid tecknande av telefonabonnemang och vid handel genom postorder.

[105] Svarsfrekvensen i senaste mätningen, genomförd v. 14 2015 och riktad till personer som spärrat sin identitet år 2014, var knappt 14 procent (n = 1 055), och det sker sannolikt en selektion vid själva anmälan till UC AB (dvs. alla som drabbats av kapning spärrar troligen inte sin identitet) och även i nästa steg, vid valet att besvara enkäten. Detta bör beaktas vid tolkning av resultaten.

UC AB:s bedömning är att alla kan drabbas; men att utsättas för identitetskapning är något vanligare bland män, högskoleutbildade, boende i villa eller radhus samt bosatta i någon av storstadsregionerna. Problemet kryper dessutom upp i åldrarna; i dag drabbas lika många 46–54- som 26–35-åringar, enligt UC AB. Snittinkomsten bland de drabbade var 530 000 kronor, enligt enkäten. Varannan person upptäcker bedrägeriet inom en vecka, vanligtvis genom att motta en kopia av kreditupplysningen.[106] En av tre upptäcker dock bedrägeriet först när de får en faktura eller inkassokrav på varor de inte beställt. De som besvarat enkäten uppgav att de fick lägga ner mellan 1,5 och 5 arbetsdagar på att åtgärda problemet. Över hälften, 6 av 10, utsattes flera gånger, och var femte person vet inte om problemet upphört. I 1–2 procent av ärendena var det någon i den utsattes närmare omgivning som låg bakom identitetskapningen. Oftast rör det sig alltså om okända förövare.

Nationellt bedrägericenter (NBC)

Polisens Nationella bedrägericenter, Utredningsenheten vid Polisregion Stockholm, har i en ny kartläggning (NBC 2015b) uppskattat att cirka 65 000 personer utsattes 2014 för någon form av identitetsintrång som möjliggjort ett bedrägeri eller försök därtill. Jämfört med föregående år innebär detta en 20-procentig ökning, en utveckling som enligt NBC förväntas att fortsätta. Enligt en beräkning kan under 2015 minst 80 000 personer ha utsatts för någon form av identitetsintrång. I beräkningen av identitetsintrångets omfattning ingår både kortbedrägerier *(card not present)*, kreditbedrägerier och bedrägerier med hjälp av sociala medier (t.ex. kapade Facebook-konton). Uppgifterna bygger på polisens verksamhetsuppföljning samt en djupare granskning av anmälningar. Vidare hämtar NBC månatligen information rörande aktuella modus från landets samtliga polisregioner.

NBC har även inom ramen för sitt uppdrag (NBC 2014a) kontrollerat anmälningar där en falsk identitetshandling antingen tagits i beslag, lämnats kvar eller fotograferats. Syftet var att kartlägga vilka typer av falska identitetshandlingar som finns i omlopp och på vilket sätt de används. NBC har även använt sig av information från NFC (Nationellt forensiskt centrum), som genomför äkthetsundersökningar av identitetshandlingar, vilket även innebär kartläggning av ursprunget. Framför allt är det olika typer av falska körkort som kommer till NFC för bedömning, där svenska körkort utgör den största andelen, följt av litauiska

[106] Enligt uppgifter från UC AB har man sett en ökning i antalet personer som ansluter sig till deras bevakningstjänst och därmed får en avisering när någon tar en kreditupplysning eller när något ändras i UC AB:s databas. Det gör det möjligt att snabbare stoppa eventuella bedrägerier.

körkort. Även falska identitetskort som utfärdats av bankerna förekommer relativt ofta.

Flertalet av de falska identitetshandlingarna var av bra kvalitet. Med detta menas att tillverkaren har lyckats imitera flera olika säkerhetsdetaljer på identitetskorten, vilket kan innebära att den falska identitetshandlingen i hög grad uppfattas som äkta. Utifrån informationen från NFC analyserade NBC omfattning, användningsområde samt spridning av de olika falska identitetshandlingarna. Det visade sig att tillverkarna ofta producerade flera olika typer av falska identitetshandlingar. Exempelvis så stod samma tillverkare för en omfattande produktion av både svenska körkort, bankutfärdade identitetskort samt lettiska körkort.

Nationellt underrättelsecentrum (NUC)

Det myndighetsgemensamma Nationellt underrättelsecentrum har under 2015 genomfört ett antal kartläggningar om identitetsrelaterad brottslighet. Dessa inkluderar förslag på åtgärder och sammanfattas i en öppen rapport med titeln *Identitetsrelaterad brottslighet* (NUC 2015b). I den framgår bl.a. att bruk av stulna eller falska identiteter förekommer vid bedrägerier och bidragsbrott, och dessutom i samband med eko- och skattebrott, förfalskningsbrott, penningtvätt, människosmuggling och människohandel.

Identitetsrelaterad brottslighet sker i hela landet, men är koncentrerad till storstadsregionerna där det finns större tillgång till brottsverktyg genom fler människor och företag. De flesta som använder identiteter i brottsligt syfte är män, men kvinnor förekommer. Ekonomisk vinning är den huvudsakliga drivkraften, enligt NUC. Företag beskrivs som centrala brottsverktyg, exempelvis genom att identiteter används i företag där man utnyttjar svart arbetskraft. Felaktiga identiteter används även för att söka ersättningar från välfärdssystemet. Folkbokföring är en förutsättning för brottet i detta fall, så de flesta av identiteterna är folkbokförda, men inte alltid på ett korrekt sätt. Det förekommer t.ex. att en person är felaktigt folkbokförd på postboxadresser eller att ett stort antal människor är skenskrivna på samma adress. NUC bedömer att ett vanligt tillvägagångssätt är att kriminella aktörer tar över och utnyttjar migranters identiteter, vilket drabbar redan utsatta människor.

Som viktiga åtgärder mot detta lyfts bland annat en bättre samsyn och effektivare informationsdelning mellan myndigheterna.

Bilaga 5

Identitetsmissbruk – närliggande lagstiftning och nytt lagförslag

Olovligt bruk av annans identitet som innebär en skada eller olägenhet för den vars identitet har använts är inte en brottslig gärning i dag; en kriminalisering ligger dock på förslag (SOU 2013:85 och Lagrådsremissen Straffrättsligt skydd mot olovlig identitetsanvändning). Samtidigt finns det redan i dag en rad bestämmelser som tangerar området, i synnerhet med utgångspunkt i Brås vida definition av identitetsmissbruk. Exempel på brottsrubriceringar är *brukande av falsk urkund* (BrB 14 kap. 10 §) och *urkundsförfalskning* (BrB 14 kap. 1 §). Det förstnämnda kan innebära att man använder exempelvis ett falskt id-kort. Urkundsförfalskning avser själva förfalskningen, exempelvis genom en manipulerad underskrift, som i ett antal av de studerade ärendena. Ett annat exempel på urkundsförfalskning är tillverkning av falska identitetshandlingar med hjälp av stulna personuppgifter, något som under senare tid vid ett flertal tillfällen skett i organiserad och storskalig form, enligt uppgifter från polisen (NBC 2015a).

Om någon däremot använder en äkta identitetshandling som är utfärdad för en annan person kan denne göra sig skyldig till *missbruk av urkund* (BrB 15 kap. 12 §). Den som använder en äkta identitetshandling utfärdad på osant innehåll kan straffas för *brukande av osann urkund* (BrB 15 kap. 11 § 3 st.) och den som medverkat till det oriktiga innehållet begår *osant intygande* (BrB 15 kap. 11 § 3 st.).

Det är inte ovanligt att en bedragare använder *dataintrång* för att komma över andras identitetsuppgifter. Dataintrång enligt BrB 4 kap. 9 c § innebär bland annat att någon olovligen bereder sig tillgång till en uppgift som är avsedd för automatiserad behandling. Syftet med intrånget eller vilka slags uppgifter det rör sig om

är oviktigt. Brottet anses vara riktat mot den som äger datasystemet, även om det drabbar dem som tillåtit att uppgifter om dem skulle registreras och lagras.

Vidare kan identitetsmissbruk i vissa fall betraktas som ett *förberedelsebrott*. Som redovisats har myndigheter ibland försökt att polisanmäla misstankar om osanna identiteter som just föreberedelsebrott, men det tycks inte finnas samsyn i denna fråga mellan landets olika bedrägerirotlar. Att se över hur den redan befintliga lagstiftningen kan tillämpas i samband med olika typer av identitetsmissbruk och söka en enhetlighet i tillämpningen kan därför vara önskvärt. Samtidigt kan det finnas ett värde i att betrakta identitetsmissbruk som ett fullbordat brott – både av signalskäl och på grund av bevissvårigheter vid förberedelsebrott. Det är också vad det nya förslaget syftar till.

Kriminalisering av olovlig identitetsanvändning

En statlig utredning (SOU 2013:85) har föreslagit att det bör bli straffbart att använda andra personers identitetsuppgifter på ett sådant sätt att det leder till en skada eller olägenhet för denne. Det nya brottet skulle kallas *identitetsintrång* och omfattas av BrB 4 kap. Den föreslagna lagtexten lyder enligt följande:

> *Den som genom att olovligen använda en annan persons identitetsuppgifter utger sig för att vara honom eller henne och därigenom ger upphov till skada eller olägenhet för den vars identitetsuppgifter används, döms för identitetsintrång till böter eller fängelse i högst två år.*

Med identitetsuppgifter menas sådana uppgifter som kan användas för att identifiera en fysisk person som är i livet. Exempel på sådana uppgifter är personnummer, samordningsnummer, namn, adress eller liknande. Avgörande är om uppgifterna ensamma eller tillsammans är tillräckligt unika för att identifiera en fysisk person, enligt författningskommentaren. Med att användningen ska vara olovlig menas att den inte ska vara tillåten enligt någon författning eller genom samtycke från den vars identitet har använts. Med skada avses vidare ekonomisk sådan och med olägenhet bl.a. praktiska besvär med att bestrida betalningsansvar och hindra fortsatta utbetalningar. Brottet skulle inte vara gradindelat och vare sig förberedelse eller försök ska kriminaliseras.[107]

[107] Flertalet remissinstanser vände sig mot det sistnämnda och menade att även förberedelse och försök till identitetsintrång bör kriminaliseras, då det är viktigt att ingripa mot denna typ av brottslighet på ett så tidigt stadium som möjligt. Några av instanserna ville även se ett gradindelat brott. Flertalet instanser var inne på att även juridiska personers identiteter bör omfattas. Överlag välkomnades förslaget och de kritiska synpunkter som fördes fram gav alltså främst uttryck för en önskan om en mer långtgående lösning snarare än ett motstånd mot att identitetsintrång bör kriminaliseras.

Regeringen ställde sig i stora delar bakom utredningens förslag, men valde att vidga vilka identitetsuppgifter som skulle omfattas, samt föreslog en annan brottsrubricering som bättre skulle fånga den nya bestämmelsens innehåll. I en lagrådsremiss (2016-02-11) föreslår regeringen att det nya brottet kallas *olovlig identitetsanvändning* och lagtexten har justerats till följande:

> *Den som genom att olovligen använda en annan persons identitetsuppgifter utger sig att vara honom eller henne och därigenom ger upphov till skada eller olägenhet för honom eller henne, döms för olovlig identitetsanvändning till böter eller fängelse i högst två år.*

Till skillnad från utredningens förslag menar regeringen, i linje med Datainspektionens remissyttrande, att även ett fotografi av en verklig person som används tillsammans med uppdiktade namn- och adressuppgifter skulle anses vara sådan identitetsuppgift som omfattas av den föreslagna bestämmelsen.[108] Justeringen tar främst sikte på situationer där någon olovligen startar ett konto på sociala medier med annan persons bild. En annan skillnad är att brottet, enligt regeringens förslag och liksom andra brott i kap. 4 BrB omfattas av en åtalsbegränsning. Det innebär att allmänt åtal ska få väckas endast om målsägaren anger brottet till åtal eller om åtal är påkallat från allmänt synpunkt.

Den nya bestämmelsen, om den träder i kraft, har ett betydande signalvärde och kan tydligare sätta det växande problemet med identitetsmissbruk på rättsväsendets agenda. Genom att betrakta olovlig identitetsanvändning som ett självständigt och fullbordat brott snarare än ett led i annan brottslighet ändras också utredningsmöjligheterna, exempelvis genom att det kommer att finnas ett större incitament att nyttja tvångsmedel (NBC 2014b, diarienr A010.488/2016). Det är dessutom angeläget[109] att enskilda som drabbas av att deras identitet missbrukas ges möjligheter att föra talan om skadestånd med hjälp av en åklagare – något som saknas med nuvarande reglering.

Däremot är det tveksamt om kriminaliseringen träffar flera specifika gärningar med bedrägligt uppsåt än dem som redan täcks av andra nuvarande straffbestämmelser i BrB 14 kap. och 15 kap. När det gäller själva vidgningen av kriminaliseringsområdet är den alltså sannolikt mer aktuell exempelvis i samband med olovligt bruk av andras identiteter på sociala medier, snarare än vid bedrägeri. Enligt polisen (NBC 2014b, diarienr A010.488/2016) förväntar man sig heller inte någon större, långvarig ökning i

[108] En relaterad lagändring, föreslagen i samma lagrådsremiss (men inte behandlad av utredningen), avser ett tillägg i straffbestämmelsen om olaga förföljelse. Denna vidgas till att omfatta även gärningar som utgör olovlig identitetsanvändning.

[109] Se remissyttrandet från Advokatsamfundet

bedrägerianmälningar, däremot en ökad belastning på andra rotlar.[110]

[110] Däremot kan det vara så att det i ett inledningsskede sker en ökning då den nya lagstiftningen uppmärksammats och fler väljer att anmäla försök till bedrägeri via ett identitetsintrång när detta just kriminaliserats.

Bilaga 6

Betalsystemets aktörer

I denna bilaga finns en genomgång av betalsystemets aktörer, vilket har bäring på framför allt bedrägliga köp. För att genomföra ett köp behövs förutom kunden och försäljaren betalsystemets aktörer, det vill säga de aktörer som administrerar kortbetalningar, som banker och betaltjänstaktörer.

Med betalsystemet menas här det system som tillhandahåller infrastruktur för att betalningar ska kunna genomföras. De tekniska innovationerna inom betalsystemen sker i snabbt tempo. Det innebär att nya aktörer etablerar sig och nya funktioner tillkommer. Till exempel utvecklas mobila betalningslösningar och olika typer av kreditbetalningar. Detta påverkar också riskerna för bedrägerier. För att denna genomgång snabbt inte ska bli inaktuell med dessa snabba förändringar beskrivs betalsystemet på en mer övergripande nivå.

För att ett kortköp ska kunna genomföras behöver kunden ett konto- eller kreditkort kopplat till ett konto; korten ges ut av kortutgivaren, vanligtvis en bank. Den säljande butiken behöver också avtal, bland annat med en bank, en systemleverantör och med en aktör som förmedlar betaltjänster mellan butik och bank (Arvidsson 2009). De sistnämnda (ofta refererade till som Payment Service Provider, PSP - på svenska s.k. betalväxlar) kan definieras som i princip alla typer av aktörer som inte är en kortutgivare eller bank, exempelvis Trustly, Paypal, Klarna och Swish.

Systemleverantörerna VISA och Mastercard är centrala aktörer vid en kortbetalning. De levererar infrastrukturen för betalprocesserna och tillhandahåller olika övergripande säkerhetsstandarder. En sådan är 3D Secure (Verified by Visa och Mastercard Secure Code) som är en säkerhetsfunktion vid betalning med Visa eller MasterCard på nätet. En annan kallas ofta ”chip och pin” (EMV-standarden, Europay MasterCard Visa). Den anses generellt vara säkrare än den tidigare mangnetspårstekniken.

Förekomsten av magnetspåret på kortet innebär dock att man fortfarande kan använda kortet hos vissa butiker och restauranger. En anledning till att magnetspåren fortfarande finns kvar på korten är att den nya tekniken inte är införd i alla länder. För att individer ska kunna handla i alla världens länder oavsett om landet infört EMV-standarden eller inte, behöver magnetremsan och betalmaskiner som läser magnetkort fortfarande finnas, menar intervjupersoner.

EU-lagstiftning kring kortbetalningar

I ett reviderat EU-direktiv (PSD2), som publicerades i slutet av 2015, utökas säkerhetskraven vid internetbetalningar, bland annat genom krav på så kallad *stark kundautentisering*.[111] En stark kundautentisering bygger på användning av två eller flera faktorer, så kallad *tvåfaktorsautentisering* (2FA). Två av följande faktorer ska ingå i identifieringen:

1. Kunskap. Något som enbart användaren känner till, t.ex. lösenord, kod, personligt id-nummer.
2. Ägande. Något som enbart användaren innehar, t.ex. säkerhetsdosa, mobiltelefon.
3. Tillhörighet. Något som användaren är, t.ex. biometriska kännetecken, såsom fingeravtryck.

Dessutom måste faktorerna vara oberoende av varandra, så att brott mot en faktor inte påverkar eller ger tillgång till de andra. Minst en av faktorerna bör också vara icke-återanvändbar och icke-replikerbar (utom för tillhörighet), och inte kunna bli stulen via internet. Rutiner för stark kundautentisering blir obligatoriska och ska tillämpas vid alla internetbetalningar, samt vid hantering av känsliga uppgifter om betalningar.

Visserligen ställer det nya EU-direktivet högre krav på säkerhet vid internetbetalningar, men kan också komma att bidra till säkerhetsrisker på nya områden, menar en intervjuperson med expertkunskap inom betalsystemen. Direktivet driver på den fortsatta avregleringen av betalmarknaden. Avregleringarna innebär att nya betaltjänstaktörer kommer att komma in på marknaden. De nya aktörerna kommer via bankerna att kunna få direkt tillgång till kundens person- och kontouppgifter. Det betyder att kunderna slipper registrera kortuppgifter varje gång ett köp görs. Kortuppgifter kan lagras och köp och betalningar kan göras enkelt och snabbt, med ett klick på en mobiltelefon.

[111] Europaparlamentets och rådets direktiv (EU) 2015/2366. Medlemsstaterna har till den 13 januari 2018 på sig att anta och offentliggöra de bestämmelser som är nödvändiga för att följa direktivet. (Europeiska unionens officiella tidning, L 337/35. 2015/12/23).

Samtidigt får fler aktörer tillgång till känsliga uppgifter som kan användas i bedrägliga syften. Intervjupersoner menar att det finns en särskild risk om de nya aktörerna saknar tillräckligt utvecklat säkerhetsarbete. I en övergångsperiod kan befintliga regleringar visa sig otillräckliga, menar en intervjuperson. Farhågor finns också för att mindre seriösa aktörer kan etablera sig på marknaden och få tillgång till kortuppgifter. Säkerhetskraven kan komma att behöva justeras och utvecklas ytterligare.

Bedrägeribrotten ökar i samhället. Det visar både frågeundersökningar till befolkningen och kriminalstatistiken. I den här rapporten beskrivs de senaste årens utveckling av bedrägeribrottsligheten, vilka typer av bedrägerier och bidragsbrott som anmäls till polisen och vilka problem som rättsväsendet möter i sitt arbete att utreda och lagföra de anmälda brotten. Vidare beskrivs hur identitetsmissbruk används som ett led i brottsligheten samt hur näringslivet och myndigheters arbete kan påverka förutsättningarna för olika typer av bedrägeribrott.

Rapporten vänder sig till personer inom rättsväsendet, på kontrollmyndigheter och inom näringslivet som arbetar med att förebygga och utreda bedrägerier och bidragsbrott.

ISBN 978-91-87335-65-5 • URN:NBN:SE:BRA-651 • ISSN 1100-6676

Brottsförebyggande rådet/National Council for Crime Prevention
BOX 1386/TEGNÉRGATAN 23, SE-111 93 STOCKHOLM, SWEDEN
TELEFON +46 (0)8 527 58 400 • FAX +46 (0)8 411 90 75 • E-POST INFO@BRA.SE • WWW.BRA.SE