JURIDISKA INSTITUTIONEN
Stockholms universitet

Bedrägerier över internet

- medelst stulna identiteter

Behrang Eslami

Examensarbete med praktik i *Straffrätt*, 30 hp
Examinator: Josef Zila
Stockholm, Vårterminen 2015

Stockholms universitet

Sammanfattning

Den snabba tekniska utvecklingen och det explosionsartade användandet av elektroniska instrument så som datorer och smarttelefoner som är uppkopplade till internet har inneburit en förflyttning av bedrägeribrotten, där allt fler bedrägeribrott sker över internet. Enligt Brå är denna typ av brottslighet den nya vardagsbrottsligheten och trenden pekar uppåt. Under 2013 anmäldes 148 000 bedrägeribrott varav 17 % hade ursprung i ett identitetsintrång. Internetanvändandet syns tydligt i människors beteendemönster när de betalar sina räkningar. År 1999 betalade 9 % av Sveriges befolkning regelbundet sina räkningar över internet. År 2012 hade siffran stigit till 79 %. [1]

Med nätbankernas, kreditföretagens och nätbutikernas intåg som en naturlig del i vårt samhälle har brottsligheten hittat en ny källa för att tillskansa sig ekonomisk vinning. De traditionella rån brotten med kofot, skarpladdade vapen, rånarluvor och flyktbil har bytts ut till en ny sorts högteknologiska bedrägeribrott. Brotten sker genom manipulation och virus som skickas ut av skickliga datorhackare som sopar igen spåren efter sig med enorm skicklighet. Problemet påverkar många i samhället och gärningsmännen lyckas på något vis alltid överlista de olika säkerhetsanordningar som finns.

I arbetet redogörs för vad som utgör ett internetbedrägeri med stulen identitet, vilka tillvägagångssätt som bedragarna använder sig av, vilka straffansvar som följer samt en redogörelse för praxis på området. Sedermera tas upp vad de genomförda internetbedrägerierna har kunnat och kan resultera i, för att sedan belysa svårigheten med bevissäkring och hur ett effektivt förundersökningsarbete kan bedrivas. Slutligen följer en redogörelse för varför en stor del av de anmälda brotten inte leder till åtal eller i vissa fall till relativt korta påföljder för de utförda gärningarna.

Vi får följa ett brottsoffer som har fått sin identitet stulen och blivit utsatt för bedrägerier till ett värde av cirka 700 000 kronor. Ett av kreditföretagen, där ett lån hade tagits i brottsoffrets namn, valde sedermera att stämma brottsoffret. I uppsatsen redogörs även för hur en förundersökningsledare som arbetar inom polisens bedrägerirotel ser på systematiken i bedrägeribrott som begås över internet med stulna identiteter och hur en f.d. åklagare som numera är bedrägerispecialist inom polismyndigheten arbetade och numera arbetar för att bekämpa brottslig-

[1] Svenska Bankföreningen, Banker i Sverige 2013.

heten. Intervjuerna tas oss med på en resa där de delar med sig av sina erfarenheter och ger sin syn på rättsområdet.

I analysen diskuteras kring de mekanismer som har lett till att bedrägeribrotten över internet med stulna identiteter har blivit så omfattande och varför rättssystemet inte kan sätta stopp för dem, för att därefter komma fram till en slutsats som utmynnar i ett konkret förslag på vilka praktiska och juridiska lösningar som kan finnas. För att komma till bukt med problematiken kan skärpta straff för bedrägeribrott vara en lösning. Ett annat tillvägagångssätt vore att lagstifta, för att genom en ad hoc lösning säkerställa att kreditgivare och företag som säljer varor och tjänster på kredit över internet säkerställer beställarens identitet genom tekniska lösningar.

I lagförslaget presenteras en teknisk lösning där kreditgivare genom elektronisk identifiering säkerställer kredittagarens eller beställarens identitet. Förslaget presenteras ur både näringsidkarnas perspektiv, konsumenternas perspektiv och ur samhällsekonomisk synvinkel.

Innehållsförteckning

Förkortningar

BrB	**Brottsbalken (1962:700)**
RB	**Rättegångsbalken (1942:740)**
PL	**Polislag (1984:387)**
RF	**Regeringsformen (1974:152)**
HD	**Högsta domstolen**
NFC	**Nationellt forensiskt centrum**
NBC	**Nationellt bedrägericentrum**
Brå	**Brottsförebyggande rådet**
RPS	**Rikspolisstyrelsen**
IT	**Informationsteknologi**
NJA	**Nytt juridiskt arkiv**
IP	**Internet protokoll adress**
VPN	**Virtuellt privat nätverk**
Kap	**Kapitel**
DNS	**Domännamnssystem**
ÅFS	**Åklagarmyndighetens föreskrifter och allmänna råd**
RPSFS	**Rikspolisstyrelsens föreskrifter och allmänna råd**
RAR	**Polisens anmälningssystem**

Förord

Med anledning av den snabba tekniska utvecklingen i samhället och det utbredda användandet av internet och elektroniska hjälpmedel, har även tillvägagångssätten för att utföra brottsliga gärningar förändrats. Ämnet har väckt stor medial uppmärksamhet efter att bedrägerier över internet på senare år har drabbat många, såväl privatpersoner som företag.

Då jag själv fick min identitet stulen år 2011, i ett fall där bedragarna lyckades ta flertalet krediter i mitt namn, väcktes ett stort intresse av att forska inom ämnet.

Jag har i samband med uppsatsskrivandet praktiserat på Advokaterna Hurtig & Partners, där jag har fått delta i det vardagliga arbetet på byrån. Arbetet har inneburit praktiskt arbete med att författa rättsutredningar, analysera domar och rättsfall, ta klientmöten samt att följa med på förhandlingar i domstol. Uppsatspraktiken har varit oerhört lärorik och jag vill tacka samtliga kollegor på Advokaterna Hurtig & Partners för den lärorika tiden, det varma mottagandet, tålamodet och hjälpsamheten. Ett synnerligt tack vill jag rikta till advokaterna Johan Åkermark och Johan Rainier för förtroendet.

Min kära mor, som alltid har bidragit med motivation, stöd och kärlek vill jag rikta en enorm tacksamhet till. Hon har lärt mig att alltid, oavsett vad, stå upp för rättvisan. Utan min mor hade jag inte varit där jag är idag!

Sist men inte minst vill jag tacka mitt födelseland Sverige, som har gett mig möjligheten att växa upp i ett tryggt land, där man får studera avgiftsfritt och har alla förutsättningar att bli framgångsrik och växa upp till att bli en god medborgare. Nu är det dags att betala tillbaka genom att stå upp för rättvisa och objektivitet. Tack Sverige!

1. Inledning

Föreställ dig att du inom loppet av en vecka får hem kreditupplysningar från ett tiotal olika företag och kreditinstitut. Av kreditupplysningarna framgår att du eller någon som utgett sig för att vara du, har ansökt om krediter eller försökt att köpa varor på kredit uppgående till sammanlagt flera hundratusen kronor. Hjärtat börjar bulta, svetten börjar rinna i pannan och du börjar andas häftigt. Kan du ha glömt att du har tagit dessa krediter? Har du börjat bli senil? Eller kan det helt enkelt vara så att någon har utgett sig för att vara du och försökt tillskansa sig ekonomisk vinning genom att ansöka om krediter och att köpa varor på kredit i ditt namn?! Hur bör du gå tillväga? Vem ska du vända dig till? Frågorna är många och för den som inte är insatt är svaren sällan självklara.

Bedrägerier som begås över internet brukar samlas under benämningen ”nätbedrägerier”. Man använder även begreppen IT-relaterad brottslighet och IT-brott. Dataintrång är det som avses med IT-brott medan man med IT-relaterad brottslighet brukar åsyfta att förövaren använder sig av digital teknik för att genomföra brottet. Just bedrägerier är nuförtiden ofta IT-relaterade.[2]

Nätbedrägerier har ökat explosionsartat i takt med den tekniska utvecklingen och bidrar till att allt fler typer av bedrägerier kan begås. Under år 2012 drabbades cirka 219 000 (16 – 79 år) personer av bedrägeribrott, vilket motsvarar cirka 3 procent av befolkningen i Sverige.[3] Statistik visar att under samma år stals 65 000 svenskars identiteter och varor som de utsatta aldrig beställt, beställdes till ett värde av 2,7 miljarder kronor.[4] Det kan ställas i relation till det totala antalet anmälda bedrägeribrott, som år 2013 uppgick till 148 000. [5]

Den ökade utsattheten beror till stora delar på den ökade internetanvändningen som har skett med anledning av den tekniska utvecklingen. Med hjälp av olovlig hantering av personuppgifter kan bedragare ansöka om att köpa tjänster, ta krediter, eller köpa varor med någon annan privatpersons identitet.

---

[2] Ahola, Mikael, Bedrägeri: introduktion och handledning för brottsutredare, 2013, s. 80

[3] Färdeman, Hvitfeldt, Irlander, Brottsförebyggande rådet, Utsatthet för brott år 2012, Resultat från nationella trygghetsundersökningen (NTU), 2013, s. 22

[4] Motion 2013/14:Ju216, riksdagen.se.

[5] Brottsförebyggande rådet, Bedrägeri och ekobrott, http://www.bra.se/bra/brott-och-statistik/bedragerier-och-ekobrott.html, hämtad 2014-01-15

1.1 Syfte

Arbetets syfte är att redogöra för tillvägagångssätten som bedragarna använder sig av för att begå bedrägerier över internet med stulna identiteter, vilka medel förövarna använder sig av, vilka straffansvar som följer och vilka tvångsmedel myndigheterna kan använda sig av för att utreda brott. Genom att redogöra för gällande rätt på området såväl som att analysera hur det kommer sig att så få anmälda brott leder till fällande dom, är syftet att klargöra för om och eventuellt vilka luckor som finns i dagens lagstiftning. Slutligen följer en presentation av ett förslag på hur arbetet med att proaktivt förhindra nätbedrägeribrott skulle kunna ske. Fokus i arbetet ligger på bedrägeribrott som utförs över internet, men omfattar till viss del även missbruk av urkund, urkundsförfalskning och oredligt förfarande.

Följande frågeställningar kommer att behandlas:

- På vilka sätt utförs de aktuella brotten?
- Varför leder så få anmälda brott till fällande dom?
- Hur kan man hitta metoder för att komma till rätta med internetbedrägerier som utförs med stulna identiteter?

1.2 Metod, material och avgränsningar

Genom att granska hur bedrägerier över internet med stulna identiteter genomförs presenteras några av de vanligaste metoderna som används för att begå brotten, vilka medel förövarna använder sig av och svårigheten med att ställa bedragarna till svars. Jag kommer således att fastställa gällande rätt och vilka tillvägagångssätt polisen och åklagarmyndigheten använder sig av vid bedrivande av förundersökning genom att intervjua en förundersökningsledare inom polisens bedrägerirotel och en f.d. åklagare som numera arbetar som bedrägerispecialist inom polismyndigheten. Med deras hjälp analyserar jag vilka luckor som finns i aktuell lagstiftning och arbetsmetodik. Slutligen är ambitionen att nå fram till en slutsats i hur man skulle kunna komma tillrätta med problematiken att så många bedrägeribrott över internet genomförs och att så få gärningsmän blir dömda för de begångna gärningarna.

Målet med arbetet har varit att ge en heltäckande bild av nätbedrägeribrott med stulna identiteter, vilket till viss del även kan omfatta vissa kortbedrägerier. Dock har vissa avgränsningar gjorts för att arbetet inte ska bli för omfattande och kortbedrägerier kommer således inte att behandlas särskilt detaljerat. Fokus ligger istället på nätbedrägeribrott där stulna identiteter har använts för att med uppsåt tillskansa sig krediter, varor på kredit eller renodlade datorkapningar med syfte att ge gärningsmannen ekonomisk vinning. Inte heller kommer någon större fördjupning att ske i försök eller förberedelse till bedrägeribrott över internet eller underlåtenhetsbrott.

Ett omfattande fokus ligger på bevisfrågor, då internetbedrägerier är svåra att bevisa, vilket kommer att redogöras för i arbetet.

Jag har även valt att intervjua ett brottsoffer som har blivit utsatt för ett bedrägeri med urkundsförfalskning, till syfte att redogöra för hur ett bedrägeribrott upplevs ur brottsoffrets perspektiv och vilka följder det kan få.

I de rättsfall där åtgärderna har lett till åtal kommer påföljderna att redogöras för och i en analys att kommenteras.

Genom att analysera de allmänt vedertagna rättskällorna, lag, förarbeten, rättspraxis och doktrin redogör jag för vad som är karakteriserande för bedrägeribrott, vilseledande och urkundsförfalskning. [6] När de nuvarande straffbestämmelserna kom till var det för att den vilseledde många gånger drabbades av skadan. Nuförtiden drabbas även kreditinstitut eller företag som exempelvis säljer varor på kredit.

Därefter sker en genomgång av de tekniska hjälpmedel som används vid nätbedrägerier, för att läsaren ska få bättre förståelse för hur ett internetbedrägeri i praktiken kan gå till.

I analysen kommer jag slutligen ge min syn på hur lagstiftaren kan agera för att komma till rätta med internetbedrägerier som sker med hjälp av stulna identiteter och på ett förebyggande sätt kunna bekämpa dem. Det lagförslag som presenteras i analysen har till syfte att skydda både brottsoffer, kreditinstitut eller säljande företag och samhället. Genom att försvåra för gärningsmännen att begå de aktuella brotten, tror jag att det kan leda till en drastisk nedgång i antalet nätbedrägeribrott med stulna identiteter.

[6] Kleineman, Juridisk metodlära, Korling, Zamboni, Studentlitteratur, 2013, s. 21-28

1.3 Disposition

Närmast i framställningen följer en redogörelse för vad som utgör bedrägeri och vilka rekvisit som ska vara uppfyllda för att ett bedrägeri ska vara fullbordat i lagens mening. Därefter sker en presentation av vilket straffansvar som följer vid fullbordade bedrägerier och vilka rekvisit som behöver vara uppfyllda för att ett bedrägeri ska anses som grovt.

I kapitel 3 redogörs för vad som menas med en stulen identitet och vilka rekvisit som behöver vara uppfyllda för att brotten missbruk av urkund och urkundsförfalskning ska vara fullbordade. Sedermera beskrivs hur man kan få klart för sig att ens identitet kan ha blivit stulen och vilka åtgärder som bör vidtas om olyckan är framme.

I kapitel 4 behandlas begreppet nätbedrägerier och hur de faktiskt kan gå till. Kapitlet handlar om de tillvägagångssätt som bedragarna kan använda sig av och belyser även svårigheten med bevis och bevissäkring. För att underlätta för läsaren kommer flertalet tekniska begrepp att redas ut, för att läsaren ska få bättre förståelse för vilka verktyg bedragarna använder sig av och hur de praktiskt fungerar. Jag kommer även att ta upp konkreta exempel på fall där nätbedrägerier har genomförts och vilka skador de har orsakat brottsoffren.

Kapitel 5 handlar om rättspraxis och korta rättsfallsreferat från fall där nätbedrägerier har genomförts och vilka påföljder som har utdömts.

I kapitel 6 sägs först något om polis och åklagares arbete respektive ansvar vid brottsutredningar och väckande av åtal. Därefter redogörs för vilka tvångsmedel som står till buds vid bedrivande av förundersökning.

Kapitel 7 presenterar en analys av de intervjuer som har genomförts med ett brottsoffer, en förundersökningsledare inom polisen och en tidigare åklagare som nu arbetar som bedrägerispecialist inom polismyndigheten. En presentation ur deras perspektiv på nätbedrägerier kommer ske för att slutligen utmynna i hur förundersökningsledaren respektive åklagaren skulle vilja att en eventuell lagändring eller förändring i arbetsmetodiken inom polismyndigheten och domstolarna bör ske för att stävja omfattningen av antalet nätbedrägerier och problematiken med att så få anmälda brott leder till fällande dom.

I kapitel 8 presenteras en analys där jag ger min syn på hur arbetet kan ske proaktivt för att på ett förebyggande sätt kunna förebygga nätbedrägerier, med fokus på elektronisk kreditgiv-

ning, då en stor del av nätbedrägerier med stulna identiteter sker vid elektronisk kreditgivning och elektronisk försäljning av varor på kredit.

Slutligen sker en presentation av ett lagförslag i kapitel 9, som har till syfte att skydda konsumenter från att få sina identiteter stulna och få krediter tagna i sitt namn. Lagförslaget motiveras noga och presenteras till förmån för både konsumenter, näringsidkare och samhället samt kommenteras ur samtliga perspektiv.

I slutordet knyter jag an till det som sades i förordet om min personliga erfarenhet av att bli utsatt för bedrägeri.

2. Om bedrägeri

Bedrägeri innebär att någon genom att agera uppsåtligt vilseleder annan eller företar en underlåtenhet till skada för den som bedras och till vinning för bedragaren. Vilseledandet kan ske på en mängd olika tillvägagångssätt. Bland annat kan en bedragare genom att lämna oriktiga uppgifter, genom manipulation av uppgifter, utsändande av falska fakturor eller så kallad ”skimming”, utföra en handling som leder till vinning för bedragaren. Med ”skimming” menas en form av kortkapning, där någon olovligen tillskansar sig informationen i magnetremsan på ett kontokort som sedan läggs över på ett annat kort.

En förutsättning för att ett bedrägeri ska anses vara förövat är att brottsoffret har vilseletts. Genom vilseledandet utför gärningsmannen en handling eller underlåtenhet, en disposition. Vilseledandet kan även bestå i att brottsoffret förmås att utföra en disposition i form av en handling eller underlåtenhet. När brottsoffrets förmås till en disposition i form av en underlåtenhet hör det till vanligheten att underlåtenheten är omedveten. Medan det i fall som brottsoffret företar en viss handling, handlingen sker medvetet dock utan vetskap om konsekvensen av handlingen.[7]

Bedrägeri kan även utföras genom så kallat datorbedrägeri, vilket framgår av 9 kap 1 § andra stycket BrB. Arbetets fokus är bedrägeribrott som begås över internet med stulna identiteter, vilket även innefattar datorbedrägerier.

Av 9 kap. 1 § BrB framgår vad lagstiftaren anser vara ett bedrägeri; ”*Den som medelst vilseledande förmår någon till handling eller underlåtenhet, som innebär vinning för gärnings-*

[7] Jareborg, Asp, Friberg, Ulväng, Brotten mot person och förmögenhetsbrotten, 2 uppl., Iustus, 2015, s. 219-228

mannen och skada för den vilseledde eller någon i vars ställe denne är, dömes för bedrägeri till fängelse i högst två år.
För bedrägeri döms också den som genom att lämna oriktig eller ofullständig uppgift, genom att ändra i program eller upptagning eller på annat sätt olovligen påverkar resultatet av en automatisk informationsbehandling eller någon annan liknande automatisk process, så att det innebär vinning för gärningsmannen och skada för någon annan".

Med internetbedrägeri avses att det aktuella brottet ska ha ägt rum på internet vilket även omfattar anstiftan, förberedelse och försök till bedrägeri som är straffbara enligt 9 kap. 11 § BrB och 23 kap. 1-2 §§ BrB.

För att bedrägeri ska rubriceras som grovt enligt 9 kap. 3 § BrB beaktas särskilt om gärningsmannen missbrukat allmänt förtroende eller begagnat falsk handling. Om gärningsmannen har använt vilseledande bokföring eller om gärningen har varit av särskilt farlig art, avsett betydande värde eller inneburit synnerligen kännbar skada är också faktorer som beaktas.

Det har i lagtexten inte ställts något krav på att en fysisk person ska ha vilseletts till någon form av disposition. Ett bedrägeribrott föreligger således när gärningsmannen olovligen påverkar resultatet av en automatisk informationsbehandling eller en process som kan liknas vid det, om förfarandet innebär vinning för gärningsmannen och skada för den som drabbas. Eftersom det i lagtexten inte anges vem som ska ha lidit skadan, behöver inte domstolen avgöra den ibland komplicerade frågan om vem som har lidit den omedelbara skadan. Det som är avgörande för ett fullbordat bedrägeribrott är om det har skett en förmögenhetsöverföring som är resultatet av att gärningsmannen olovligen har ingripit i den automatiska informationsbehandlingen och på så vis påverkat det slutliga utfallet.

Om gärningsmannen olovligen påverkar en automatisk informationsbehandling utan att förmögenhetsöverföring sker, döms gärningsmannen istället för oredligt förfarande enligt 9 kap. 8 § BrB. För oredligt förfarande döms gärningsmannen om gärningen inte har inneburit vinning för gärningsmannen men gärningen i övrigt svarar mot bedrägeri. För att dömas för oredligt förfarande krävs dock att ett vilseledande ska ha skett. [8]

Karakteriserande för bedrägeribrott är att gärningsmannen genom vilseledandet, vilket kan beskrivas som att genom att orsaka någon eller något att felaktigt tro något, förmår någon

[8] Prop. 1985/86:65 s. 43-45

eller något till en handling eller underlåtenhet som slutligen innebär en förmögenhetsöverföring.[9]

Orsakande av handlingen, dispositionen, sker i många fall utan den bedragnes vetskap vid nätbedrägerier. Man har i praxis gjort avsteg från att det måste vara en medveten disposition för brottsoffret. I praxis har man dömt för bedrägeri även om brottsoffret inte har haft någon uppfattning om en disposition. Det karakteriserande har varit att brottsoffret inte har utfört dispositionen och således inte vetat om dispositionen eller haft för avsikt att dispositionen ska ske.[10]

2.2 Vilseledande

Ett vilseledande består i att framkalla en felaktig föreställning hos offret eller att skapa, vidmakthålla eller förstärka en villfarelse som brottsoffret redan har.[11] Den straffbara gärningen vid bedrägeri består i ett vilseledande som gör att den som vilseletts vidtagit en åtgärd eller underlåtit att göra något som inneburit skada för brottsoffret och vinning för gärningsmannen. Det är den vilseleddes perspektiv som är utgångspunkt vid bedömningen av vilseledandet. Även om den som har vilseletts framstår som lättlurad och naiv för att ha ”gått på” gärningsmannens vilseledande, föreligger även ett vilseledande i lagens mening. För många bedrägerier är det kännetecknande att de drabbade ofta är personer som på grund av hög ålder eller nedsatt förmåga att motstå erbjudanden som kan te sig lockande blir bedragna. [12]

[9] Jareborg, Asp, Friberg, Ulväng, Brotten mot person och förmögenhetsbrotten, 2 uppl., Iustus, 2015, s. 219-220

[10] Jareborg, Asp, Friberg, Ulväng, Brotten mot person och förmögenhetsbrotten, 2 uppl., Iustus, 2015, s. 233-234

[11] Jareborg, Asp, Friberg, Ulväng, Brotten mot person och förmögenhetsbrotten, 2 uppl., Iustus, 2015, s. 220

[12] Holmquist, Rolf, Brotten i näringsverksamhet, Norstedts, 2013, s. 90-91

2.3 Vad innebär förmögenhetsöverföring?

Med förmögenhetsöverföring avses att den skadelidande ska ha åsamkats lidande i form av en ekonomisk skada samtidigt som bedragaren eller någon annan ska ha fått ekonomisk vinning av handlingen.[13]

Bedrägeri består sammanfattningsvis av ett vilseledande som orsakar någon form av disposition och som sedermera leder till förmögenhetsöverföring till vinning för bedragaren och till skada för den bedragne.

Dispositionen ska innebära både skada för brottsoffret och vinning för gärningsmannen i form av förmögenhetsöverföring, för att ett bedrägeri ska vara förövat. Gärningsmannens vinning såväl som annan som gärningsmannen med uppsåt bereder vinning, är straffbart och karakteriseras som bedrägeri enligt BrB 23:7.[14]

2.4 Vilka straffansvar råder vid bedrägeri?

9 kap 1 § BrB definierar vad som utgör bedrägeri. För bedrägerier över internet kan det omfatta att gärningsmannen olovligen har tagit över en annan persons identitet, genom vilseledande eller underlåtenhet fått vinning av handlingen och skadat den bedragne. Vid bedrägeribrott döms gärningsmannen till fängelse i upp till två år. Vid grovt brott döms gärningsmannen till fängelse i lägst sex månader och högst sex år, vilket framgår av 9 kap 3 § BrB.

Den som utger sig för att vara någon annan eller sanningslöst åberopar annans identitetshandling, gör sig skyldig till missbruk av urkund, BrB 15 kap 12 §. Straffansvar råder med böter eller fängelse i högst sex månader som följd. Om brottet är att anse som grovt, döms till fängelse i högst två år.

Vid bedrägeribrott döms vanligtvis till villkorlig dom och böter som påföljd. I praxis kan man se att det råder en betydande försiktighet att vid straffmätningen när påföljden rubriceras som grovt bedrägeri. Det framgår bland annat av rättsfallet NJA 1983 s. 441. HD:s praxis kan tolkas på så vis att brottets art som argument vid bedrägeribrott i regel inte talar för fängelse som

[13] Friberg, Brottsbalk (1962:700) 9 kap. 1 §, Lexino 2013-05-15

[14] Jareborg, Asp, Friberg, Ulväng, Brotten mot person och förmögenhetsbrotten, 2 uppl., Iustus, 2015, s. 244

påföljd. I många av NJA-fallen har påföljdsfrågan inte refererats utan fokus har legat på frågor som har att göra med huruvida de olika rekvisiten för brottet har varit täckta av uppsåt. Slutsatsen blir att bedrägeribrottens art inte tillmäts någon större betydelse som skäl för fängelse vid bedrägeribrott.

Det framgår av brottstatistik att det år 2011 dömdes eller meddelades straffansvar eller meddelades strafföreläggande för bedrägeri till böter i endast 16 fall. Till strängare påföljd dömdes det i 897 fall. Av dessa utdömdes 99 fängelsestraff, skyddstillsyn i 180 fall varav 1 med fängelse. I 11 fall dömdes även till kontraktsvård och i 21 fall utdömdes även samhällstjänst som en förstärkning av skyddstillsynen. Av samtliga 897 fall, där påföljden inte stannade vid böter, fick gärningsmännen villkorlig dom i 578 fall, varav det i 15 av fallen även utdömdes samhällstjänst. 2 fall överlämnades till rättspsykiatrisk vård, samtidigt som det i 13 fall dömdes till ungdomsvård och till ungdomstjänst i 25 fall.[15]

Det genomsnittliga fängelsestraffet var 4 månader. Det högsta fängelsestraffet, två år, utdömdes i 5 fall. I 505 fall utdömdes böter, där böter kombinerades med villkorlig dom i de flesta fall.

Till grovt bedrägeri dömdes samma år till böter i endast 1 fall. Av samtliga 324 grova bedrägerier som utfördes under år 2011 dömdes till fängelse i 153 fall. I 51 fall dömdes till skyddstillsyn, varav 1 med fängelse, 5 med kontraktsvård och 5 med samhällstjänst. I 115 fall dömdes till villkorlig dom, varav det i 27 fall förenades med samhällstjänst. I ett av fallen överlämnades gärningsmannen till rättspsykiatrisk vård. Vidare dömdes till ungdomsvård i 2 av fallen och till ungdomstjänst i 1 fall. Det genomsnittliga fängelsestraffet för de som dömdes till fängelse för grovt bedrägeri var 1 år och 7 månader. I 34 fall dömdes till fängelse mellan två och fyra år och till mer än fyra år i 1 fall.[16]

2.4.1 Vad avgör om ett bedrägeri ska rubriceras som grovt?

För att utdöma straffansvar för grovt bedrägeri beaktar man särskilt huruvida gärningsmannen har begagnat falsk handling. Om beloppet som bedrägeriet avser inte kan bedömas som sär-

[15] Sterzel, Månsson, Borgeke, Kezovska, Palm, Reimer, Påföljdspraxis, 5 uppl., Jure Förlag, 2013, s. 559-560

[16] Sterzel, Månsson, Borgeke, Kezovska, Palm, Reimer, Påföljdspraxis, 5 uppl., Jure Förlag, 2013, s. 559-560

skilt betydande, döms istället för bedrägeribrott av normalgraden och urkundsförfalskning. Ett halvt basbelopp är en beloppsgräns som tillämpas.[17]

Det framgår av lagkommentaren till 9 kap 3 § BrB att det vid bedömande av huruvida brottet är grovt krävs en helhetsbedömning. Särskilt beaktas om gärningsmannen missbrukat allmänt förtroende, begagnat falsk handling, om gärningen varit av särskilt farlig art, avsett betydande värde eller inneburit synnerligen kännbar skada. Beträffande värdet gör man en objektiv bedömning, medan det avseende synnerligen kännbar skada avgörs genom en subjektiv bedömning. En riktlinje som tillämpas i praxis för tolkningen av betydande värde är densamma som vid grov stöld (8 kap. 4 § BrB), nämligen fem basbeloppet, vilket för närvarande uppgår till cirka 220 000 kr.[18]

3 Vad innebär identitetskapning?

Med identitetskapning menas att en gärningsman olovligen tar över en annan persons identitetsuppgifter. Genom att kapa annans identitet kan gärningsmannen beställa varor eller ta krediter i dennes namn. Det kan handla om en persons namn, personnummer, adress eller andra uppgifter som innebär att bedragaren kan legitimera sig som brottsoffret, för att tillskansa sig varor, krediter eller annat som leder till vinning för bedragaren och till skada för den bedragne.

ID-kontrollen är i den dagliga handeln många gånger undermålig. Oerfarna och unga butiksbiträden har många gånger inte fått någon grundlig genomgång i hur man utför en kontroll av en ID-handling och hur en ID-kontroll bör genomföras för att säkerställa att handlingen är äkta och tillhör personen som utger sig för att vara den som legitimerar sig. Det kan hända att ID-handlingen inte granskas gentemot den person som lämnat fram ID-handlingen. Oavsett om kortet är äkta eller en välgjord kopia, hjälper det inte såvida man inte kontrollerar identiteten på den som utger sig vara personen på den presenterade ID-handlingen. [19]

[17] Sterzel, Månsson, Borgeke, Kezovska, Palm, Reimer, Påföljdspraxis, 5 uppl., Jure Förlag, 2013, s. 560

[18] Friberg, Brottsbalk (1962:700) 9 kap. 3 §, Lexino 2012-07-01

[19] Ahola, Mikael, Bedrägeri: introduktion och handledning för brottsutredare, 2013, s. 98

ID-kapning är i sig att anse som ett dataintrång enligt 4 kap. 9 § BrB. Däremot konsumeras det olagliga intrånget vid bedrägerier.[20]

3.1 Missbruk av urkund

Med urkund avses enligt 14 kap 1 § andra stycket BrB en handling som har upprättats till bevis, har betydelse som bevis och som har en utställarangivelse och originalkaraktär. Det kan också vara en elektronisk handling som har upprättats till bevis eller har betydelse som bevis, där en utställarangivelse som kan kontrolleras föreligger som även kan kontrolleras på ett tillförlitligt sätt. En urkund kan även utgöras av ett bevismärke som har originalkaraktär, som har ställts ut till bevis om en persons identitet, om en viss rättighet eller prestation.

Den som utger sig för att vara en annan person, genom att åberopa en identitetshandling, pass eller annan urkund som är utställd till viss person, gör sig skyldig till brottet missbruk av urkund. Brottet kan även bestå av att gärningsmannen använder sig av en kopia av en identitetshandling, pass eller annan urkund och påstår att det är en riktig kopia av handlingen. Förfarandet är brottsligt och gärningsmannen kan dömas för missbruk av urkund till böter eller fängelse i högst sex månader. Om brottet är grovt, döms till fängelse i upp till två år, enligt 15 kap 12 § BrB.

I vardagligt språkbruk kallas förfarandet identitetsstöld eller identitetskapning.[21]

3.1.2 Urkundsförfalskning

Den som genom att skriva annan, verkligen eller påhittad, persons namn eller genom att på annat sätt falskeligen förskaffa sig annans underskrift, framställer falsk urkund eller genom förfalskning fylla ut en äkta urkund under förutsättning att åtgärden innebär fara i bevishänseende, döms för urkundsförfalskning. För brottet råder straffansvar och gärningsmannen kan dömas till fängelse i upp till två år, enligt 14 kap 1 § BrB.

[20] Ahola, Mikael, Bedrägeri: introduktion och handledning för brottsutredare, 2013, s. 96

[21] Polisen, Identitetsstöld – Skydda dig, https://polisen.se/Utsatt-for-brott/Skydda-dig-mot-brott/Bedrageri/Identitetsstold---Skydda-dig/ (Hämtad 2015-02-19)

För ringa brott, döms gärningsmannen enligt 14 kap 2 § BrB för förvanskning av urkund till böter eller fängelse i högst sex månader. För att brottet ska bedömas som ringa krävs att urkunden ska ha varit av mindre betydelse eller att gärningen har begåtts för att hjälpa någon till hans eller hennes rätt.

Om brottet är grovt, döms för grov urkundsförfalskning till fängelse i lägst sex månader och högst sex år, enligt 14 kap 3 § BrB. Vid bedömande av om brottet ska anses som grovt tar man i beaktande om förfalskningen har avsett en arkivhandling av vikt hos myndighet, eller om urkunden har utgjort en handling som är särskilt betydelsefull i den allmänna omsättningen. Hänsyn tas också till om gärningen är av särskilt farlig art.

3.1.3 Skillnaden mellan falsk respektive osann urkund

När en person gör sig skyldig till urkundsförfalskning är urkunden falsk. Till skillnad från vid osant intygande så är urkunden osann. När en urkund är falsk innebär det att den till alla delar inte härrör från den angivna utställaren av urkunden. Det innebär därmed att den angivna utställaren inte står bakom det som ska bevisas med urkunden. Man åstadkommer en falsk urkund genom att utföra ett angrepp på handlingen eller bevismärket i sig. En äkta urkund blir falsk genom att gärningsmannen fyller ut eller falskeligen ändrar urkunden.

En osann urkund är inte korrekt i sak. Det kan handla om att någon för skens skull upprättar en urkund rörande en rättshandling. Vid lämnandet av en osann uppgift om vem man är kan det bedömas som urkundsförfalskning. Man har i praxis ansett att handlandet vid osant intygande av urkunder av mindre vikt och i vissa situationer bör föranleda straffansvar enligt 15 kap 11 § BrB för osant intygande. Det har gällt fall där den som har skrivit under en handling inte velat att det ska framgå att personen i fråga skrivit under handlingen utan istället velat dölja sin identitet. Om gärningsmannen har syftat till något mer än att lämna en oriktig identitetsuppgift så har denne istället dömts för urkundsförfalskning.

För att straffansvar för osant intygande ska aktualiseras krävs att den framställda falska eller osanna urkunden måste innebära fara i bevishänseende. Det innebär att det måste ha förelegat fara för att urkunden ska ha kommit till användning, att den ska ha kunnat förväxlas med en äkta eller sann urkund samt att ett användande sannolikt skulle medföra skada eller olägenhet. För att det ska vara fråga om en urkund krävs inte att innehållet behöver vara av kvalificerat

slag. Bevisvärdekravet är knutet till rekvisitet fara i bevishänseende som syftar på själva åtgärden och inte på begreppet urkund. Det är således förfalskningsåtgärden eller lämnandet av den osanna uppgiften som ska innebära fara i bevishänseende. Även om gärningsmannen framställer en falsk urkund på sådant vis att förfalskningen kan avslöjas, kan det innebära straffansvar för urkundsförfalskning enligt 14 kap 1 § BrB. Om gärningsmannen har haft uppsåt att bruka den falska urkunden kan det räcka för att straffansvar ska aktualiseras. [22]

3.2 Hur får man klart för sig att ens identitet har blivit stulen?

Om man upptäcker att någon har köpt varor, tjänster eller tagit krediter i ens namn, kan man ha råkat ur för bedrägeri genom identitetsstöld. Det kan gå till på så vis att man brevledes får hem kopior på kreditupplysningar som har tagits i ens namn, bekräftelse på utförda köp av varor eller tjänster eller fakturor och kvitton avseende köp av varor eller tjänster. [23]

Kreditupplysningsföretagen har skyldighet att i enlighet med 11 § kreditupplysningslagen (1973:1173) skicka en kopia på kreditupplysningen till den som avses med upplysningen. Åtgärden ska ske samtidigt som upplysningen görs och är kostnadsfri för den som kreditupplysningen avser. I kopian ska framgå vem som bedriver kreditupplysningsverksamheten, ändamålen med behandlingen, de uppgifter som upplysningen innehåller, möjligheten att få rättelse av eventuella uppgifter samt vem som har begärt upplysningen.

3.3 Vad ska man göra om man har fått sin identitet stulen?

Om en person har fått sin identitet stulen bör händelsen genast polisanmälas. Det kan ha gått till på det viset att någon har försökt köpa varor, tjänster eller ta krediter i ens namn. Vid upptäckt bör man samtidigt vidta andra åtgärder för att begränsa eventuella skador. Man kan exempelvis spärra sitt personnummer hos de olika kreditupplysningsföretagen. Det innebär att

[22] Holmquist Rolf, Brotten i näringsverksamhet, Norstedts, 2013, s. 136-137

[23] Polisen, Identitetsstöld – Utsatt, https://polisen.se/Utsatt-for-brott/Olika-typer-av-brott/Bedrageri/Identitetsstold--utsatt/ (Hämtad 2015-02-19)

kreditupplysningsföretagen inte lämnar ut några kredituppgifter på den spärrade personen när en begäran om kreditupplysning lämnas av ett kreditinstitut eller annan näringsidkare.[24]

Om man får hem en faktura avseende exempelvis ett köp som har utförts i ens namn, bör man genast bestrida fakturan. Att kontakta banken och kontrollera samtliga konton, spärra bankkort, kontrollera folkbokföringsadressen hos Skatteverket samt kontrollera att ingen eftersändning har gjorts av posten är adekvata åtgärder att vidta vid misstanke om att man har blivit utsatt för brott.[25]

4. Om nätbedrägerier

Nätbedrägerier kan ske på många olika sätt, exempelvis genom trojaner, maskar, kapade konton på sociala medier och diverse virus. Handlandet behöver dock inte alla gånger innebära ekonomisk skada för offret och ekonomisk vinning för bedragaren. I en del fall leder de dock till att förövarna kommer över personuppgifter, identitetshandlingar eller koder, som används när brotten genomförs.

Bedragarna lyckas ofta dölja alla spår som kan leda till dem. Genom att bedragarna använder sig av skyddade IP-adresser, servrar och anonyma nätverk är det utan kraftiga resurser svårt att komma åt dem. De är i många fall tekniskt kunniga och kan tillvägagångssätten för att kunna dölja samtliga elektroniska och virtuella spår som kan leda fram till dem.

4.1 Hur kan man säkra spår efter en bedragare på internet?

Genom att lagra uppgifter om användarnas IP-adresser, DNS-nummer samt information från loggar där man kan se vilken typ av webbläsare eller utrustning, t.ex. iPhone, iPad, Mac eller PC som använts. Myndigheterna kan med utövande av tvångsmedel och med hjälp av aktuell internetleverantör, ta reda på var personen som har besökt en webbplats, som är en hemsida på internet, eller vidtagit åtgärder på webbplatsen, befann sig vid just det tillfället. Med webbläsare avses den programvara som används för att besöka diverse webbplatser, hemsidor, på

[24] http://www.creditsafe.se/vanliga-fraagor/spaerra-ditt-personnummer/ (hämtad 2015-05-22)

[25] Polisen, Identitetsstöld – utsatt, https://polisen.se/Utsatt-for-brott/Olika-typer-av-brott/Bedrageri/Identitetsstold--utsatt/ (Hämtad 2015-02-11)

internet. Det är webbläsaren som gör att internetanvändaren kommer åt de olika webbplatser som har lagts upp på internet genom webbservrar.[26] Uppgifterna om vilken webbläsare eller utrustning som en gärningsman har använts sig av kan vara väldigt viktiga för en eventuell utredning, såvida gärningsmannen inte har använt sig av en skyddad IP-adress eller genom en trojan använt någon annans IP-adress.

Vissa internetleverantörer har dynamiska IP-adresser, vilket innebär att användarna tilldelas en ny IP-adress vid varje uppkopplingstillfälle. Det leder till att bevisning måste säkerställas skyndsamt. I praktiken innebär det att en IP-adress från en internetanvändare ena dagen, kan komma från en annan användare dagen därpå. Vissa internetleverantörer, så som exempelvis Bredbandsbolaget, har statiska IP-adresser, vilket innebär att IP-adressen alltid är den-samma.[27]

Med DNS-nummer menas en hierarkisk databas där all information lagras och är till för att förenkla adressering av datorer på internet. Det är själva databasen som kopplar ihop ett IP-nummer med ett domännamn, vilket är en fysisk hemsida. Man kan genom DNS-servern se vilken hemsida en dator har besökt vid vilken tidpunkt.[28]

4.2 Bevisning

Som nämnts ovan, är uppgifter om var en bedragare har befunnit sig, mellan vilka tider bedrägeriet har pågått, vilka verktyg bedragaren har använt sig av och eventuella spår av IP-adresser eller mobiltelefoner av stor betydelse för att utreda nätbedrägeribrott.

Tele- och internetoperatörer har sedan den 1 maj 2012 skyldighet att lagra uppgifter om trafikinformation i sex månader. Det innebär att uppgifter om telefonitjänst som avser den uppringandes och den uppringdes IP-adress måste lagras. Likaså datum och tid för på- och avloggning för de tjänster som har använts. Det rör sig om uppgifter som är nödvändiga för att spåra och identifiera en viss kommunikationskälla, vilket innefattar datum, tidpunkt, varaktighet, typ av kommunikationsutrustning, lokalisering av mobil kommunikationsutrustning vid

[26] http://www.google.se/intl/sv/goodtoknow/web/101/ (Hämtad 2015-05-20)

[27] Internetservice i Väst AB, Vad är en IP-adress? http://www.hittaip.se/info.php (Hämtad 2015-02-10)

[28] https://www.iis.se/lar-dig-mer/guider/dns-internets-vagvisare/sa-fungerar-dns/ (Hämtad 2015-05-18)

kommunikationens början och slut samt slutmålet för kommunikationskällan. Det framgår av 6 kap 16 § lag (2003:389) om elektronisk kommunikation.

Beträffande internetåtkomst och tillhandahållande av internetåtkomst ska användarens IP-adress, abonnent, registrerad användare, datum och tid för på- och avloggning samt kapacitet för överföring som har använts lagras. Operatörerna har även skyldighet att lagra uppgifter som identifierar den utrustning där kommunikationen har avskilts från den lagringsskyldige till den enskilde abonnenten. [29]

4.2.1 Svårigheten med bevissäkring

Eftersom det finns många komplicerade sätt att dölja vem som är verklig huvudman bakom utförda handlingar över internet, kan det många gånger vara svårt att säkerställa bevisning som kan leda fram till att hitta en gärningsman.

Företag eller privatpersoner som blir utsatta för bedrägeri har inte några tvångsmedel att använda sig av, men kan ha tillgång till värdefull information till nytta för en brottsutredning. Således är det viktigt att samarbetet mellan berörda myndigheter, de drabbade företagen och privatpersonerna fungerar. På så vis kan bevisning säkerställas för att myndigheterna på ett effektivt sätt ska kunna hitta den eller de gärningsmän som har genomfört eller försökt genomföra bedrägerierna.

En utredning ska bedrivas så snabbt som möjligt, enligt skyndsamhetsprincipen. Vid misstanke om nätbedrägeribrott, är det därför viktigt att inleda förundersökning snabbt och bedriva den så effektivt som möjligt, för att gärningsmännen inte ska kunna dölja spåren efter sig.

Polisen kan förutom att begära uppgifter hos internetleverantörerna med hänvisning till 6 kap 17a § lag (2003:389) om elektronisk kommunikation, använda sig av tvångsmedel så som beslag, husrannsakan, upptagningar och avlyssningar av elektronisk kommunikation enligt 27-28 kapitlet i rättegångsbalken (1942:740). Det krävs dock att någon är misstänkt för brottet för att det överhuvudtaget ska vara möjligt för polisen att använda tvångsmedlen i RB.

IP-adresser kan som nämnts vara statiska, dynamiska eller i vissa fall även skyddade. I många fall kan ett starkt bevismedel vara vem som har varit mottagare av de utförda betalningarna

[29] SFS 2012:128

eller överföringarna som bedrägeriet har gett upphov till. Eftersom vanliga medborgare har begränsade möjligheter att säkerställa sådan information från banker och betalningsmottagare, krävs en effektiv uppföljning av polisen för att med tvångsmedel kunna säkerställa information som kan läggas till grund för en eventuell förundersökning. I Svea hovrätts domar i mål B 906-07 samt B 1019-12 har de mottagande kontona varit avgörande för att kunna fälla bedragarna för de begångna brotten. Slutsatsen som kan dras är att de mottagande kontona utgör starka och konkreta bevis, medan IP-adresser och DNS-uppgifter kan värderas något lägre. Om en IP-adress är dynamisk, är uppgifterna i princip värdelösa, om inte omedelbar uppföljning och bevissäkring utförs. Givetvis har internetleverantörerna möjlighet att göra sökningar på IP-adresser, även fast de är dynamiska. Polisens begäran och tvångsmedel är dock avgörande för att det ska vara möjligt.

Polisen kan genom att ta datorer, mobiltelefoner eller andra verktyg som har använts till att begå nätbedrägeribrott i beslag enligt 27 kap. RB. Genom att få tillgång till de elektroniska hjälpmedel som har använts för att begå nätbedrägeribrott kan bevis som kan leda utredningen framåt säkerställas. Genom att genomsöka en dator, mobiltelefon eller annat elektroniskt hjälpmedel som använts vid ett nätbedrägeribrott kan information som har lagrats finnas tillgänglig. Det kan röra sig om uppgifter kring vilka internetsidor den misstänkte gärningsmannen har besökt, som kan ha koppling till brottet. Det kan även röra sig om koder, dokument rörande falska ID-handlingar eller program för att styra trojaner eller maskar.

Det krävs dock att det finns en misstänkt gärningsman för att beslag ska bli aktuellt. Då kan även hemliga tvångsmedel bli aktuella att använda.

4.2.2 Att följa pengarna

Det har i många bedrägeriärenden tagits upp att polisen ska följa pengarna, för att på så vis få mer ledtrådar om en eventuell gärningsman, med anledning av att det många gånger är mottagaren av pengarna som är gärningsmannen, eller åtminstone en medhjälpare som kan tillföra utredningen mer information. Ett problem med att följa pengarna är dock att bankväsendets hantering av pengar och överföringar till stor del har datoriserats. Det får till följd att en banktransaktion kan ske på en millisekund. I många fall använder en bedragare sig av olika banker i olika länder. Pengarna kan således skickas mellan många olika länder och konton på extremt kort tid. När svenska myndigheter utreder misstänkta bedrägerier där pengarna har överförts

till konton utomlands, kräver många banker att det har gjorts en anmälan om internationell rättshjälp, för att de ska lämna ut uppgifter om transaktioner. Det kan ta flera veckor och ibland upp till flera månader innan polisen får uppgifter om en enda transaktion. Om det har gjorts många transaktioner i ett ärende, kan det dröja väldigt lång tid innan polisen får upp spåren till den bank där pengarna slutligen hamnat. En bedragare väntar sällan på att bli påkommen, utan pengarna tas många gånger ut i kontanter ganska omgående efter att de har nått slutkontot. Resultatet av att följa pengarna blir oftast en utredning om hur pengarna har förflyttats och slutligen från vilket konto och eventuellt vilket bankkontor eller bankomat pengarna har tagits ut. [30]

4.3 Exempel på hjälpmedel och tillvägagångssätt

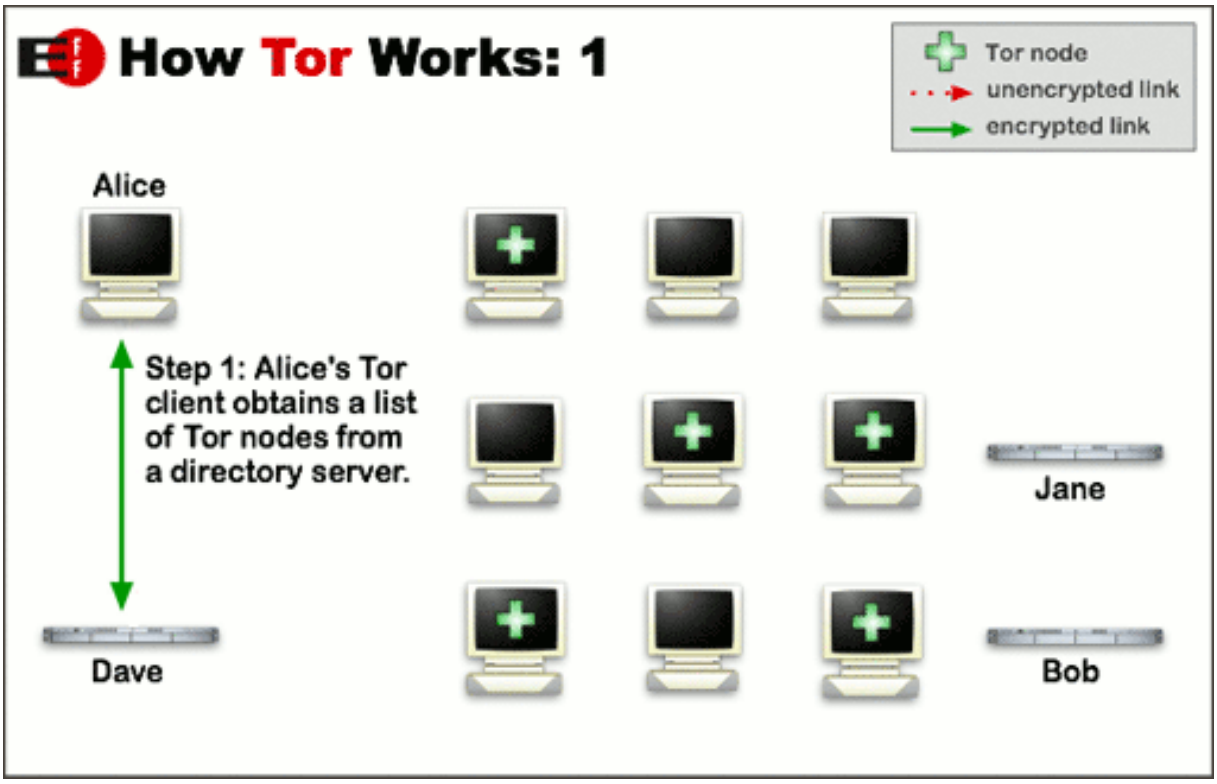
Genom sidan fejk.se kan man slumpa fram uppgifter avseende bland annat personnummer. Det går även att komma över en persons uppgifter genom sidor som upplysning.se och ratsit.se. En bedragare som har tillgång till en persons uppgifter, kan använda dessa för att köpa varor, tjänster eller ta krediter i den personens namn.

4.3.1 TOR-nätverket

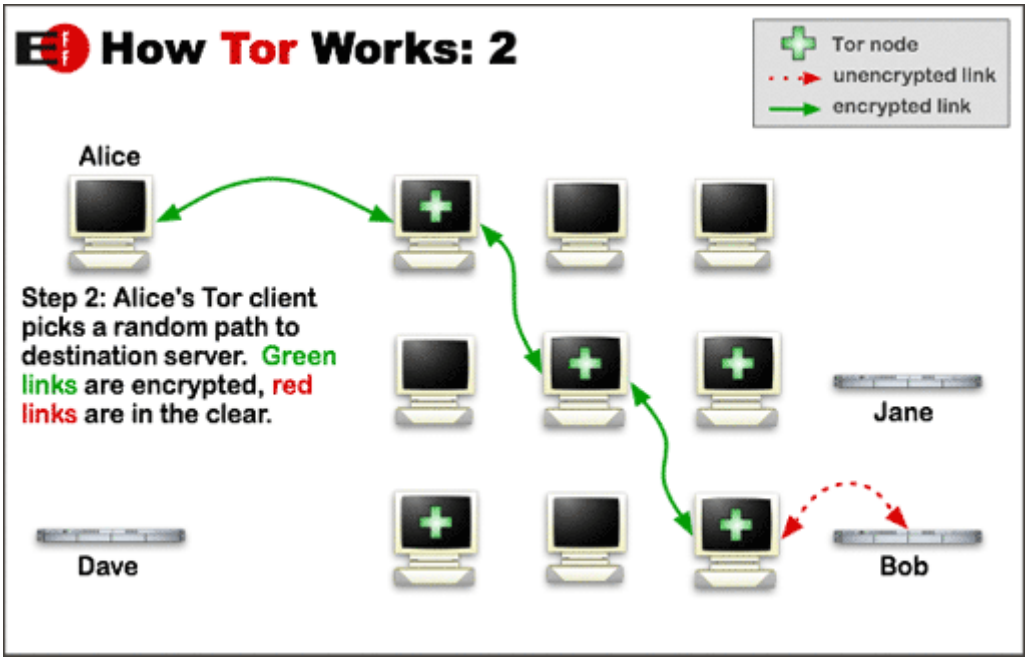
Exempel på ett anonymt nätverk där användarna är helt anonyma på internet är nätverket TOR. Nätverket utvecklades initialt för att nyttjas av den amerikanska marinkåren och skydda sekretessbelagd kommunikation. TOR-nätverket består av virtuella tunnlar som resulterar i att användarna kan vara helt anonyma på internet genom att de inte efterlämnar några spår efter sig när de besöker en internetsida eller vidtar åtgärder på internet. Det får givetvis till följd att en bedragare som har använt sig av TOR-nätverket blir svår att spåra.[31]

[30] Ahola, Mikael, Bedrägeri: introduktion och handledning för brottsutredare, 2013, s. 285

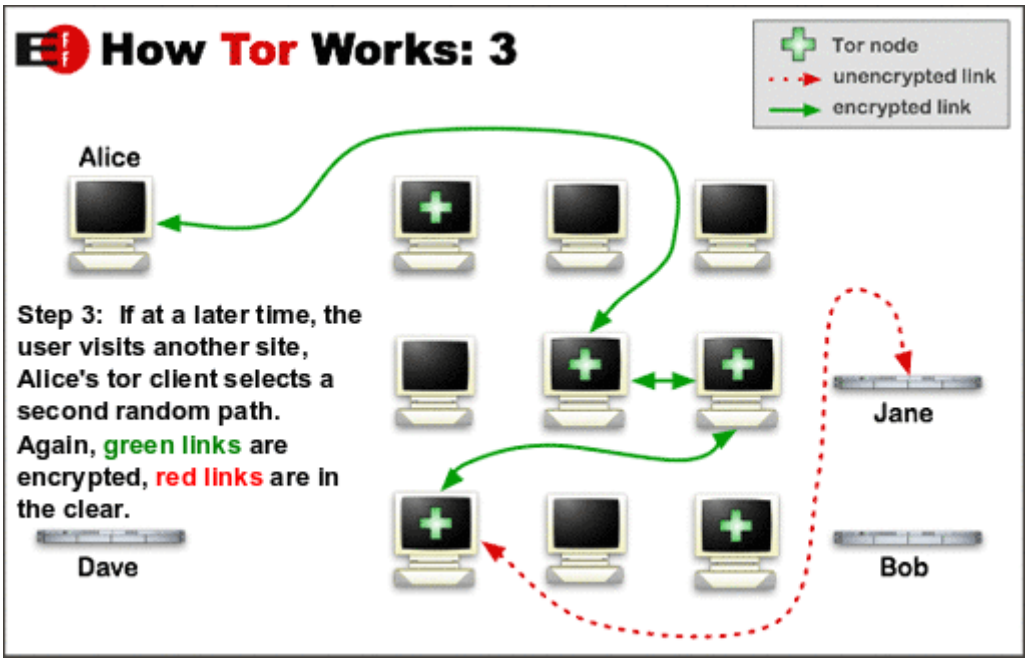
[31] TOR, About TOR, https://www.torproject.org (Hämtad 2015-02-09)



Bildkälla: https://www.torproject.org/about/overview.html.en



Bildkälla: https://www.torproject.org/about/overview.html.en



Bildkälla: https://www.torproject.org/about/overview.html.en

4.3.2 Trojaner

Trojaner är datorprogram eller skadliga koder som kan utge sig för att vara till för nytta eller nöje, men som i själva verket agerar på egen hand så snart datoranvändaren har installerat programmet på datorn. Programmet kan då utföra egna åtgärder på datorn, spionera på datoranvändare samt kopiera, ändra eller blockera information från datorn. En trojan kan också attackera andra datorer eller skicka meddelanden från den dator där intrånget har ägt rum. [32] En gärningsman kan genom att använda sig av en trojan göra sig skyldig till bedrägeri enligt 9 kap 1 § 2 st. BrB eller dataintrång enligt 4 kap 9 c § BrB.

Genom en så kallad banktrojan kan konto- eller kreditkortsinformation stjälas. De utformas specifikt för att stjäla sådan information som är knuten till ett bank- eller betalningssystem, för att tillskansa sig uppgifter som kan komma till nytta vid eventuella bedrägerier. Brotten sker uteslutande över internet och går att skydda sig mot genom antivirusprogram. [33]

[32] Goldberg, Larsson, Korthuset, Norstedts, 2014, s. 247-248

[33] Vad är en Trojan?, Kaspersky Lab, http://www.kaspersky.com/se/internet-security-center/threats/trojans (hämtad 2015-02-16)

När en trojan tar kontrollen över en dator kan den installera en så kallad ”keylogger”, som är ett datorprogram med vars hjälp alla tangenttryckningar på en dator registreras. Keyloggern registrerar alla knappar som pressas ned, vilket leder till att den kan registrera hemliga användarnamn, lösenord eller annan känslig information. [34]

Typexemplet på en trojan som används vid ett nätbedrägeri kan ske genom att brottsoffret laddar hem en fil till datorn, så som en film eller ett spel. Om filen är ”smittad” med en trojan börjar den genast registrera knapptryckningar. När internetanvändaren sedan loggar in på sin internetbank fungerar allt som vanligt, för att sedan gå något långsammare och därefter sakta upp något. Internetanvändaren kan då få uppfattningen att systemet kan ha fastnat. I samband med det kan en ruta komma upp, där användaren uppmanas att på nytt knappa in sina uppgifter. Uppgifterna som knappas in går direkt vidare till bedragaren som genast kan använda sig av uppgifterna för att logga in på användarens internetbank för att tömma den på tillgångar.

Trojaner kan även användas för att kapa datorer och kräva användaren på pengar. Exempelvis kan bedragaren låsa användarens dator, tangentbord och mus för att sedermera lägga upp en bild på skärmen där användaren uppmanas betala en lösensumma på ett visst konto för att få datorn upplåst.

Om man upptäcker att man har haft en trojan på datorn är det viktigt att man byter samtliga lösenord till alla konton, så som e-postkonton, sociala medier, spelsidor, FTP-konton mm.[35]

4.3.3 Maskar

Maskar består av ett enskilt program som installerar sig själv på datorn och infekterar den, till syfte att skicka en kopia av sig själv vidare till nästa dator. Maskarna fortplantar sig genom att skicka sig vidare till andra datorer genom ett nätverk eller över internet. En mask kan ta full kontroll över en dator och komma över information som finns på datorn. De är beroende av

[34] Övervakning och loggegenskaper, Relytec, http://www.relytec.com/keylogger_se/keylogger.htm (hämtad 2015-02-16)

[35] Ahola, Mikael, Bedrägeri: introduktion och handledning för brottsutredare, 2013, s. 81-82

säkerhetshål i en dator eller ett nätverk för att kunna spridas. Genom att installera en brandvägg eller antivirusprogram kan man skydda sig mot maskar. [36]

4.3.4 VPN-tunnlar

VPN står för virtuellt privat nätverk. Något förenklat kan man säga att en dator som ansluter sig till internet med hjälp av en VPN-tunnel gör det med en annan dator som mellanhand. Trafiken kan på så vis krypteras och kan vara omöjlig att förstå för en okunnig. På så vis kan en bedragare begå brott på internet, sopa igen spåren efter sig och om någon kunnig analytiker lyckas förstå krypteringen, så kommer man endast till den dator som har agerat mellanhand, vilket kan vara en oskyldig datoranvändare som har fått sin dator kapad genom en trojan eller mask.[37]

4.3.5 Anonyma nätforum

Shadowcrew är exempel på ett anonymt nätforum där det köpslogs om personuppgifter på människor från hela världen. Uppgifterna var till nytta för bedragare som hade uppsåt att begå nätbedrägeribrott. Utseendemässigt såg Shadowcrew ut som ett vanligt köp- och säljforum på internet. Skillnaden var att det som såldes var stulna eller falska ID-kort, stulna bank- eller kreditkortnummer och andra uppgifter som kan leda till straffansvar. För en bedragare som släpptes in i nätforumet Shadowcrew öppnades en värld av det mesta som behövdes för att stjäla stora och snabba pengar, så länge man var villig att betala för uppgifterna. Shadowcrew växte så småningom till att bli en av nätets största forum för kriminella där det dagligen diskuterades kring bedrägerier och köpslogs om uppgifter som behövdes för att kunna begå nätbedrägeribrott.[38]

[36] What is a computer virus or a computer worm?, Kaspersky Lab, http://www.kaspersky.com/internet-security-center/threats/viruses-worms (hämtad 2015-02-16)

[37] Goldberg, Daniel, Larsson, Linus, Korthuset, Norstedts, 2014, s. 91-92

[38] Goldberg, Daniel, Larsson, Linus, Korthuset, Norstedts, 2014, s. 86-90

4.3.6 Exempel på nätbedrägeribrott med hjälp av en trojan

År 2007 uppdagades att stora summor pengar hade stulits ur Nordeas internetbank med hjälp av en trojan. Nordeas säkerhetssystem för internetbanken hade på den tiden sett likadant ut i flera år. Kunderna använde ett plastkort för att skrapa fram en kod för att logga in på internetbanken och skrapade fram ytterligare en kod för att godkänna en transaktion. Skrapkoderna var lyckade eftersom många användare tyckte att bankdosorna var krångliga. Det var ett vanligt sätt för Nordeas kunder att använda sig av internetbanken, men blev i slutändan en genväg som straffade sig.

Systemet ställde två fyrsiffriga koder mellan en angripare och kundens besparingar. Den trojan som framtagits var utformad för att kunna utnyttja den svagheten. En kund som fått sin dator infekterad av en trojan fick de koder som knappades in på datorn skickade till bedragaren, som i lugn och ro kunde logga in på de drabbade kontona och föra över pengarna till sina egna konton. Samtidigt som kunden trodde att dennes utförda transaktioner genomförts och att eventuella besparingar fanns kvar på kontot, i tryggt förvar hos banken. Inom loppet av ett par månader stals över 8 miljoner kronor från cirka 250 Nordeakunder. Sammanlagt greps 160 personer av polisen. De var misstänkta för att ha agerat som målvakter, det vill säga mellanhänder, genom att ha lånat ut sina konton för att de olovliga transaktionerna skulle kunna genomföras. Man ansåg att det höga antalet gripna personer tydde på att polisen enbart hade rört sig i bedrägeriligans lägre skikt. Således lyckades man inte gripa någon av huvudmännen. Det spekulerades dock kring att en datorkunnig person måste ha agerat som huvudman, då bedrägerierna genomfördes på ett tekniskt kvalificerat vis.

Genom att implementera ett nytt system, cirka tre månader efter att bedrägerierna uppmärksammats i media, lyckades Nordea komma tillrätta med bedrägerierna. Genom att kunderna fick knappa in sin kod på en säkerhetsdosa, kunde trojanen som var utformad för att samla in de fyrsiffriga skrapkoderna inte längre användas. Det skulle dröja till år 2012 innan Sverige skulle bli drabbat av en stor våg trojaner som siktar in sig på internetbanker. 2007 års upplaga som riktade in sig på Nordeakunder hade uppgiften att stjäla två koder och skicka iväg dessa för senare användning.

2012 års upplaga av banktrojaner var dock betydligt mer avancerad. Den agerade i samma stund som kunden trodde att denne var inloggad på sin internetbank. Den la sig som ett falskt lager mellan kundens dator och den riktiga internetbanken och fick på så vis allt att se normalt

ut. Inloggningsrutor och logotyper låg precis där de brukade på skärmen, allt för att det skulle se så normalt ut som möjligt, trots att det bara var en kuliss. I bakgrunden dirigerades koderna från säkerhetsdosorna vidare till den riktiga internetbanken, som bedragaren kontrollerade. När brottsoffret trodde sig utföra betalning av en räkning utfördes i själva verket en transaktion till ett konto som bedragaren eller en målvakt som bedragaren anlitat kontrollerade. Det var inte heller bara det mottagande kontot som byttes ut, utan även beloppet. Det kunde ändras från 300 kronor till 50 000 kronor. Trojanen startade överföringar till ett värde av 140 miljoner kronor på omkring ett år, med start under år 2012. Bedrägerierna drabbade alla storbanker, som dock lyckades stoppa en del av dem.[39]

5. Polis och åklagare

Under en pågående förundersökning kan åklagare besluta om tvångsmedel, till syfte att driva utredningen framåt. Åklagaren ska vid beslutande om tvångsmedel vara objektiv och även beakta de omständigheter som är till den misstänktes fördel. Det föreligger en detaljerad reglering av vilka tvångsmedel som får användas och under vilka förutsättningar de får användas.[40]

5.1 Vilka tvångsmedel står till buds?

Åklagaren kan besluta om husrannsakan, anhållande, häktning och reseförbud för den misstänkte. Vid husrannsakan kan föremål av betydelse för utredningen hittas som kan tas i beslag och som kan tänkas vara till förmån för utredningen. För att ett föremål ska kunna tas i beslag krävs inte att beslaget görs hos den misstänkte eller att brottet på något sätt är kvalificerat. Förutsättningar för beslag stadgas i 27 kap 1 § RB. De situationer då beslag kan aktualiseras är när beslaget kan ha betydelse för utredning av brott, vara avhänt någon genom brott, vara

[39] Goldberg, Daniel, Larsson, Linus, Korthuset, Norstedts, 2014, s. 249-253

[40] Åklagarmyndigheten, Tvångsmedel, http://www.aklagare.se/Aklagarens-roll/Forundersokningen/Tvangsmedel/ (Hämtad 2015-02-26)

förverkat på grund av brott eller ha betydelse för utredning om förverkande av någon form av brottslig verksamhet enligt 36 kap 1 § BrB. [41]

5.1.2 Beslag

Beslag innebär att en form av besittningsrubbning sker, för att ge utredande myndigheter möjlighet att utröna om ett brott har ägt rum. En vanlig grund för beslag är att föremålet skäligen ska antas ha betydelse för utredning om brott. Exempelvis kan datorer och mobiltelefoner tas i beslag för att innehållet ska kunna undersökas. Likaså flygkvitton, hotell- och restaurangnotor som kan styrka var en person har befunnit sig eller bekräfta att en viss kontakt har varit aktuell mellan olika personer som har varit involverade i ett brott. [42]

Beslag kan delas in i tre olika kategorier:

- Utredningsbeslag, där syftet är att utreda brott eller förverkande av utbyte från brottslig verksamhet.
- Förverkandebeslag, där syftet är att kunna säkra eventuellt framtida förverkande.
- Återställendebeslag, där syftet är att säkra framtida återställande av föremål som kan ha avhänts någon genom brott.

Det finns inga begränsningar i fråga om hos vem beslag får göras, utöver de generella begränsningarna. Så tillvida kan beslag drabba såväl misstänkta personer för ett eventuellt brott, som icke misstänkta personer. Men även företag och personer som saknar direkt koppling till brottet och utredningen kring brottet kan drabbas. [43]

5.1.3 Hemliga tvångsmedel

Med hemliga tvångsmedel avses hemlig avlyssning av elektronisk kommunikation som överförs i ett elektroniskt kommunikationsnät. Hemlig avlyssning av elektronisk kommunikation

[41] Beslagshandbok, Utvecklingscentrum i Malmö, Åklagarmyndigheten, november 2013, s. 4-9

[42] Lindberg, Rättegångsbalk (1942:740) 27 kap. 1 §, Lexino 2014-07-01

[43] Lindberg Gunnel, Rättegångsbalk (1942:740) 27 kap. 1 §, Lexino 2014-07-01

får endast användas vid förundersökning av brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år, enligt 27 kap. 18 § RB.

Även hemlig övervakning av elektronisk kommunikation kan vara aktuell vid förundersökning av brott för vilket det inte är föreskrivet lindrigare straff än fängelse i sex månader, enligt 27 kap. 19 § RB. Med hemlig övervakning av elektronisk kommunikationen avses:

”1. meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller annan adress,

2. vilka elektroniska kommunikationsutrustningar som har funnits inom ett visst geografiskt område, eller

3. i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits.”

Det krävs att någon är skäligen misstänkt för brottet och att åtgärden är av synnerlig vikt för utredningen för att hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation ska få ske. Tvångsmedlen kan även användas i syfte att utreda vem som skäligen kan misstänkas för brottet, om åtgärden är av synnerlig vikt för utredningen, enligt 27 kap 20 § RB.

5.2 Åklagarens roll

Många gånger är det åklagaren som leder förundersökningen, men som av hög arbetsbelastning inte alltid har utrymme att på ett aktivt sätt leda arbetet. Åklagaren har tre huvuduppgifter; att utreda brott, att fatta beslut om åtal ska väckas eller inte samt att föra det allmännas och målsägandens talan i domstolen. Anvisningar om det är åklagare eller polis som ska leda förundersökningen anges i Rikspolisstyrelsens föreskrifter och allmänna råd 403-5, (RPSFS 2005:11) respektive Åklagarmyndighetens föreskrifter och allmänna råd ÅFS (2005:09). I de fall då brottet inte anses vara av enkel beskaffenhet, är det åklagaren som leder förundersökningen. När åklagaren har fått ansvar för utredningen är det denne som bestämmer i alla frågor som rör utredningen. Det är förundersökningsledaren som har ansvar för helheten av förundersökningen, vilket framgår av 1 a § förundersökningskungörelsen (1947:948). Men då

åklagaren är den som beslutar om vilka åtgärder som ska vidtas, är det denne som beslutar vilka av polismyndighets resurser som ska användas samt hur de ska användas.

När åklagaren har tillräckligt mycket bevis för att kunna väcka åtal i domstol är utredningen klar. Åklagaren ska då väcka åtal och föredra målet samt lägga fram bevisen i ett sammanhang i enlighet med 23 kap 2 § RB. [44]

6. Praxis

I rättsfallet HovR B 5233-12 som meddelades av Svea hovrätt, begagnade sig bedragaren av målsägandens kontokortuppgifter för att beställa varor över internet. Hon dömdes för bedrägeri, för att olovligen ha påverkat resultatet av en automatisk informationsbehandling eller liknande process, till villkorlig dom och bötesstraff.

Av Göta hovrätts dom HovR B 2274-12 kan man utläsa att gärningsmannen har utgett sig för att vara företrädare för en juridisk person och med uppsåt att sälja produkterna vidare tillskansat sig ekonomisk vinning, till skada för säljaren NetOnNet AB. Påföljden bestämdes till villkorlig dom, då gärningsmannen endast dömdes för en av åtalspunkterna.

I rättsfallet HovR B 2679-09 nådde hovrätten över Skåne och Blekinge slutsatsen att de tilltalade genom ”skimmad” kontokortinformation utfört köp av varor och tjänster till betydande värden. De dömdes för grovt bedrägeri, försök till grovt bedrägeri, grovt bedrägeri medelst brukande av falsk urkund och förberedelse till fängelse i 1 år och 6 månader respektive grovt bedrägeri till fängelse i 1 år och 3 månader.

Av rättsfallet B 8025-13 som meddelades av Svea hovrätt framgår att gärningsmännen, medelst brukande av falsk urkund gjorde sig skyldiga till flera grova bedrägerier över internet. Genom att ansöka om lån för miljonbelopp och beställa varor över internet, har gärningsmännen lämnat spår efter sig i form av undertecknade skuldebrev, uttag från bankomater och bankkontor samt IP-adresser. Polisen har med hjälp av IP-adresserna kunnat säkerställa varifrån bedrägerierna har genomförts, till styrkande av att det har varit de tilltalade som har ut-

[44] Ahola, Mikael, Bedrägeri: introduktion och handledning för brottsutredare, 2013, s. 50-51

fört dem. De tilltalade dömdes till fängelse i 8 månader, 1 år och 6 månader respektive 1 år och 9 månader.

I rättsfallet B 6351-13 fastställde Svea hovrätt tingsrättens domslut. Under en av åtalspunkterna hade den tilltalade ansökt om kredit över internet i annans namn. Han gjorde sig därmed skyldig till grovt bedrägeri medelst urkundsförfalskning. En förmildrande omständighet utgjordes dock av att den tilltalade betalade tillbaka skulden när brottet hade upptäckts. Påföljden blev fängelse i 1 år för samtliga sex åtalspunkter, där endast en av de utgjordes av nätbedrägeribrott.

7. Intervjuer

7.1 William Varga, brottsoffer

Under sommaren 2012 märkte William att hans post slutade dyka upp i brevlådan. Han väntade på att ett betalkort som han beställt inför en kommande semesterresa skulle anlända, men som aldrig gjorde det. Han tog sedermera kontakt med företaget igen och beställde ett betalkort på nytt, som aldrig heller dök upp. William började då ana oråd och ringde till Upplysningscentralen för att ta reda på om någon eller några har tagit en kreditupplysning på honom. Det visade sig sedermera att ett 15-tal kreditupplysningar från diverse kreditföretag hade tagits på honom och han ringde till polisen för att upprätta en anmälan då han misstänkte att hans identitet hade stulits.[45]

William som bad polisen ta detta på största allvar begärde att polisen skulle spana vid hans brevlåda för att se vem som tog hans post, men fick information om att polisen inte hade resurser till det och avrådde bestämt honom från att själv spana efter en eventuell gärningsman. William kontaktade sedermera posten för att eftersöka mer information. Han kunde efter diskussioner med posten konstatera att hans farhågor visat sig vara befogade. Av posten fick han information om att de delat ut viss specifik post och han kunde konstatera att den specifika posten inte kommit honom till handa.

[45] 0201-K232619-12

För att inte bli utsatt för fler bedrägeriförsök vidtog William drastiska åtgärder och spärrade sitt personnummer hos samtliga kreditupplysningsföretag, beställde hämtning av all sin post på postkontor och ringde till alla företag där kreditupplysning tagits och eventuell kredit beviljats och förklarade händelseförloppet. Det tog närmare 100 timmar av hans tid att kontakta alla och skicka in kopior på polisanmälan, förklara händelseförlopp och bestrida samtliga fakturor för de krediter som tagits i hans namn.

I efterhand misstänker William att någon har stulit hans post, där även hans lönespecifikation har legat och hans personnummer har framgått. Genom att få tillgång till hans personnummer har bedragaren lyckats öppna ett konto i Skandiabanken och dessutom lyckats beställa ett Bank-ID. Därefter har bedragaren tagit krediter till ett värde av ca. 700.000 kr. Utredning har visat att pengarna från krediterna som har beställts har förts över till kontot i Skandiabanken, där bedragaren har kunnat disponera över pengarna.

Bedragaren har även försökt att köpa mobiltelefoner och teckna mobilabonnemang, vilket han dock inte lyckades med då försäljarna anade att något inte stod rätt till och blockerade transaktionerna.

Förundersökningen lades sedermera ned, eftersom bedragaren var misstänkt och dömd för andra grövre brott. Åklagaren valde därför att inte väcka åtal med anledning av åtalsunderlåtelse enligt RB 20:7 1 st. 3p samt 23:4a 1 st. 2 p. Det innebär att åklagaren väljer att inte väcka åtal om den tilltalade är misstänkt för flera andra liknande eller grövre brott och bedömer att åtal för brottet inte skulle få någon eller endast en liten betydelse för straffet. Syftet är att rättsväsendets resurser ska användas så effektivt som möjligt för att utreda och lagföra andra grövre brott.[46]

Polisen lyckades med andra ord identifiera gärningsmannen i fråga men då denna gjort sig skyldig till annan så allvarlig brottslighet att polisen bedömde att de brott som William utsatts för inte skulle påverkat påföljdsdelen vid åtal. Med andra ord hade polisen vetskap om vem som utsatte William för brott. Nedläggningsbeslutet betyder inte att William inte har utsatts för brott, utan är en rättspolitisk åtgärd för att spara på domstolarnas och polisens resurser.

Konsekvenserna för William har varit många. Han har tvingat spärra sin identitet vilket försvårar enkla vardagsbestyr som exempelvis att hyra en bil eller att teckna ett abonnemang.

[46] Åklagarmyndigheten, Åtalsunderlåtelse och förundersökningsbegränsning, http://www.aklagare.se/Aklagarens-roll/Atalsbeslutet/Atalsunderlatelse/ (hämtad 2015-04-09)

Hans kreditbetyg, vilket av bankerna internt benämns ”scoring”, bedöms som låg och han har idag sämre möjlighet att bli beviljad kredit av banker och kreditgivare.[47] Han har fått spendera många timmar med att korrespondera med polis, kreditgivare och banker för att reda ut det inträffade och mildra följderna. Förutom de praktiska ingreppen i hans vardagsliv har det varit belastande att leva med oron om vad som ska ske och den otrygghet det innebär att bli utsatt för brott.

Dessutom krävde en av kreditgivarna, Forex Bank, som beviljade en kredit om 200 000 kr, William på ersättning. Det ledde till att företaget stämde honom och tvisten upptogs i tingsrätten, där Forex sedermera återkallade sin talan med anledning av att det inte kunde anses styrkt att William tagit den kredit som bolaget gjorde gällande.[48]

7.2 Evert Norberg, förundersökningsledare inom bedrägerisamordningen

Evert Norberg menar att det huvudsakliga problemet som har lett till en lavinartad ökning av bedrägerier är på grund av att ID-handlingar är lätta att kopiera och förfalska. Utbudet av samtliga olika varianter av ID-handlingar förenklar för bedragarna att förfalska en ID-handling. Det kan nämligen vara svårt för medborgarna att hålla koll på alla olika ID-handlingar som finns. Till och med nationellt forensiskt centrum (NFC) kan ibland ha svårt att urskilja en äkta handling från en falsk handling, då förfalskningar kan vara extremt välgjorda. Eftersom det florerar många falska legitimationer och det med anledning av den tekniska utvecklingen har blivit lättare att ta fram förfalskningar kan förövarna till och med lyckas förfalska ID-handlingarna med brottsoffrets personuppgifter men bedragarens bild på den falska ID-handlingen.

En anledning till att så få anmälda brott faktiskt leder till en fällande dom är enligt Evert Norberg att en målsägande i många fall reagerar för sent eller att det tar så pass lång tid från det att brottet förövats till att målsäganden blir varse om det. I vissa fall kan det också vara så att brottsoffret tar kontakt direkt med företagen där bedrägerierna har utförts istället för att upprätta en anmälan till polisen. Det leder till att polisen riskerar att gå miste om värdefull in-

[47] https://www.bankofscotland.co.uk/HelpCentre/pdf/credit-scoring-guide.pdf (hämtad 2015-05-20)

[48] Stockholms tingsrätt, målnummer T 14989-14

formation till brottsutredningen som kan vara avgörande för att kunna identifiera en misstänkt gärningsman.

Så fort en polisanmälan om ett misstänkt bedrägeri kommer in till polisen agerar man skyndsamt och inleder förundersökning. Polisen tar då kontakt med de företag där de misstänkta bedrägerierna har ägt rum för att ta reda på uppgifter om vilken eventuell kredit, vara eller tjänst som beviljats eller lämnats ut och vilka uppgifter som finns registrerade eller lagrade. I många fall är det svårt att hitta en misstänkt gärningsman, för att på så sätt kunna gå vidare i utredningen. Det krävs att bevisning säkras för att kunna fastställa en misstänkt gärningsman.

I slutändan är det åklagaren som håller i utredningen och om åklagaren bedömer att man inte kan hitta en misstänkt gärningsman eller att bevisningen inte håller för en fällande dom, läggs förundersökningen ned. Det är däremot av stor vikt att ha en god dialog mellan åklagare och förundersökningsledare för att kunna bedriva förundersökningen så effektivt som möjligt och för att åtal i slutändan ska kunna väckas. Alla ärenden går inte att utreda och vissa ärenden kan dessutom vara av civilrättslig karaktär. Polisen har interna regler att följa och har inte möjlighet och resurser till att utreda alla anmälda brott.

7.2.1 NBC

I början av 2013 startade Polismyndigheten i Stockholms län ett nationellt bedrägericenter (NBC) till syfte att samordna resurserna och upptäcka de bedrägerier som hänger ihop och sker i stor skala. NBC har ett nationellt uppdrag och har ansvar för att hantera bedrägeribrotten. NBC är uppdelad på tre ben med ett polisoperativt ben med tre förundersökningsledare, den brottspreventiva delen och metodutvecklingen. Inom metodutvecklingen har man hjälp av bland annat analytiker och databashanterare. De har till uppdrag att samordna arbetat och se till att landets poliser drar åt samma håll för att arbetet ska bedrivas mer effektivt och samordnas bättre. Ambitionen är att öka medvetenheten om de problem som finns och hur man kan komma till bukt med dem.

NBC har upprättat ett nätverk från respektive polisområde för att hämta ut och lämna information till samtliga polisstationer i landet. Man ger ut direktiv och tips på hur man ska jobba mer effektivt, när det kommer nya brottsvågor så rapporteras det snabbt ut till samtliga polismästardistrikt.

7.2.2 Från gärning till åtal

Efter att ett bedrägeribrott har förövats, polisanmälts och registrerats i polisens anmälningssystem (RAR) hamnar det hos bedrägeriroteln i Stockholm. Därefter görs en bedömning i ärendet för att ta reda på om det finns substans för att komma vidare i ärendet och vilka eventuella frågetecken som kan föreligga. Polisen skickar sedan ut förfrågningar för att få tillgång till information och bevisning från den eller de som kan tänkas inneha sådan information. Initialt krävs skyndsamhet för att bevissäkra. Exempelvis kan det handla om förfrågningar till internetleverantörer, telefonoperatörer eller bevakningsfilmer från postutlämningskontor. Tele- och internetleverantörer har skyldighet att lagra uppgifter för brottsbekämpande ändamål. Det rör sig om uppgifter som är nödvändiga för att spåra och identifiera en viss kommunikationskälla. Det innefattar även datum, tidpunkt, varaktighet, typ av kommunikationsutrustning, lokalisering av mobil kommunikationsutrustning vid kommunikationens början och slut samt slutmålet för kommunikationskällan. Det framgår av 6 kap 16 a § lag (2003:389) om elektronisk kommunikation.

Internetleverantörerna har skyldighet att lagra uppgifterna i sex månader från den dag då kommunikationen avslutades, enligt 6 kap 16 d § lag (2003:389) om elektronisk kommunikation. Enligt Evert Norberg är det dock inte alla som följer lagstiftningen. Vissa internetföretag lagrar inte uppgifter så länge som de borde och är inte alltid behjälpliga med att lämna ut begärd information, trots att det kan röra sig om omfattande brottsutredningar. Av 6 kap 16 f § framgår att den som är skyldig att lagra uppgifterna ska lämna ut uppgifterna utan dröjsmål och utan att verkställande av utlämnandet röjs.

Att polisen får ut uppgifterna behöver dock inte alltid leda till att de lyckas fastställa vem som har begått brotten. För straffansvar krävs att åklagaren lyckas bevisa att en viss person har begått de aktuella brotten. Uppgifterna från en tele- eller internetleverantör kan ge polisen uppgifter om vem som tecknat sig för abonnemanget, det behöver dock inte innebära att det är just den personen som har utfört handlingarna. I ett autentiskt fall hade en bedragare varit på besök hos sin mor och vid det tillfället kopplat upp sig mot hennes internet, för att därefter via sin bärbara dator begå nätbedrägeribrott. I det fallet kunde utredningen peka på att bedragaren varit på besök hos modern vid det aktuella tillfället och utfört vissa handlingar som modern varken hade intresse av eller kompetens att utföra.

Det kan även vara så att vissa postutlämningsställen inte lagrar sina övervakningsfilmer mer än ett visst antal timmar. Således behöver polisen agera skyndsamt. Det har dock hänt att rätt person på plats som har haft kunskapen om tekniken inte har varit på plats och då har det lett till att bevisningen har gått om intet. Många gånger är polisen begränsad baserat på hur länge teknisk bevisning finns. Exempelvis så lagras övervakningsfilmer från Stockholms tunnelbana i tre dygn.

När polisen har fått tillgång till bevismaterialet analyseras allt bevismaterial för att därefter ta ställning till om man kan komma vidare i utredningen med det material man har eller om det krävs ytterligare bevisning. Parallellt med arbetet kring bevisningen eftersöks eller efterlyses eventuella misstänkta gärningsmän. Polisens samordningsenhet lämnar därefter över ärendet till utredningsgruppen som får förhöra eventuella misstänkta gärningsmän och vittnen.

För att ta reda på om åtal kan väckas kontrollerar man sedermera i misstankeregistret och brottsregistret. Efter vad som framkommit i eventuella förhör kan polisen ta ställning till hur man ska gå vidare eller om ärendet ska läggas ned. Om polisen bedömer att man inte kan styrka att den misstänkte gärningsmannen har begått brottet läggs förundersökningen ned.

”Polisen ska inte utöva domarens jobb att bedöma, men måste objektivt kunna styrka brott".

- Evert Norberg, förundersökningsledare på bedrägeriroteln i Stockholm.

7.3 Marie Wallin, åklagare

Marie Wallin är åklagare men arbetar för tillfället inom polismyndigheten som specialist inom bedrägerier. Hon berättar att man i Stockholm har slagit ihop de tre olika bedrägerirotlarna och på det viset har lyckats få en bättre samordning och ett bättre samarbete mellan åklagare och polis. Det har lett till att arbetet med utredningarna bedrivs mycket mer konstruktivt och effektivt.

En viktig parameter att ha med i brottsutredningar är att allt som medborgarna uppfattar som brottsligt inte alltid är det enligt lagens mening. Statistiken som Brå levererar över anmälda brott kan i vissa fall vara missvisande, då vissa anmälda ”brott” kan vara av civilrättslig karaktär. När förundersökningen sedermera läggs ned, hamnar det anmälda ”brottet” i statistiken bland anmälda brott och förundersökningar som har lagts ned, trots att det i själva verket inte

har varit ett brott av straffrättslig karaktär. Polisen har dock skyldighet att utreda eventuella brott och åklagaren har skyldighet att väcka åtal och ställa gärningsmännen till svars om de objektiva kraven för att det ska anses vara brott enligt lagens mening är uppfyllda.

En bevissvårighet med bedrägeribrott som förövas över internet är att gärningsbeskrivningen emellanåt kan vara svår att förtydliga, då mycket kan peka åt ett håll, men brottet i själva verket kan visa sig ha gått till på ett helt annat sätt. Exempelvis behöver ett IP-nummer inte alltid vara kopplat till en person. En IP-adress kan, som konstaterat ovan, vara antingen statisk eller dynamisk.

När bedragaren har gjort sig skyldig till internetbedrägeri med en stulen identitet och tagit en kredit via ett kreditinstitut, då kan man i vissa fall följa pengarna. Vid nätbedrägeribrott där krediter har tagits, så kan man följa var pengarna har satts in. På så vis kan man följa kontot och pengarna. Om det visar sig att det inte är förövaren som använder kontot då, kan i varje fall kontohavaren åtalas för penningtvättsbrott enligt lag (2014:307) om straff för penningtvättsbrott.

7.3.1 Användandet av tvångsmedel under utredningen

De tvångsmedel som står åklagaren till buds att använda är beroende av straffvärdet för det aktuella brottet som den misstänkta är misstänkt för att ha begått. Ju högre straffvärde ett brott har, desto fler tvångsmedel kan åklagaren nyttja vid bedrivande av förundersökningen. Åklagaren kan inte agera på känsla, utan måste tillämpa objektivitetsprincipen. De tvångsmedel som åklagaren väljer att använda måste grundas på straffvärdet för brottet och misstankegraden. Om straffvärdet för bedrägeri av normalgraden utökas, då kan åklagaren vidta fler åtgärder, men detta går inte i dagsläget med tanke på proportionalitetsprincipen. Proportionalitetsprincipen är en princip baserad på rättssäkerhet, till syfte att det ska råda en balans mellan de medel som används och de mål som ska uppnås. Åtgärderna ska inte gå utöver vad som är nödvändigt med hänsyn till ändamålet.

Marie Wallin anser att de har tillräckliga tvångsmedel för att kunna bedriva en utredning effektivt, så länge man är medveten om hur man ska hantera dem. Svårigheterna uppstår när det misstänkta brottet har ett lågt straffvärde och det med hänsyn till proportionalitetsprincipen kan vara oskäligt att använda sig av vissa tvångsmedel. Som åklagare får man bygga sitt åtal

på farligheten, systematiken i brotten, artbrott etc. Bedrägeribrott leder exempelvis sällan till fängelse som påföljd, utan stannar oftast vid böter och villkorlig dom.
På frågan om eventuell straffskärpning skulle kunna vara aktuellt för bedrägeribrott, sett ur politisk synvinkel, menade Marie Wallin att det vore mer beaktansvärt att diskutera skärpta straff för brott mot person, inte brott som avser pengar.

”Straffvärdet för brott av normalgraden behöver kanske inte vara högre, men vid grova bedrägerier skulle det kunna vara aktuellt och då utsattheten är på ett annat sätt i sådana fall. Skärpta straff, vad ska det leda till? Fängelse leder sällan till rehabilitering. Många gånger är det återfallsbrottslingar. Frihetsberövande straff ska mer skydda samhället från brottslingarna och deras gärningar, än syfta till att rehabilitera brottslingarna.”

- Marie Wallin, åklagare, f.n. bedrägerispecialist inom polismyndigheten.

7.3.2 Utredningen

I vissa fall kan utredningen köra fast och inte komma längre. Exempelvis kan det röra sig om svårigheten med att säkerställa bevisning eller att det föreligger en förundersökningsbegränsning. Förövaren kan vara dömd för ett annat grövre brott och då begränsas förundersökningen med anledning av åtalsunderlåtelse. Straffvärdet rabatteras och på så vis kan vissa brott inte leda till åtal/fällande dom. Åklagaren kan inte gå till domstolen med 1000 åtalspunkter. Allmänheten har inte riktigt förståelse för hur straffsystemet är uppbyggt och att vi i Sverige har straffrabatt. Förfarandet med straffrabatt kan leda till att en utredning kan läggas ned, om åklagaren bedömer att något straff inte kommer att utdömas för de misstänkta gärningarna. Straffmätningen kontra brottet är det som är avgörande för att kunna driva utredningen vidare och ta upp det allmännas resurser. Åklagaren försöker då att sålla bort vissa brott eftersom denne inte kan väcka åtal för alla misstänkta gärningar. Med anledning av att domstolen inte kommer att döma på allt och då kommer inte den åtalade i sin tur att dömas för allt. Man tar istället upp domstolens tid i onödan, vilket kan skapa irritation och tar upp resurser i onödan.
En rutinerad åklagare får ganska snabbt en bild framför sig kring vilken bevisning som behövs för att styrka brottet och på så vis övertyga domstolen och få till en fällande dom. Enligt Marie Wallin krävs det dock att den polis som företar förundersökningen har god kunskap i hur man ska bedriva en förundersökning. Polisen behöver veta hur åklagare och domstol re-

sonerar och hur bevisvärderingen sker. Om polisen har god insikt i hur processen i domstol går till och vilka beviskrav som ställs så kan förundersökningen bedrivas mer effektivt och allt material som åklagaren kan tänkas behöva för att få till en fällande dom kan därmed säkerställas.

Samordningen mellan olika enheter inom polisen spelar en stor roll under utredningen. Framförallt för att kunna nysta upp systematiken vid stora bedrägerihärvor där många målsäganden kan tänkas finnas. Det krävs även att arbetet med att säkerställa bevisningen sker skyndsamt och hanteras rättssäkert, för att kunna åberopas i domstol. Viktiga aspekter i exempelvis en övervakningsfilm är att datum, tidpunkt, och om det är rätt person stämmer med gärningsbeskrivningen för brottet. En polis som har dålig erfarenhet inom rättssystemet kan stöta på vissa svårigheter vid bedrivande av förundersökningen om man missar viktiga detaljer.

Sedan årsskiftet har ett nytt system initierats inom polisen vilket har lett till att datasystemen har synkroniserats nationellt, till syfte att en förundersökning ska bedrivas på samma vis över hela landet och för att ge utredande poliser större möjligheter. Tidigare har det funnits lokala föreskrifter som har skiljt sig beroende på vilken del av landet förundersökningen har bedrivits.

7.3.3 Åtal

När åklagaren väcker åtal i komplicerade och omfattande bedrägerimål, där bedragaren har begagnat sig av exempelvis VPN-tunnlar, trojaner, maskar eller anonyma nätverk krävs en elementär sakframställan av åklagaren. Teknikaliteterna kan vara svåra för rätten att förstå och exakt hur brottet faktiskt har förövats. För att domstolen ska kunna bilda sig en uppfattning om vad målet rör och vad de olika tekniska begreppen innebär, kan det ibland krävas att åklagaren kallar en sakkunnig som vittne, för att reda ut och förklara de olika tekniska begreppen och systematiken i dessa. Det krävs en viss pedagogik samtidigt som det kan vara som att balansera på en knivsegg, för att inte dumförklara rätten. Det handlar om att ge alla i rättssalen en förståelse för vad gärningen handlar om. Under målsägandeförhör och förhör med den misstänkte kan åklagaren gå in på detaljer kring det tekniska, för att därefter ta in en sakkunnig expert som verifierar de tekniska detaljerna till syfte att ge rätten en ökad förståelse för vad det handlar om. Åklagaren måste på ett trovärdigt och pedagogiskt sätt förklara för rätten hur händelseförloppet/brottet har gått till.

”Förstår rätten det objektiva för att kunna se vad som är bevisat?”

- Marie Wallin, åklagare, f.n. bedrägerispecialist inom polismyndigheten.

7.3.4 Hur kan man stävja problematiken med nätbedrägerier?

Ett gemensamt problem bland alla kreditgivare är att rutinerna är alldeles för undermåliga med att säkerställa kundernas identitet. Man skulle behöva se över nya lösningar, som exempelvis chip i ID-handlingar eller ett bättre nyttjande av identifiering genom fingeravtryck. En annan lösning vore elektronisk identifiering.

Att dessutom informera och utbilda personal som arbetar med att verifiera ID-handlingar manuellt vid utlämning av varor och krediter på exempelvis postutlämningsställen skulle kunna bidra till att färre bedragare kan ta ut varor och krediter i annans namn. Enligt Marie Wallin finns det många exempel på fall där personalen inte har varit noggrann eller har varit stressad och därför inte uppmärksammat vissa brister i en presenterad ID-handling. Har personalen däremot god information om exakt vilka sorters ID-handlingar som finns och exakt hur de ska se ut, hur man verifierar äktheten av dessa så kommer det med stor sannolikhet att ge positiva utslag.

Genom att öka bevakningen i samhället med fler kameror kan man även säkerställa mer bevisning i brottmål. Polisen har exempelvis med hjälp av bankomatkameror kunnat samla värdefull bevisning, vilket har lett till fällande domar i åtal avseende bland annat misshandel, där misshandeln har skett i nära anslutning till bankomaten. Kamerorna i bankomaten har således lyckats fånga brottet på film och åklagaren har med exakt datum- och tidsangivelse kunnat presentera när och hur brottet har ägt rum. Även övervakningsfilmer från 7-eleven har lett till fällande domar i bedrägerimål. Där har bedragaren på ett skickligt sätt gjort sig skyldig till grov stöld genom att stjäla bankomatkortet genom målsägandens ficka och därefter gått till bankomaten och begått bedrägeriet. Åklagaren har genom övervakningsfilmen lyckats styrka brottet väldigt noggrant. Gärningsbeskrivningen har på så vis blivit mer transparent med tidsangivelser exakt på sekunden och med detaljer kring hur brottet har förövats.

8. Analys och slutsats

Inom straffrätten råder legalitetsprincipen som medför att lagen ska tolkas restriktivt. Det innebär att det som står uttryckligen i lagtexten är det som gäller. Utrymme för fristående bedömningar är små då legalitetsprincipen är grundlagsstadgad, enligt RF 1:1 och 2:10. Det får till följd att tolkningen av begreppet bedrägeri kan behöva utökas av lagstiftaren, för att omfatta vissa typer av nätbedrägerier som kan vara svårare att bevisa och tolka in under begreppet.

När en person har drabbats av dataintrång eller nätbedrägeri och fått krediter tagna i sitt namn eller fått sitt konto tömt på likvida medel är standardsvaret från banken eller kreditgivaren att ”alla får sina pengar tillbaka”. Det får gemene man att tänka att brottet har gjorts ogjort, medan det i själva verket är iscensatt från bankernas och kreditgivarnas sida för att få oss att tänka precis så. Om brottsoffret får sina pengar tillbaka, eller slipper betala tillbaka krediten som har tagits i dennes namn, då finns ingen anledning till oro för den som har blivit utsatt för bedrägeriet. Då finns det heller ingen anledning till att nysta vidare i varför brottet har kunnat äga rum. Banker och kreditgivare tycker många gånger att det är värt att ersätta den som har blivit utsatt för bedrägeri, för att de i slutändan ska kunna maximera sin vinst och minimera mängden dålig uppmärksamhet för sig själva. [49]

I de flesta fall av nätbedrägerier, läggs ansvaret för att upprätta en polisanmälan i den bedragnes händer. Endast i de mest omfattande bedrägerifallen kan banken eller kreditgivaren vara den som märker bedrägeriet före brottsoffret. Det får till följd att om den drabbade inte vidtar åtgärder, så kan denne bli återbetalningsskyldig. Fallet med William Varga ovan är ett typexempel på ett sådant bedrägerifall. Tack vare Williams snabba och handlingskraftiga agerande lyckades han undkomma betalningsansvar. Ett av bedrägeriärendena ledde dessutom till en rättstvist, som han med hjälp av ett skickligt juridiskt ombud lyckades undkomma betalningsansvar för.

I en perfekt värld, där banker och kreditgivare i en samordnad insats, samlar polisanmälningar som lämnas in direkt från bankernas bedrägeriavdelningar skulle det leda till att arbetet inom polisens bedrägerirotel skulle kunna ske betydligt mer effektivt vid omfattande organiserade nätbedrägerier. Resurser skulle således även frigöras till andra former av polisarbete, vilket

[49] Goldberg, Daniel, Larsson, Linus, Korthuset, Norstedts, 2014, s. 11-12

skulle leda till att fler bedrägerier skulle kunna stoppas och fler gärningsmän skulle kunna ställas till svars. Det är dock inget som banker och kreditgivare tidigare har varit intresserade av. Att samarbeta med polisen skulle kunna leda till att alla uppgifter i ett bedrägerifall blev allmänt kända. Det skulle kunna få förödande konsekvenser för banker och kreditgivare om allmänheten skulle inse hur utbredda nätbedrägerierna är och hur enkla de, i vissa fall, är att genomföra. [50]

Antingen är det lönsamt att införa säkerhetssystem som är ogenomträngliga, vilket då följer av en strikt ekonomisk logik att det borde göras omedelbart och fullt ut. Eller så är det alldeles för kostsamt att byta ut systemen, vilket gör det mer lönsamt att ersätta bestulna och bedragna kunder istället för att täppa till systemens hål. Det leder till att man hellre tystar ned antalet bedrägerifall och låter allmänheten vara ovetandes om vad som sker bakom kulisserna. Så länge de slipper betala ur egen ficka så är kunderna nöjda. Vid en viss punkt kan det dock hända att kostnaden för bedrägerierna tippar över och överstiger kostnaden för att täppa till de hål som finns i säkerhetssystemen. Då kan det gå väldigt fort för banker och kreditgivare att implementera nya säkerhetssystem. Men inte heller de åtgärderna behöver vara helt perfekta. Det kan räcka med att uppgradera systemen så pass mycket att bedrägerierna ska kosta mer i tid eller pengar att genomföra, än vad brottslingen faktiskt gör i vinst. Det får automatiskt till följd att brottslingarna hittar nya eller andra brott att begå, mot andra måltavlor. [51]

Det kan även vara på så vis att ju fler bedrägerier en bank eller kreditgivare väljer att stoppa, desto fler legitima transaktioner riskerar att stoppas på vägen. Det får till följd att banker och kreditgivare går miste om viktiga affärer, vilket kan leda till att kunderna vänder sig till något annat företag för att genomföra sina affärer eller transaktioner. Ur bankernas och kreditgivarnas perspektiv är säkerhet inget självändamål. Det är intressant så länge det innebär att lönsamheten för näringsidkarna ökar. Att stoppa bedrägerierna helt och hållet är nästintill en omöjlig uppgift. Däremot fokuserar många banker och kreditgivare på att hålla de på en rimlig nivå, så att kreditförlusterna inte blir allt för höga. Det handlar om en avvägning mellan att kostnaderna skenar iväg så mycket att det inte är rimligt att stoppa bedrägerierna, till att bedrägerierna inte får urholka hela systemet och ge sken av att säkerhetssystemen är så dåliga att kunderna tappar förtroende.[52]

[50] Goldberg, Daniel, Larsson, Linus, Korthuset, Norstedts, 2014, s. 140-143

[51] Goldberg, Daniel, Larsson, Linus, Korthuset, Norstedts, 2014, s. 206-207

[52] Goldberg, Daniel, Larsson, Linus, Korthuset, Norstedts, 2014, s. 230-236

Ross Andersson, professor i säkerhetsteknik vid Cambridge University jämför bedrägerifall med fall där en flygolycka har skett. När en flygolycka inträffar kastar sig polis, brandkår, luftfartsmyndigheter, flygpersonalens fackförbund, media och politiker över den tragiska flygolyckan och kommenterar vad som har hänt och kommer med förslag på hur liknande olyckor ska kunna förhindras. Det finns en stark upparbetad mekanism för att flygbolagen ska lära sig av sina misstag. Ross Andersson menar att det är tvärtom i banksfären. Där utreder bankerna hellre intrången själva, för att information inte ska läcka ut till media och allmänheten. De interna utredningarna sker oftast till syfte att lista ut hur bankerna ska agera för att samma typ av bedrägeri inte ska kunna inträffa igen, inte för att ställa aktuella gärningsmän till svars. Det får till följd att bedragarna hinner sopa igen spåren efter sig och fly, innan brottet har hunnit anmälas till polisen. I andra fall kan det vara så att bankerna inte släpper ifrån sig information vid eventuella brottsutredningar. Det finns starka incitament att tysta ned det inträffade, för att på så vis göra det omöjligt för utomstående att granska säkerhetssystemens luckor. Det får till följd att det i slutändan inte är någon som granskar det inträffade och inte heller någon som lär sig av sina misstag. [53]

8.1 Reflektioner och slutsats

Att lagstiftningen inte har hängt med den tekniska utvecklingen har resulterat i att många gärningsmän slipper straffansvar. Även problematiken med att samla bevismaterial skyndsamt och behovet av att bedriva en snabb och effektiv förundersökning får till följd att brottslingar som är duktiga på nätbedrägerier effektivt kan sopa undan spåren efter sig. Det leder till att utredningarna kör fast och sedermera läggs ned. Således anser jag att den nuvarande lydelsen i 9 kap 1 § BrB kan behöva en uppdatering. På så vis kan ett förtydligande av bedrägeribrottet implementeras och begreppet bedrägeri vidgas.

Av rättsfallsreferaten i avsnitt 6 framgår att straffvärdet för bedrägeribrott är relativt lågt. För att påföljden ska resultera i kännbara och avskräckande fängelsestraff för bedragarna krävs att brottet rubriceras som grovt bedrägeri. Den framtagna brottsstatistiken i avsnitt 2.4 avslöjar även att bötesstraff kombinerat med villkorlig dom är den vanligaste påföljden för bedrägeribrott. Den direkta slutsats som jag drar av det är att lagstiftningen inte är tillräckligt avskräck-

[53] Goldberg, Daniel, Larsson, Linus, Korthuset, Norstedts, 2014, s. 244-245

ande för att förmå gärningsmännen till att inte begå de aktuella brotten. En straffskärpning i avskräckande syfte skulle kunna resultera i att färre brott begås. Sanktionerna för att begå bedrägeribrott behöver ha en avskräckande verkan och inte finnas till enbart som straff. När en gärningsman har lyckats tillskansa sig ekonomisk vinning till betydande värden krävs kännbara påföljder som straff, för att förmå andra att inte begå samma misstag. Min bedömning är att lagstiftaren genom straffskärpning kan uppnå viss effekt, i form av att lagstiftningen kan agera avskräckande för den som planerar att begå bedrägeribrott.

Straffskalan har, som konstaterats i tidigare avsnitt i uppsatsen, inte bara betydelse för straffmätningen, utan också för hur utredningen av brottet prioriteras och vilka tvångsmedel som kan och får användas under utredningen. Straffskalan återspeglar även lagstiftarens och samhällets syn på hur klandervärt det aktuella brottet är. Att bli utsatt för bedrägeri utgör många gånger ett intrång i brottsoffrets privata sfär och kan uppfattas som kränkande. Det kan även få allvarliga ekonomiska och sociala konsekvenser för den drabbade. Med anledning därav finns skäl att se över straffskalan för bedrägeribrotten så att straffskalan återspeglar brottens svårhet och de konsekvenser som brottsoffren många gånger får leva med.

Problemet med nätbedrägeribrott är som konstaterat omfattande och behöver åtgärdas. Åtgärderna kan ske genom lagstiftning, för att hindra att bedragare lyckas tillskansa sig ekonomisk vinning och skada både näringsidkare och privatpersoner. En annan åtgärd vore även ett starkare samarbete mellan banker, kreditgivare och polismyndigheten. Om fler bedragare åtalas för de brott de har begått kommer öka förtroendet för rättssystemet att öka bland banker, kreditgivare och allmänheten.

Ett förslag som presenterades av Evert Norberg, förundersökningsledare inom polisens bedrägerirotel, vore att förhindra urkundsförfalskningar och missbruk av urkund genom att implementera nya krav på hur ID-handlingar ser ut, används och dess äkthet säkerställs. Införandet av högre krav på elektronisk identifiering är en faktor som skulle kunna bidra till att antalet urkundsförfalskningar och missbruk av urkund minskar markant.

Slutsaten är att en straffskärpning av bedrägeribrott kombinerat med ett implementerande av lagförslaget som presenteras i avsnitt 9, kan få till följd att färre brottsoffer drabbas av nätbedrägeribrott och att samhället således kan spara resurser som kan användas till att utreda andra brott.

Att lagstifta behöver inte vara den bästa lösningen, det går givetvis inte att lagstifta om allt. Jag anser dock att problematiken med nätbedrägerier inte har nått sin kulmen ännu. Bedragarna kommer säkerligen att hitta nya tekniska system och tillvägagångssätt som proaktivt behöver bekämpas. Genom att ställa högre identifieringskrav så skulle en del av brotten kunna förhindras. Det finns även mycket som talar för att samtliga parter skulle kunna vinna på ett lagförslag som ställer högre krav på identifiering vid kreditgivning och försäljning av varor på kredit över internet. Det skulle inte förhindra samtliga nätbedrägerifall, men om endast en del av fallen kan förhindras skulle det innebära en vinst för näringsidkarna, brottsoffer och samhället. Nedan presenteras ett framtaget lagförslag, för att skärpa identifikationskraven för banker och kreditgivare vid konsumentkreditgivning över internet. Lagförslaget syftar till att ställa krav på kreditgivare att säkerställa kredittagarens identitet via tekniska verktyg och elektronisk identifiering.

9. Lagförslag

Den snabba tekniska utvecklingen inom området att sluta bindande elektroniska avtal har i vissa fall fått till följd att rättsväsendet har halkat efter och har stora svårigheter att komma till rätta med denna relativt nya brottslighet. För att stärka konsumentskyddet och proaktivt komma till rätta med de omfattande problem som uppstår vid identitetsstöld krävs lagstiftning på området. Frågan torde inte kunna regleras på ett tillfredsställande sätt med andra medel. För att värna om konsumenters rättigheter vid ingående av kreditavtal så föreslår jag att Riksdagen inför en lag om krav på identitetskontroll vid elektronisk kreditgivning.

9.1 Förslag till lagtext

Lag (XXXX-XX) om identifieringskrav vid kreditgivning till konsumenter över internet.

1 § Denna lag innehåller bestämmelser om yrkesmässig verksamhet med konsumentkrediter som består i att elektroniskt lämna eller förmedla krediter till konsumenter. Lagen gäller verksamhet med konsumentkrediter som drivs med tillstånd enligt lagen (2004:297) om bank- och finansieringsrörelse och lagen (2014:275) om viss verksamhet med konsumentkrediter.

Denna lag gäller även för utländska företags verksamhet med konsumentkrediter i Sverige.

2 § I lagen avses med

elektroniskt konsumentkreditavtal: avtal om kredit som ingåtts elektroniskt mellan konsument och kreditgivare,

konsument: en fysisk person som handlar huvudsakligen för ändamål som faller utanför näringsverksamhet,

kreditgivare: kreditinstitut som faller under lagen (2004:297) om bank- och finansieringsrörelse och lagen (2014:275) om viss verksamhet med konsumentkrediter.

elektronisk identifiering: en process inom vilken personidentifieringsuppgifter i elektronisk form, som unikt avser en fysisk eller juridisk person eller en fysisk person som företräder en juridisk person, används.

autentisering: en elektronisk process som gör det möjligt att bekräfta den elektroniska identifieringen för en konsument.

3 § Innan elektroniskt avtal om konsumentkredit ingås ska kredittagarens identitetet autentiseras genom elektronisk identifiering. Detta ska ske genom verifierad e-legitimation, bank-ID, mobilt bank-ID eller av berörd myndighet andra godkända elektroniska identifieringsverktyg.

4 § Finansinspektionen har tillsyn över att bank- och kreditinstitut följer skyldigheterna enligt denna lag.

5 § Om verksamhet bedrivs i strid med denna lag ska Finansinspektionen förelägga verksamhetsutövaren med vite. Vid upprepade förseelser ska Finansinspektionen besluta om återkallelse av tillstånd beviljat enligt lagen (2004:297) om bank- och finansieringsrörelse och lagen (2014:275) om viss verksamhet med konsumentkrediter.

6 § Denna lag träder i kraft den XX-XX-XXXX.

9.2 Motiv

Bedrägerier över internet har som konstaterat ovan ökat explosionsartat. Offentlighetsprincipen gör det möjligt för vem som helst att anonymt få tillgång till offentliga myndigheters personregister. Sociala medier så som Facebook är också en vanlig källa till information om pri-

vatpersoner. Med hjälp av olovlig hantering av personuppgifter kan bedragare elektroniskt ansöka om kredit hos befintliga kreditinstitut. Internetbedrägerier är svåra och tidskrävande att utreda och polisen saknar ibland tillräckliga resurser. Svårigheterna med att hitta bedragarna ligger ofta i deras skickliga döljande av alla elektroniska spår, t.ex. genom skyddade IP-adresser, servrar och anonyma nätverk. De enskilda brotten rör i vissa fall mindre summor vilket leder till att polisen, med hänvisning till 23 kap 4a § RB, ofta lägger ner utredningar i brist på resurser. Polismyndigheten har nyligen upprättat ett nationellt bedrägericenter, NBC, med uppgift att huvudsakligen fokusera på denna typ av brottslighet. Där ligger dock tyngdpunkten på att hitta och lagföra bedragarna medan lagförslaget i stället syftar till att förhindra att bedrägeribrott, i samband med kreditgivning, överhuvudtaget sker. Det är således en proaktiv lösning.

Om kreditföretagen använder sig av ett elektroniskt identifieringsverktyg kan en identifiering av kredittagaren utföras med betydligt säkrare resultat än utan. Med ett sådant verktyg identifierar sig kredittagaren elektroniskt och kreditgivaren måste autentisera uppgifterna innan ett avtal kan komma till stånd.

9.2.1 Konsumentperspektivet

Ur ett konsumentskyddsperspektiv motiveras den lagstiftning som jag föreslår av de många problem som uppstår för en privatperson som fått sin identitet stulen. Personnumret måste då spärras vilket medför många praktiska problem i det dagliga livet. Vid anmälan om brott inleds sedan en process genom rättssystemet, där bevisbördan till viss del ligger på den drabbade. I förarbetet (SOU 2013:85) om identitetsstöld poängteras den svåra integritetskränkning som detta brott medför vilket i sin tur kan leda till stress, ångest och depressioner. Privatpersoner behöver därför ett starkare skydd eftersom kreditgivning över internet ökar. Vad som ytterligare motiverar en ad hoc lösning av problemet genom lagstiftning är lagens möjligheter att bekämpa den organiserade brottslighet som frodas inom detta område. Med anledning härav krävs en proaktiv insats, där krafttag tas mot problemet med identitetskapningar. En lagstiftning om krav på identitetskontroll vid elektronisk kreditgivning till konsumenter kan bidra till att stävja problemet. Genom införande av lagförslaget åläggs kreditgivarna skärpta krav för att noggrant kontrollera och säkerställa kredittagarnas identitet. Det kan antas leda till att antalet bedrägerier med stulna identiteter minskar.

Införandet av identifieringskrav kan innebära ökade svårigheter för vissa personer att ansöka om kredit via internet. Dels finns det personer som inte har tillgång, eller möjlighet att ansluta sig till något av de identifieringssystem som finns tillgängliga på marknaden. Dels innebär identifieringskravet ett ytterligare steg i den snabba digitaliseringen av samhället. För de grupper som redan har svårigheter att anpassa sig till denna, på grund av låg kunskap om och förståelse för den digitala världen, medför införandet ännu en tröskel, eftersom det involverar ytterligare ett moment som måste utföras. Den sammanlagda nytta som ett införande av identifieringskrav vid krediter tagna över internet uppnår, överväger dock de eventuella problem som det kan medföra.

9.2.2 Näringsidkarperspektivet

Lagförslaget främjar även kreditgivarna som, på grund av bedrägerierna, i hög utsträckning drabbas av ökade kostnader i form av högre personalkostnader för att hantera alla bedrägerianmälningar samt de kreditförluster som uppstår. Anslutande till de identifieringssystem som krävs vid ett införande av identifieringskrav vid kreditgivning till konsumenter över internet kräver, kommer initialt att öka kreditgivarnas kostnader. Skärpta krav på identifiering kommer dock medföra att fullbordade bedrägerier minskar markant, vilket innebär minskade kreditförluster för kreditgivarna, lägre arbetsbelastning och därmed minskade personalkostnader. Ur ett långsiktigt perspektiv kommer således kreditgivarna att minska sina kostnader och på så vis att gynnas av lagförslaget.

9.2.3 Samhällsekonomiska aspekter

Lagstiftaren bör anpassa sig till dagens snabba tekniska utveckling genom att införa en lagstiftning för att uppnå säker elektronisk identifiering vid kreditgivning på internet. Genom att lagstifta i frågan och därmed säkerställa att kreditgivarna autentiserar kredittagarnas identitet uppnås två rättsekonomiska fördelar. Det kan även antas att bedrägeribrotten kommer att minska i sin helhet, dels leder det till en effektivisering av brottsutredningar vid nätbedrägerier.

Genom att färre bedrägeribrott begås, blir resultatet att företagen gör färre kreditförluster och att utsatta privatpersoner slipper risken att skuldsättas och eventuellt hamna hos Kronofogden. Det sparar i sin tur det allmännas resurser genom att färre ärenden anmäls, vilket tar upp resurser hos polisen, rättsväsendet och Kronofogden. Det gynnar således samhället ur ett samhällsekonomiskt perspektiv.

Lagförslaget kommer slutligen att resultera i ett ökat förtroende för elektronisk kreditgivning, vilket leder till att fler vågar förlita sig på den elektroniska kreditgivningsmarknaden. Ökade krav på kreditgivare leder dessutom till självsanering av branschen vilket får till följd att mindre seriösa aktörer försvinner från marknaden. Detta i sin tur leder till ytterligare ökat förtroendekapital för de kreditgivare som anpassar verksamheten efter den nya lagstiftningen.

Lagförslaget kan tänkas indirekt leda till positiva miljöeffekter genom att ett ökat förtroende för elektroniska transaktioner leder till ett stegvis virtualiserande av samhället. Detta innebär färre transporter, minskade utsläpp, minskad kontant- och pappershantering.

9.2.4 Förhållandet till gällande rätt

I dagsläget finns det ingen reglering på området avseende krav på identifiering vid elektronisk kreditgivning. Lagar där man skulle kunna tänka sig att finna bestämmelser av denna art är t.ex. konsumentkreditlagen och lagen (2014:275) om viss verksamhet med konsumentkrediter, men så är inte fallet. Inte heller lagen (2000:832) om kvalificerade elektroniska signaturer nämner något om elektronisk identifiering. Lagförslaget kolliderar därmed inte med någon lag utan utgör ett komplement till befintlig lagstiftning.

Dagens reglering ger straffrättsligt skydd mot bedrägeriet när någon annans identitet olovligen används, däremot finns det inte något straffrättsligt skydd mot själva användandet av någon annans identitet. Ny lagstiftning är dock under beredande. I SOU 2013:85 föreslås att olovlig användning av andras identitetsuppgifter bör straffbeläggas.

En föregångare på området är Finland. I den finska konsumentskyddslagens 7 kap 15 § stadgas att en kreditgivare innan ett avtal om konsumentkredit ingås noggrant ska kontrollera den sökandes identitet. Om identiteten kontrolleras elektroniskt, ska kreditgivaren använda en identifieringsmetod som uppfyller kraven i lagen (7.8.209/617) om stark autentisering och elektroniska signaturer.

Lagförslaget står även i överensstämmelse med Europaparlamentets och Rådets Förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG. Denna syftar till att öka förtroendet för elektroniska transaktioner på den inre marknaden genom att tillhandahålla en gemensam grund för ett säkert elektroniskt samspel mellan medborgare, företag och offentliga myndigheter, och därigenom öka effektiviteten hos offentliga och privata nättjänster, elektroniska affärsverksamheter och e-handel i unionen. Enligt förordningen bör medlemsstaterna uppmana den privata sektorn att frivilligt använda medel för elektronisk identifiering där detta behövs för nättjänster eller elektroniska transaktioner. Medlemsstaterna har dock även möjlighet att genom lagstiftning införa nationella bestämmelser.

9.2.5 Sammanfattning av lagförslaget

Nätbedrägerier med identitetsstölder ökar lavinartat och en stor del av dessa utgörs av ingående av konsumentkreditavtal i annans namn. Denna typ av brottslighet är svårutredd och leder till stora negativa ekonomiska, praktiska och emotionella konsekvenser för de privatpersoner som drabbas. Då elektronisk kreditgivning ökar behövs ett starkare skydd. Proaktiva insatser, där krafttag tas mot problemet med identitetskapningar, krävs därför. Lagförslaget om krav på identitetskontroll vid elektronisk kreditgivning till konsumenter syftar därför till att förhindra att elektroniska kreditavtal ingås med någon annans identitet. Det mesta tyder på att marknaden för elektronisk kreditgivning kommer fortsätta att öka vilket gör frågan till ett långsiktigt och växande problem. Lagstiftning är därför nödvändig för att nå ett effektivt och tillfredsställande skydd.

Lagförslaget utgör en pedagogisk, konkret och konstruktiv lösning på det befintliga problemet. Det passar även systematiskt väl in i gällande rätt på området. De eventuella problem som ett införande av identifieringskrav vid krediter tagna över internet kan medföra för vissa konsumentgrupper, uppvägs av den sammanlagda nytta som ett sådant införande uppnår.

Införandet av lagen om identifieringskrav vid kreditgivning till konsumenter över internet leder dessutom till ekonomiska fördelar för samhället i stort genom att bedrägeribrotten kan antas minska i sin helhet och genom en effektivisering av brottsutredningar vid elektroniska bedrägerier. Det är även till kreditgivarnas fördel som ur ett långsiktigt perspektiv drabbas av färre bedrägeriförsök vilket leder till minskade kreditförluster och kostnader för att hantera

dessa. Det kan också antas att införandet av ett identifieringskrav kommer att leda till en självsanering av branschen, vilket inte bara är en vinst ur konsumenthänsyn utan även gagnar de seriösa aktörerna på marknaden.

10. Slutord

När jag själv fick min identitet stulen under år 2011 märkte jag det först genom att jag fick hem en kopia på en kreditupplysning, där Resurs Bank hade tagit en kreditupplysning på mig. Dagen därpå kom ännu en kreditupplysning, från Hallbergs Guld, där någon hade försökt köpa smycken på kredit till ett värde av 15 000 kr. Ett par dagar senare fick jag två brev från Telia, som välkomnade mig som ny kund och abonnent. Jag insåg då att något inte stod rätt till och ringde till respektive företag för att ta reda på mer. Samtliga var hjälpsamma och gav mig rådet att polisanmäla händelsen och skicka en kopia till dem. Därefter återkallades alla krav och jag hade turen att slippa allvarliga konsekvenser. Förundersökningen lades dock ned och polisen hittade aldrig den eller de gärningsmän som hade gjort sig skyldiga till att ha stulit min identitet och utfört bedrägerierna. Mitt handlingskraftiga agerande resulterade i att jag kom lindrigt undan. Men alla har inte en sådan tur. Brottsoffer som har insikt i hur man ska agera handlingskraftigt om man blir utsatt för brott för att skydda sina tillgångar och lindra skadeeffekterna av brottet, har bättre möjligheter att vidta åtgärder än den som inte har den insikten. Om en person exempelvis är bortrest under en längre period och inte har möjlighet att agera lika snabbt som jag gjorde, då är dennes chanser betydligt sämre att slippa eventuella betalningskrav. Eller om någon är sjuk eller på annat sätt har nedsatt handlingsförmåga, kan det påverka handlingskraftigheten hos den utsatte.

Med anledning därav är det hög tid för lagstiftaren att agera och se över den lagstiftning som finns idag. Antingen genom att stifta nya lagar som ställer högre krav på näringsidkarna, eller genom att skärpa straffansvaret för bedrägerier, missbruk av urkund, urkundsförfalskning och osant intygande.

Källförteckning

Litteratur

Ahola, Mikael, Bedrägeri: introduktion och handledning för brottsutredare, 1 uppl., Norstedts Juridik, 2013

Goldberg, Daniel, Larsson, Linus, Korthuset – hur tjuvarna flyttade ut på nätet och varför din bank lät det hända, Norstedts, 2014

Holmquist, Rolf, Brotten i näringsverksamhet, 3 uppl., Norstedts, 2013

Jareborg, Nils, Asp, Petter, Friberg, Sandra, Ulväng, Magnus, Brotten mot person och förmögenhetsbrotten, 2 uppl., Iustus, 2015

Kleineman, Jan, Juridisk metodlära, Korling Fredric, Zamboni, Mauro, upplaga 1:3, Studentlitteratur, 2013,

Sterzel Georg, Månsson Catharina, Borgeke, Martin, Kezovska, Gina, Palm, Mats, Reimer, Stefan, Påföljdspraxis, 5 uppl., Jure Förlag, 2013

Svenska Bankföreningen, Banker i Sverige 2013

Offentligt tryck

Propositioner

Prop. 1985/86:65

Med förslag till ändring i BrB m.m. (vissa frågor om datorrelaterade brott och ocker)

Statens offentliga utredningar

Stärkt straffrättsligt skydd för egendom, SOU 2013:85

Myndighetspublikationer

Färdeman, Hvitfeldt, Irlander, Brottsförebyggande rådet, Utsatthet för brott år 2012, Resultat från nationella trygghetsundersökningen (NTU), 2013

Beslagshandbok, Utvecklingscentrum i Malmö, Åklagarmyndigheten, november 2013,

Elektroniska källor

Motion 2013/14:Ju216, riksdagen.se (hämtad 2015-02-16)

Brottsförebyggande rådet, Bedrägeri och ekobrott, http://www.bra.se/bra/brott-och-statistik/bedragerier-och-ekobrott.html, hämtad 2014-01-15

Friberg, Sandra, Brottsbalk (1962:700) 9 kap. 1 §, Lexino 2013-05-15

Friberg, Sandra, Brottsbalk (1962:700) 9 kap. 3 §, Lexino 2012-07-01

Lindberg, Gunnel, Rättegångsbalk (1942:740) 27 kap. 1 §, Lexino 2014-07-01

Polisen, Identitetsstöld – Skydda dig, https://polisen.se/Utsatt-for-brott/Skydda-dig-mot-brott/Bedrageri/Identitetsstold---Skydda-dig/ (hämtad 2015-02-19)

Polisen, Identitetsstöld – Utsatt, https://polisen.se/Utsatt-for-brott/Olika-typer-av-brott/Bedrageri/Identitetsstold--utsatt/ (hämtad 2015-02-19)

Internetservice i Väst AB, Vad är en IP-adress? http://www.hittaip.se/info.php (hämtad 2015-02-10)

TOR, About TOR, https://www.torproject.org (hämtad 2015-02-09)

Vad är en Trojan?, Kaspersky Lab, http://www.kaspersky.com/se/internet-security-center/threats/trojans (hämtad 2015-02-16)

Övervakning och loggegenskaper, Relytec, http://www.relytec.com/keylogger_se/keylogger.htm (hämtad 2015-02-16)

What is a computer virus or a computer worm?, Kaspersky Lab, http://www.kaspersky.com/internet-security-center/threats/viruses-worms (hämtad 2015-02-16)

Åklagarmyndigheten, Tvångsmedel, http://www.aklagare.se/Aklagarens-roll/Forundersokningen/Tvangsmedel/ (hämtad 2015-02-26)

Åklagarmyndigheten, Åtalsunderlåtelse och förundersökningsbegränsning, http://www.aklagare.se/Aklagarens-roll/Atalsbeslutet/Atalsunderlatelse/ (hämtad 2015-04-09)

https://www.iis.se/lar-dig-mer/guider/dns-internets-vagvisare/sa-fungerar-dns/ (hämtad 2015-05-18)

http://www.google.se/intl/sv/goodtoknow/web/101/ (hämtad 2015-05-20)

https://www.bankofscotland.co.uk/HelpCentre/pdf/credit-scoring-guide.pdf (hämtad 2015-05-20)

http://www.creditsafe.se/vanliga-fraagor/spaerra-ditt-personnummer/ (hämtad 2015-05-22)

Bildkällor

https://www.torproject.org/about/overview.html.en (Hämtad 2015-02-09)

Rättsfall

NJA 1983 s. 441

Svea hovrätts dom i mål HovR B 5233-12

Göta hovrätts dom i mål HovR B 2274-12

Hovrätten över Skåne och Blekinges dom i mål HovR B 2679-09

Svea hovrätts dom i mål B 8025-13

Svea hovrätts dom i mål B 6351-13

Svea hovrätts dom i mål B 1019-12

Svea hovrätts dom i mål B 906-07

Stockholms tingsrätts mål med målnummer T 14989-14