Oppdragsrapport nr. 2-2010

Lisbet Berg og Ragnhild Brusdal

Identitetstyveri i tillitsfulle systemer

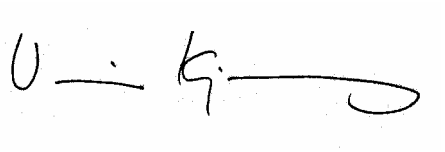
SIFO

Oppdragsrapport nr. 2 – 2010

STATENS INSTITUTT FOR FORBRUKSFORSKNING
Sandakerveien 24 C, Bygg B
Postboks 4682 Nydalen
0405 Oslo
www.sifo.no

SIFO Statens institutt for forbruksforskning
National Institute for Consumer Research

Oppdragsrapport nr. 2 - 2010

Tittel	**Antall sider**	**Dato**
Identitetstyveri i tillitsfulle systemer	50	03.02.2010
Forfatter(e)	**Prosjektnummer**	**Faglig ansvarlig sign.**
Lisbet Berg og Ragnhild Brusdal	11-2009-27	

Oppdragsgivere:

Barne-, likestillings- og inkluderingsdepartementet, Nærings- og handelsdepartementet, Fornyings-, administrasjons- og kirke-departemenet

Sammendrag:

Det finnes ikke god statistikk i Norge som kan si noe sikkert om omfanget av identitetstyveri. Men uansett hvor stort eller lite omfanget av identitetstyveri skulle være, er det å bli utsatt for identitetstyveri alvorlig for de som rammes.

Identitetstyveri i tillitsfulle systemer

En foreløpig vurdering av identitetstyveri i Norge

av

Lisbet Berg og Ragnhild Brusdal

2010

STATENS INSTITUTT FOR FORBRUKSFORSKNING
postboks 4682 Nydalen, 0405 Oslo

Forord

Barne-, likestillings- og inkluderingsdepartementet, Nærings- og handelsdepartementet og Fornyings-, administrasjons- og kirkedepartementet har bedt SIFO om å samle tilgjengelig kunnskap om *identitetstyveri,* og samtidig vurdere behovet for undersøkelser som kan belyse dette fenomenet ytterligere. I det foreliggende notatet drøftes relevante og anvendelige definisjoner, og vi viser til tall som kan si noe om omfanget og hvilke problemer identitetstyveri representerer for ofrene.

Vi har snakket med representanter for institusjoner og bedrifter som kan tenkes å ha kunnskap om feltet. Her kan nevnes: Datatilsynet, Finanstilsynet, ØKOKRIM, NorSIS, Politidirektoratet, Kripos, Finansnæringens fellesorganisasjon og Sparebankforeningen, Forbrukerrådet, teleselskaper, banker, Veivesenet, Skattedirektoratet, Skattekontoret, Brønnøysund registrene, Kredittopplysningsbyråer, m.fl. Ikke alle hadde opplysninger som var relevante for prosjektet.

Til prosjektet har det vært knyttet en referansegruppe bestående av Magnar Aukrust (JD), Sjur Eigil Dahl (NHD), Cort Archer Dreyer (FAD), Ellen Gjemdal (FIN), Eivind Gram-Johannessen (BLD), Torbjørn Hagerup Nagelhus (JD), Åste Marie Skullerud (FAD), Camilla Closs Walmann (BLD), Liv Hilde Westrheim (NHD), Jens Christian Westly (FIN) som har bidratt med nyttige innspill og diskusjoner.

En spesiell takk til identitetsofrene som har delt sine erfaringer og historier med oss.

SIFO, 1.3.2010

Innhold

Sammendrag

Identitetstyveri – eller *uautorisert tilegning og misbruk av en annens identitet* - benyttes i ulike former for svindel og representerer i følge Datatilsynet (2009) en risiko for norske enkeltpersoner og bedrifter i form av økonomisk tap, invasjon av privatsfæren, praktiske problemer, avmakt og mistenkeliggjøring. Det forekommer ikke informasjon i tilgjengelige registre som kan si noe om det totale omfanget av identitetstyveri. Det er også vanskelig å si noe om omfanget fordi fenomenet er avgrenset, definert og operasjonalisert på svært forskjellig vis. Uansett frykter man både i Norge og internasjonalt at identitetstyveri er et økende problem. I denne utredningen har vi samlet informasjon og eksisterende tallmateriale som kan belyse fenomenet identitetstyveri i Norge, og sammenstilt dette med informasjon og tallmateriale fra USA, Canada og Danmark. Vi har også intervjuet representanter for institusjoner og bedrifter som på ulikt vis er berørt av fenomenet identitetstyveri og vi har funnet fram til fem identitetstyveriofre som har beskrevet sine historier for oss.

Både tallmaterialer fra andre land, og våre egne intervjuer med ofre for identitetstyverier, kan tyde på at de fleste, men ikke alle, ofre ender opp økonomisk skadefrie. Det er gjerne tredjepart – banken, små og store bedrifter, organisasjoner og institusjoner – som rammes økonomisk: En bedrift som er lurt av en ID-tyv kan ikke fakturere den som er frastjålet sin identitet. De som blir frastjålet sin identitet rammes først og fremst av tidstap og problemer knyttet til oppryddingsarbeidet med å bevise uskyld overfor en - ofte lang - rekke av kreditorer, og et betydelig psykisk ubehag som kan utgjøre en stor belastning over lang tid.

Omfanget av identitetstyveri avhenger av hvordan begrepet defineres og operasjonaliseres, og det kan være hensiktsmessig å se identitetstyveri som en totrinnsprosess: Trinn I viser til ID-tyvens uautoriserte tilegning av personopplysninger, mens trinn II viser til selve misbruket eller bedrageriet basert på en annens identitet. En estimering av trinn I må ta utgangspunkt i personopplysninger på avveie, herunder stjålne bankkort (med bilde), stjålne og bortkomne pass og førerkort, samt datatyverier av f.eks. registre med konto- og personopplysninger. Omfanget på trinn I viser til mulighetsgrunnlaget. En estimering av trinn II må ta utgangspunkt i kriminalitetsstatistikk eller rapporteringer av misbruk basert på representative undersøkelser der identitetstyveri utgjør en egen kategori. Omfanget på trinn II viser til selve misbruket, eller skadene forårsaket ved identitetstyveri. Et tredje mål – som omfatter både trinn I og trinn II, er antall personer som er rammet av identitetstyveri. Vårt inntrykk er at det totale omfanget av identitetstyverier pr. i dag hovedsakelig estimeres på bakgrunn av landsrepresentative offerstudier – altså antall personer rammet av identitetstyveri (USA, Canada, Danmark og Norge).

Det er viktig å huske at *ett* identitetstyveri gjerne resulterer i *mange* bedragerier. Dermed gir det å registrere antall bedragerier, eller misbruk, et helt annet tall en det å registrere identitetstyveri-*ofre*. Begge mål sier imidlertid noe om alvorligheten av problemet.

Alle vi har snakket med i forbindelse med prosjektet mener identitetstyveri er et viktig felt som fortjener større oppmerksomhet, både på registreringssiden og forebyggingssiden. Det er også et felt hvor man forventer en økning eller et større trykk. Det har likevel vist seg vanske-

lig å få ut informasjon som kan si noe om omfanget, enten fordi registreringer ikke finnes, ikke er godt systematisert eller sentralisert, eller generelt sett er mangelfulle. Temaet kan også være ømtålig på bedriftsnivå fordi det å være rammet av ID-tyver antas å kunne påvirke organisasjoners og bedrifters omdømme. Flere informanter etterspør felles registreringer som vil gjøre det mulig å overvåke utviklingen over tid.

Avslutningsvis vil vi vise til tidligere direktør i Forbrukerrådet Per Anders Stalheims lov: *For å få gode systemer må man plassere ansvaret for at noe kan gå galt hos den aktør som kan påvirke risikoen.* Hvis ansvaret legges på forbrukerne, mister institusjonene insitamentet til å lage sikre systemer. Eksempelvis tror vi at utvikling av bankenes velfungerende registre over gyldige og ugyldige bankkort, som i dag er koplet opp mot betalingsterminaler verden rundt, er motivert av bankenes gevinst av å redusere kortsvindel.

For å redusere/hindre økning av omfanget av identitetstyverier, er det også viktig at ansatte i bedrifter og forbrukerne selv blir oppmerksomme på fenomenet, og dermed viser større aktsomhet i forhold til relevante persondata.

1 Innledning

På oppdrag fra Barne-, likestillings- og inkluderingsdepartementet, Nærings- og handelsdepartementet og Fornyings-, administrasjons- og kirkedepartementet har vi her samlet tilgjengelig kunnskap om *identitetstyveri.* I det foreliggende notatet drøftes ulike definisjoner, og vi viser til tall som kan antyde noe om omfanget og hvilke problemer identitetstyveri representerer for ofrene.

Det har vært sagt at Norge framstår som en *stående buffét* for de som vil begå ID-kriminalitet. Hvis dette er riktig, er det svært bekymringsfullt. Dersom fenomenet identitetstyveri får utvikle seg fritt, kan befolkningen i verste fall miste tilliten til finansielle og offentlige institusjoner. Dette vil kunne innebære at forbrukerne ikke lenger vil føle det trygt å benytte bankkort eller å handle på nettet, noe som vil få store konsekvenser for både markedene og velferden.

Norge er et land kjennetegnet av at befolkningen har svært høy tillit til hverandre og til offentlige institusjoner og systemer (ESS 2009, Sødal & Johansen 2009). Tillit er selve limet i samfunnet (Elster 2000). Men veien fra funksjonell tillitsfullhet til naivitet kan være kort. Vi låser ikke alltid dørene, lar ting stå ute om natten og vi gir fra oss privat informasjon i troen på at de fleste er ærlige. Utenlandske kriminelle har beskrevet oss som naive (Angell 2009). Noen stiller spørsmål ved om ikke også systemene i Norge har innslag av naivitet. Datatilsynet mener at få personer i offentlig sektor tenker gjennom faren for masseinnhøsting av informasjon, og at det er lite kritisk sans i forhold til hva som tilgjengeliggjøres for offentligheten (Datatilsynet 2009:22). For eksempel er de lett tilgjengelige, åpne skattelistene, med navn og formuesforhold, en gavepakke til ID-tyver og andre kriminelle (Apenes i Datatilsynet referert i VG, se Fjellheim & Andersen 2009).

Det kan virke som et paradoks at identitetstyveriet næres av nettopp åpenhet, tillitsbaserte systemer og en tillitsfull befolkning, samtidig som identitetstyveriets verste konsekvens er tapt tillit til systemene. Paradokset kan knyttes til offentlige myndigheters politikk om en åpen forvaltning og et sterkt offentlighetsprinsipp på den ene siden, og nødvendigheten av sikre systemer på den andre siden. Videre er det slik at brukervennlige, lønnsomme og effektive systemer bygd på åpenhet og tillit gjerne fortrekkes framfor beskyttelse og sikkerhetskontrollerende systemer. Men er det slik at valget står mellom enkle, effektive og risikable systemer – mot tunge, trege og trygge systemer?

Både i Norge og internasjonalt ser vi en trend som går på å tette huller som har gjort identitetstyveri enkelt. Blant annet er det både i Danmark[1] og Norge anno 2009 gjort endringer slik at det ikke lenger skal være like enkelt for en ID-tyv å få endret et offers adresse, som gjerne er første steg i en ID-tyveriprosess. Det er også mulig å reservere seg mot å få skatteligningen i posten og pass kan man nå hente hos politiet. Videre er alle nye bankkort utstyrt med chip,

[1] For å hinder misbruk av andres identitet har de i Danmark innført legitimeringsplikt ved adresseforandring. (Kruize 2009: 12)

noe som skal gjøre det vanskeligere med 'skimming'[2]. I Norge har NorSIS (Norsk Senter for Informasjonssikring) ledet Identitetstyveriprosjektet, som er finansiert og har partnere fra både offentlige og private institusjoner. Prosjektets hovedmålsetning er å; *redusere/bremse omfanget og konsekvensene av identitetstyverier og misbruk av personopplysninger* (NorSIS 2009:5, www.idtyveri.info). Både Datatilsynet (2009: 10-18) og Identitetstyveriprosjektet (NorSIS 2009: 13-22) skisserer en rekke konkrete tiltak som skal forebygge identitetstyveri (Se også: The President's Identity Theft Task Force Report 2008) .

Fenomenet identitetstyveri er komplekst og vanskelig å avgrense. Dette gjør det problematisk å estimere omfanget av identitetstyveri. For å vise bredden og kompleksiteten vil vi innledningsvis derfor gi eksempler på svært forskjellige, men helt reelle, typer av identitetstyveri, slik begrepet gjerne forstås i Norge. Dernest vil vi kort drøfte fenomenet og ulike definisjoner før omfanget av identitetstyveri - basert på både norske og utenlandske beregninger - kan vurderes. I vurderingen av omfanget av identitetstyverier i Norge tar vi først utgangspunkt i såkalt offerundersøkelser, dvs. beregninger av omfang basert på landsrepresentative surveys. Deretter drøftes tall – og mangel på tall – fra eksisterende registre som kan si noe indirekte om utbredelsen av identitetstyveri.

1.1 Metode

Hensikten med denne utredningen har vært å samle statistikk og innsikt om fenomenet identitetstyveri. Vi har nærmet oss feltet fra flere vinkler: i) *Intervjuer med representanter for institusjoner og bedrifter* som på ulikt vis er berørt av fenomenet identitetstyveri. ii) *Dokumentstudier* med fokus på eksisterende tall og registre som kan si noe om utbredelsen av fenomenet i Norge, Danmark, USA og Canada. iii) *Intervjuer med identitetstyveriofre*.

Vi har gjennomført ansikt til ansikt intervjuer med personer i ØKOKRIM, NorSIS, Datatilsynet og Finanstilsynet. Disse intervjuene ble tatt opp på lydbånd. Alle har fått tilsendt og lest gjennom rapporten før den er offentliggjort (passivt samtykke). I tillegg har vi hatt telefonsamtaler med personer i Politidirektoratet, Kripos, Finansnæringens fellesorganisasjon og Sparebankforeningen, Forbrukerrådet, Teleselskaper, Banker, Veivesenet, Skattedirektoratet, Skattekontorer, Brønnøysund registrene og Kredittopplysningsbyråer.

Gjennom dokumentstudiene har vi samlet og drøftet tall som kan si noe om utbredelsen av identitetstyveri. Herunder representative offerstudier fra Norge og utlandet, og registerdata som kan si noe om mulighetsgrunnlaget (stjålne pass og bankkort) samt tall som kan antyde noe om utviklingen (rapporterte misseligheter). Vi har også søkt etter ulike måter å forstå fenomenet identitetstyveri, og funnet fram til illustrerende eksempler på tilfeller av identitetstyverier som viser kompleksiteten på feltet. Til slutt har vi gjennomført intervjuer med fem ofre for identitetstyverier. Deres historier er skrevet ned, og de har lest gjennom og godkjent historiene slik vi forteller dem i dette notatet.

Selv om vi vet at identitetstyveri forekommer i Norge, har vi få sikre data om omfanget. For å få et bilde av hvor stort omfang identitetstyveri har i Norge, kan man nærme seg feltet på to måter: i) Gjennom såkalte offerundersøkelser, der et representativt utvalg av befolkningen blir intervjuet om identitetstyveri, eller ii) gjennom eksisterende statistikk som kan belyse omfanget av identitetstyverier, som: stjålne bankkort (meldt til bank), telesvindel (meldt til teleoperatør), tyveri av dataregistre (meldt til politi), anmeldte tyverier av autentiserende dokumenter (pass, førerkort), samt annen statistikk som kan indikere noe om utbredelsen av identitetstyveri, for eksempel endringer i antallet som stenger mulighet for kredittvurdering-

[2] 'Skimming' viser til ID-tyveri basert på uautorisert kopiering av andres bankkort, for eksempel under uttak av penger fra minibank eller under betaling med kort i butikk.

er[3]. Begge tilnærmingene har svakheter. I dette notatet presenteres og vurderes først tallmateriale fra såkalte offerundersøkelser (fra Norge, Danmark, USA, Canada), deretter presenteres og vurderes tallmaterialer fra andre kilder.

[3] ID-tyven vil ofte prøve å opprette en fiktiv adresse på offeret, for at offeret ikke skal bli varslet av purringer og kredittvurderinger. Ny adresse er også nyttig dersom ID-tyven ønsker å motta varer på adressen.

2 Konkrete eksempler på identitetstyveri

Konsekvensene av identitetstyverier kan være svært forskjellige: Fra simpel kortsvindel som stort sett rammer bankene (hvis dette skal regnes som identitetstyveri), til svært alvorlig identitetssvindel som kan gå på livet løs. Kruize (2009:12) rapporterer om tilfeller fra England der borgere har blitt utsatt for *identitetskloning* (Meulen 2006) som har vært så gjennomgripende at offeret har vært tvunget til 'pseudoside', dvs. formelt erklære seg selv som avdød og få ny identitet (Stove & Valeur 2007: 37).

Særlig i de tilfellene der tyveriet ikke blir oppklart og gjerningsmann tatt, kan identitetstyveri være svært alvorlig. Det mest ubehagelige ved uoppklarte identitetstyverier er at identitetsmisbruket kan gjenoppstå om og om igjen, kanskje med års mellomrom. Vi skal heller ikke undervurdere det psykiske ubehaget og det tidkrevende økonomiske oppryddingsarbeidet ofrene for identitetstyveri påføres. Et offer for identitetstyveri blir sittende med bevisbyrden for at det ikke er de som har lånt penger, kjøpt varer eller begått kriminalitet.

I det følgende skal vi gi noen eksempler på ulike typer av identitetstyverier. Identitetstyveri kan være svært enkelt. Den enkleste form for identitetstyveri er misbruk av en annens lett tilgjengelige personopplysninger, som navn og adresse, ved bestilling av varer og tjenester:

En mann bestilte ved flere anledninger hotell i eget navn, men med en navnebrors adresse, og stakk av fra regningene. Navnebroren mottok dermed flere store hotellregninger med både restaurant- og barbesøk. Dette identitetstyveriet ble ganske raskt oppklart. (SIFO-intervju 2009)

Manipulering av adresser står sentralt i mange identitetstyverier fordi dette gjør at det tar lengre tid før offeret for identitetstyveriet blir klar over at hans eller hennes identitet misbrukes. Opprettelse av fiktive adresser gir også ID-tyven mulighet til å bestille og motta varer i en annens navn, og til å få tilgang på post med personopplysninger:

I et tilfelle ble ID-tyven avslørt etter å ha etablert ni forskjellige hotmail-adresser i navnene til personer fra sitt nabolag, for å kunne omadressere ofrenes post. Hensikten var å få tilgang på brev med ofrenes person- og konto-opplysninger, samt for bestilling av varer og tjenester i andres navn. (Arendt 2009)

Det er identitetsbevis (pass, sertifikat og bankkort m/bilde) på avveie som er den mest kritiske faktor i identitetstyveriet (Datatilsynet 2009:19). Stjålne identitetsbevis blir gjerne videresolgt til spesialister på ID-svindel. ID-tyven melder gjerne adresseendring for offeret før han tar opp kredittlån og kredittkjøp:

Så tidlig som i1995 opplevde en 1. amanuensis å bli utsatt for identitetstyveri etter husinnbrudd, der hans lommebok med blant annet sertifikat, bankkort og visittkort ble stålet. Tyven solgte identifikasjonspapirene videre til en rusavhengig med identitetstyveri som spesiale. Det første ID-tyven gjorde var å melde flytting for amanuensen, deretter kontaktet han Cresco og fikk kredittkort med kredittgrense 70.000 NoK. Kreditten ble tatt ut umiddelbart og

regningene sendt den fiktive adressen, slik at vår amanuensis ikke ble varslet om at noe var galt. Han hadde meldt innbrudd og tyveri til politiet og stengt sine bankkort, og kjente ikke til identitetstyveriet før han ble oppringt fra en våken ekspeditør hos Thorn utleiebyrå, som hadde reagert på en 'litt sliten' kunde som presenterte seg med amanuensens visittkort og skulle leie fullt utstyr til 'sin nye leilighet'. Ekspeditøren ringte altså den riktige amanuensen og sjekket historien, ringte deretter politiet og oppholdt ID-tyven med tegning av leiekontrakter, inntil politiet kom og tok ID-tyven på stedet. Cresco dekket tapet av kredittgjelden, men etterspillet for amanuensen innebar blant annet ubehaget ved å bli 'avslørt' som lite kreditverdig da han senere skulle betale en bedre restaurantmiddag med kreditkort. Amanuensen brukt mye tid på å få slettet kredittanmerkninger. (SIFO-intervju 2009)

Det kan ta lang tid før man oppdager at man er utsatt for identitetstyveri, og det kan være tilfeldigheter som gjør at det oppdages. Selv om økonomisk svindel ved identitetstyveri i siste instans i prinsippet skal ramme tredjepart - bankene og firmaene som er tappet – har offeret ofte store ubehag og belastninger knyttet til oppnøsting og opprydding i uføret for å gjenopprette både økonomisk- og lovlydig- troverdighet:

I 2002 ble en kvinne frastjålet vesken sin som lå i bilen mens hun leverte barn i barnehagen. I vesken lå både hennes og hennes manns bankkort. Innbruddet ble meldt og kortene sperret, men et stengt bankkort med bilde gjelder som identifikasjonsdokument og kan fortsatt utnyttes. Innbruddstyven solgte bankkortene videre til en ID-tyv, som blant annet opprettet diverse forbrukslån – med ektemannens bankkort som legitimasjon. Offeret for identitetstyveriet ble første gang oppmerksom på at hans identitet var på avveie da han ble oppringt av en hvitevare butikk, som kunne opplyse om at han hadde 14 av de opprinnelige 40 tusen kronene til gode på sitt forbrukslån. I tillegg til flere forbrukslån, opprettet ID-tyven femten mobilabonnementer på den stjålne identiteten. Kortet ble også brukt til å betale regninger i drosjer, restauranter og butikker uten betalingsterminal. Over en lang periode dumpet det stadig regninger etter ID-tyven i familiens postkasse. Mest ubehagelig var det å bli innkalt til politiet etter at ID-tyven hadde presentert og legitimert seg som offeret da han ble tatt for naskeri. Offeret er lettet over ikke å ha lidd økonomiske tap etter identitetstyveriet. Problemet har først og fremst vært knyttet til usikkerheten og ubehaget som følger med et identitetstyveri, med gjentagende forhold som må ryddes opp i. For eksempel tok det mye tid å få slettet alle kreditanmerkningene etter missligholdt kredit – og problemer når familien selv skulle låne penger fordi de har måttet stenge tilgangen på kredittopplysninger. Identitetstyveriet er ikke oppklart. (SIFO-intervju 2009)

Et identitetstyveri kan resultere i svært mange bedragerier og oppryddingsarbeidet kan være formidabelt:

En ung mann ble frastjålet lommebok med blant annet flere bankkort (med bilde) og sertifikat. Bankkortene, som ble sperret umiddelbart etter tyveriet, ble aldri brukt for å ta ut penger, men som legitimasjon ved opprettelse av kreditt, og som legitimasjon for å ta ut penger fra offerets sparekonto. ID-tyven opprettet til sammen syv kredittkort i offerets navn, to telekontoer og klarte fire ganger å ta ut penger på hans sparekonto. Offeret for identitetstyveriet har regnet ut at ID-tyven til sammen fikk ut penger og verdier for mer enn 500.000 kroner på disse - til sammen tretten - bedrageriene. Selv har han ikke lidd økonomisk tap. I hans tilfelle var det verste med å bli utsatt for identitetstyveri det tidkrevende, og ofte ubehagelige, administrative arbeidet – som aldri så ut til å ta slutt. Man blir ikke møtt med en serviceinnstilling når man ringer til en bedrift for å fortelle at de har blitt svindlet av en ID-tyv. For å slette den falske gjelden etter hvert enkelt bedrageri måtte han ringe utallige telefoner, sende kopi av politianmeldelsen og egenerklæring om at det ikke var han som hadde handlet eller tatt ut penger. Selv etter at sakene var løst og den falske gjelden slettet, kom det likevel ofte nye krav. Heller ikke banken klarte stoppe ID-tyven fra å ta ut penger fra offerets konto, som jo lykkes med dette flere ganger. Til sammen brukte han rundt regnet 80 oppstykkede timer, fordelt over flere år, på oppryddingsarbeidet.

I lommeboken lå også to konsertbilletter. Etter tapet av lommeboken fikk vår mann utstedt nye konsertbilletter, men ID-tyven var så frekk at enten han selv, eller noen han hadde gitt billettene, satt på hans plasser. Dette var før selve misbruket av hans identitet hadde startet, og han har i ettertid angret at han ikke gjorde anskrik, men tok til takke med at dørvakten ga ham nye plasser. (SIFO intervju 2010)

Selv om enkelttilfeller av identitetstyverier - slik det er beskrevet over - oppleves svært alvorlig for de som rammes, er det identitetstyveri i stor skala – masseidentitetstyveri – som er mest skremmende. Skremmende fordi de kan ramme hele samfunn i form av tapt tillit til sentrale institusjoner og tapt tillit til myndigheters evne til å forhindre kriminalitet. Tillit er selve limet i samfunnet (Elster 2000), og bare fantasien setter grenser for hvordan tapt tillit i befolkningen til myndigheter og finansielle systemer vil kunne påvirke samfunnet generelt og markedet spesielt. Det foregår allerede internasjonal ID-kriminalitet i stor skala:

Gjennom å rekruttere ansatte i en husbank i USA fikk en identitetstyveri-ring tilgang på låne-kundenes persondata med finansielle opplysninger. Informasjonen ble brukt til å forfalske sertifikater, som deretter ble brukt til å få kontroll med - og tømme - ofrenes kontoer, opprette kredittkontoer i ofrenes navn, samt bestilling av varer til store verdier. En atten måneders etterforskning ledet til at identitetstyveri-ringen ble avslørt og ring-lederen straffet. (Task Force Report 2008: 41)

Alvorligheten i slike registerdata tyverier er en kombinasjon av det store antallet potensielt nye identitetstyveriofre og den store uvissheten om hva som har skjedd – eller når det kan komme til å skje noe - med de solgte personopplysningene. Fordi selve svindelen kan komme år etter at tyveriet av personopplysningene fant sted, er det vanskelig å kalkulere hvor mange som er rammet:

Tidenes største nettbaserte identitetstyveri – utført av en internasjonal 'retail hacking ring' ledet av en tidligere regjeringsrådgiver på kredittkortsvindel(!) – ble avslørt i USA i januar 2008. I august ble de 11 medlemmene tiltalt for å ha stjålet rund 100 millioner dollar og distribuert rundt 40 millioner kredit- og debetkortnumre fra amerikanske dagligvarekjeder gjennom å bryte seg inn ('hacking' med installering av 'malware') i nettbetalingssystemene til Heartland Payment Systems. Dette antas å være tidenes største identitetstyveri, med saksøkte fra USA, Estonia, Ukraina, China og Hviterussland. Aktørene antas å ha truffet hverandre på internett. (Task Force Report 2008: 38)

Også nordmenn kan være rammet av masseidentitetstyveri:

I oktober 2009 ble det oppdaget datainnbrudd som rammet Visa- og Mastercard-systemene i Spania. Tusenvis, kanskje flere hundre tusen, konto- og personopplysninger er på avveie. Norske banker ble også varslet om at norske turister i Spania kunne være blant ofrene. I dette tilfellet fikk norske banker lister over kunder som eventuelt kan være berørt av svindelen. De norske bankene skal da sette i gang en kombinasjon av sperring av kort og overvåking. Anders Bigseth i Teller (tidligere Visa Norge AS) sier at i slike saker vil kortbrukerne normalt få dekket sine tap, og at oppgjøret vil stå mellom kortutsteder og eventuelt stedet der svindelen har skjedd. (Knudsen 2009)

Tredjepart – den som normalt blir økonomisk skadelidende etter et identitetstyveri – kan også være sentrale offentlige institusjoner: Masseidentitetstyveri av personopplysninger har vært benyttet til å tappe USA's helseressurser. Den stjålne identiteten rammer da, i hvert fall i første omgang, kun tredjepart:

Gjennom stjålne pasientlister med navn, adresser, SSN (Social Security Number) og pasient-opplysninger, samt ved å opprette fiktive apoteker en rekke steder i USA, klarte ID-tyver å svindle til seg milliarder av dollars gjennom fiktive salg – med påfølgende refusjoner fra Me-

dicare. ID-tyvene meldte fiktive salg av alt fra medisiner til proteser og rullestoler, som de deretter fikk refundert. Langt fra alle, men noen, meldte fra til Medicare om at de verken trenger, har søkt om eller fått nevnte nye protese eller rullestol. Men innen personene bak de 'falske trengende' får tid til å reagere er apotekene for lengst forsvunnet. Økonomisk rammer svindelen staten, dvs. amerikanske skattebetalere. Grunnen til at svindelen er mulig er manglende kontrollrutiner – fordi, som de ansvarlige forsvarer seg med; kontroll er ressurskrevende og dyrt. (CBS News: 60 minutes 2009)

Identitetstyveri behøver ikke være motivert av økonomisk vinning. Mangler ved offentlig helsevesen i USA har bidratt til identitetstyverier. Mange slike identitetstyverier skjer innen den nærmeste familie og nære omgangskrets:

En kvinne i USA ble kjent skyldig i identitetstyveri etter at hun hadde tatt kopi av en familievenns Social Security card, for å bruke dette til medisinsk behandling. Hun ble idømt erstatningsansvar og fengselstraff (Task Force Report 2008: 42).

Også fra Norge har vi eksempler på identitetstyveri motivert av sosial nød:

Et par, som tidligere var fratatt tre barn, tok en annen kvinnes identitet for bruk i graviditetskontroll for ikke å bli fratatt sitt fjerde barn. De hadde tilegnet seg kvinnens fødsel- og personnummer etter et bilkjøp – og skiftet kvinnens fastlege på nettet. Imidlertid ble de likevel avslørt etter at fornærmede ble innkalt til ultralydundersøkelse pr. post. (Gustad 2009)

Ressurssenter for identitetstyveriutsatte (ITRC 2008:28) har rettet spesiell oppmerksomhet mot identitetstyveri fra barn i USA. I sin studie finner de flere tilfeller av barn som har fått sin identitet misbrukt fra før fylte ett år. Det er ofte belastede foreldre eller steforeldre som står bak identitetstyverier fra barn. Og slike tyverier blir sjeldent oppdaget før barnet fyller 18 år:

En sytten år gammel gutt ble sjokkert da han verken fikk studielån eller jobb pga svært alvorlige kredittanmerkninger. Verken hans mor eller han selv hadde vært klar over at noen hadde brukt hans persondata (SSN) til å kjøpe en husbåt for 40.000$ da gutten bare var syv år gammel. Lånet ble aldri tilbakebetalt, og guttens kreditverdighet hadde vært ødelagt de siste ti årene uten at gutten visste om dette. Etter møysommelig oppryddingsarbeid ble gutten renvasket for mistanke. Man fant aldri ut hvem som hadde misbrukt guttens personalia – det kunne vært hvem som helst med tilgang på hans personopplysninger ved skoler, helsestasjoner, tannlege m.m. (SpendOnLife 2009)

Identitetstyveri behøver ikke ramme økonomisk, men kan være alvorlig for det, særlig når det rammer barn. Personopplysninger som blir misbrukt for å skade en annens omdømme – for eksempel gjennom å konstruere Facebook-profiler på bakgrunn av ulovlig bruk av en annens bilde og personopplysninger – regnes også som identitetstyveri:

En tolv år gammel gutt hadde besøk av en klassekamerat. Sammen gikk de inn på internett og Facebook uten at gutten tenkte over at han skulle skjule innloggingskoden på PC'en eller facebook-siden sin. En dag han kom på skolen ble han møtt av medelever som var sinte, sårede og fornærmede etter å ha mottatt ekle meldinger fra ham på Facebook. Sammen med sin mor gikk han deretter inn på Facebook hvor de finner at noen har lagt ut stygge kommentarer og sendt ekle hurtigmeldinger i hans navn. Forholdet ble straks meldt til politiet, som tok saken alvorlig. Ved hjelp av avsenders IP-adresse fant politiet fram til den tidligere kameraten. Det viste seg at gutten også hadde merket seg alarmkoden i fornærmedes hjem, han hadde vært i vesken til moren og tatt skriftlig kopi av bankkort opplysninger m.m. Selv om forholdet ble oppklart og konfliktrådet koblet inn, måtte gutten som fikk misbrukt sin identitet bytte skole. (SIFO intervju 2009)

Dette notatet skal kun omhandle identitetstyveri som går ut over fysiske personer og ikke juridiske personer (bedrifter, institusjoner). Likevel, som en indikasjon på hvor vanskelig det kan være å rydde opp etter identitetstyveri, siterer vi fra den falske nettstedet 'Kripos offisielle hjemmeside' (www.uncletaz.com/norsktaz/kripos, nedlastet januar 2010). Her kan vi blant annet lese:

"Uten kriminalitet i samfunnet ville ikke Kripos ha noen funksjon, og vi ville alle bli arbeidsledige. Men for at Kripos skal ha en funksjon, må etaten bekjempe kriminaliteten, og dermed paradoksalt nok arbeide for sine egne oppsigelser. Denne problematikken har blitt forsøkt løst ved at man henlegger eller ignorerer visse alvorlige saker, slik at kriminaliteten kan blomstre nok til å skaffe Kripos bevilgninger for neste valgår. Det er som når brannfolk tenner skogbranner for at naturen skal holdes i balanse. Av samme grunn hender det at politiet selv begår visse straffbare handlinger, for balansens skyld." (Uncletaz.com 2009)

Dette illustrerer at selv Kripos har problemer med å få slettet falske nettsteder som kan skade deres omdømme.

3 Hvordan er identitetstyveriet forstått, definert og operasjonalisert?

I følge straffeloven kan identitetstyveri ramme både fysiske personer, juridiske personer (bedrifter), samt nasjoner. I dette notatet fokuseres identitetstyveri som rammer personer. Men det er ikke bare den som blir frastjålet sin identitet som blir skadelidende ved et identitetstyveri fra fysiske personer. Som regel vil bankene være ansvarlige for å erstatte en kundes tap ved kortsvindel/opprettelse av kreditt på stjålen identitet. Bedrifter blir økonomisk rammet gjennom at den som har blitt frastjålet sin identitet ikke kan faktureres for varer sendt til ID-tyvens fiktive adresse. I siste instans vil samfunnet rammes gjennom tapt tillit til systemets evne til å forhindre misbruk av forbrukernes og borgernes identiteter. Omdømmet til politi, bank og rettsvesen vil kunne avhenge av hvordan disse institusjonene forholder seg til identitetstyveri som fenomen.

Identitetstyveri er et komplekst fenomen og vanskelig å avgrense. Det er ikke enighet rundt hvordan identitetstyveri skal defineres eller forstås (McNally & Newman 2008). Selve begrepet er også kritisert, da det påpekes at offeret slett ikke *mister* sin identitet etter et identitetstyveri, slik det er vanlig med andre tyverier. Identiteten blir snarere kopiert og misbrukt.

De fleste enes om at identitetstyveri handler om uautorisert tilegning av andres personopplysninger og/eller identifikasjonspapirer med hensikt om å misbruke disse. Men der slutter enigheten. Noen ser ut til å reservere identitetstyveri for vinningsforbrytelser, mens for eksempel *Identitetstyveriprosjektet* i Norge også inkluderer det å skade en annens omdømme (NorSIS 2009).

Det er også uenighet om tradisjonell kortsvindel skal inkluderes i begrepet eller ikke. Sproule & Archer (2009) mener simpel kortsvindel ikke skal regnes som identitetstyveri, fordi konsekvensene for de som rammes er så små. Det er knyttet direkte og indirekte kostnader til kortsvindel for enkeltpersoner gjennom egenandel og krav til redegjørelse for sikker forvaltning av pinkoder, men så lenge det ikke er utvist uaktsomhet ved bruk og oppbevaring av kort og kode, er omkostningene relativt små. Økonomiske tap belastes i all hovedsak bankene. Konsekvensene er gjerne langt større der den stjålne identiteten blir brukt til å opprette ny kreditt. I slike tilfeller får ofrene en stor jobb i fanget i tillegg til mulige direkte økonomiske tap. Grunnen til at kredittkortsvindel ikke oppleves like alvorlig blant de som rammes, skyldes ganske sikkert at finansnæringen her er 'føre var' og har systemer som tross alt stopper svindelen raskt gjennom at kontoer effektivt stenges og kortene blir ugyldige. Og aller viktigst: det er systemer som effektivt avslører bruk av kort som ikke er gyldige. (I motsetning til illegitim bruk av bortkomne norske pass og sertifikater).

Konstruksjon av *fiktive* identiteter, som bruk av forfalskede pass (Haakaas, Aftenposten 18.01.2009[4]) eller sertifikater, blir ikke regnet som identitetstyveri, ganske enkelt fordi det ikke er noen fysisk person som har blitt frastjålet sin identitet. .

[4] Bare på Gardermoen blir det årlig tatt 150 personer med falske pass. På verdensbasis er 20 millioner pass meldt stjålet. I tillegg er produksjon av falske pass storindustri i land som Thailand, Ukraina og Tyrkia. I Vest-Europa er

Noen vil si at identitetstyveri er en totrinnsprosess; først tilegning av personopplysninger og/eller identitetsdokumenter, dernest selve misbruket, skaden, eller svindelen. Andre vil si at første trinn er identitetstyveri, mens andre trinn er identitetssvindel (Javelin Strategy & Research 2008, 2009). Når omfang av identitetstyveri/identitetssvindel skal estimeres, tas det ofte utgangspunkt i ofrene, og ofrene er naturlig nok ikke klar over at de har vært utsatt for identitetstyveri før andre trinn, dvs. før selve misbruket har skjedd, og de er blitt gjort oppmerksomme på dette (Datatilsynet 2009:8).

3.1 Ulike definisjoner av identitetstyveri

Vi vil kort også presentere hvordan begrepet er definert og forstått i OECD, samt av sentrale aktører i Danmark og USA, før vi ser på hvordan den norske straffeloven omtaler Identitetskrenkelse, og til slutt Datatilsynets og NorSIS' definisjon. Først OECD, som har valgt følgende definisjon:

"ID theft occurs when a party acquires, transfers, possesses, or uses personal information of a natural or legal person in an unauthorized manner, with the intent to commit, or in connection with, fraud or other crimes." (OECD 2009:16).

I OECDs definisjon regnes det som identitetstyveri hvis man tilegner seg andres personopplysninger på en uautorisert måte med hensikt om å begå svindel, eller i forbindelse med svindel eller andre ulovligheter. I OECD's definisjon inkluderes altså både tilegnelsen av personopplysningene og svindel/ulovligheter inn under identitetstyveri.

Kruize (2009) bygger på Det danske rådet for IT-sikkerhet og definerer identitetstyveri slik:

"Identitetstyveri skjer, når personer tilegner sig andres personoplysninger og udgiver sig for at være disse personer. Det kan skje elektronisk ved brug af bankoplysninger, cpr-numre eller kodeord eller ved at bruge den andens identitetspapirer (sygsikringsbevis, kørekort, m.m). Det er også tale om identitetstyveri, når en person køber produkter, fx over internettet, ved hjælp af en andens person- og kontooplysninger." Kruize (2009:6)

Kruize påpeker at denne definisjonen på identitetstyveri viser til to trinn; i) tilegning av en annens personopplysning, og ii) å utgi seg for å være denne personen ved kjøp av produkter. Implisitt inkluderer han selve svindelen i definisjonen.

Federal Trade Commission (FTC) har siden 1997 årlig produsert *Consumer Complaint Report,* som også omfatter antall klager/rapporteringer av identitetstyverier i USA (Federal Trade Commission 2009). De benytter denne definisjonen av begrepet:

"Identity theft occurs when someone uses your personally identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes"(Federal Trade Commission 2010)

Det amerikanske analysebyrået Javelin Strategy & Research har gjennomført årlige kvantitative studier på temaet siden 2003. I motsetning til FTC, OECD og den danske definisjonen, skiller Javelin Strategy & Research mellom identitetstyveri (Identity Theft) og identitetsvindel (Identity Fraud). Mens identitetstyveri i følge Javelin Strategy & Research omhandler

---

det oppdaget slik produksjon i Frankrike, Storbritannia og Spania i fjor, sier Kripos leder Roll-Matthiesen til Aftenposten (Haakaas 2009).

ethvert tyveri av personopplysninger, begrenses identitetsvindel til tilfeller der stjålne personopplysningene blir brukt til økonomisk vinning.

"Identity theft: the unauthorized access to personal information. Identity theft can occure without fraud. For example, it can occur with large scale data breaches.

Identity fraud: The unauthorized use of some portion of another's personal information to achieve illicit financial gain. Identity fraud can occur without identity theft. For example, it can occur with relatives who are given access to personal information or by the use of randomly generated payment card numbers." (Kim 2008:16)

Både i Datatilsynets rapport om Identitetstyveri (2009)[5] og i det norske ID-tyveriprosjektet (NorSIS 2009) skilles det mellom tyveri og svindel:

"Identitetstyveri: *Innsamling, besittelse, overføring, reproduksjon eller annen manipulering av en annen persons personlige informasjon med den hensikt å skade andres omdømme, begå svindel eller annen kriminell handling.*

Identitetssvindel: Ervervelse av penger, varer tjenester, og andre fordeler eller unngåelse av forpliktelser gjennom bruk av falsk identitet." (Datatilsynet 2009:19) Datatilsynets og NorSIS' definisjon av identitetstyveri er i overensstemmelse med straffeloven § 202 om *Identitetskrenkelse* der det heter*:*

Med bot eller fengsel inntil 2 år straffes den
som uberettiget setter seg i besittelse av en annens
identitetsbevis, eller opptrer med en annens identitet
eller med en identitet som er lett å forveksle
med en annens identitet, med forsett om å
a) oppnå en uberettiget vinning for seg eller en annen,
eller
b) påføre en annen tap eller ulempe.

I straffeloven om Identitetskrenkelse skal det foreligge et *forsett* om svindel, men selve svindelen eller skaden forårsaket av identitetstyveriet, holdes utenfor.

3.2 Vår operasjonalisering

Datatilsynet og NorSIS skiller mellom identitetstyveri og identitetssvindel i sin definisjon. Imidlertid, i forsøkene på å beregne omfanget av fenomenet identitetstyveri, er det først og fremst det å få misbrukt sine personopplysninger i forbindelse med svindel som er gjenstand for kvantifisering. Også i dagligtalen dekker 'identitetstyveri' hele prosessen, det vil si den uautorisert tilegning av persondata og selve misbruket. Vi velger derfor å bruke begrepet identitetstyveri om både trinn I og trinn II. Med andre ord legger vi oss nærmere opp mot OECDs og Danmarks definisjon. I Tabell 1 skisseres hva vi legger i identitetstyveri:

[5] Det påpekes i fotnote at definisjonen ikke er enstemmig vedtatt av identitetstyveriprosjektgruppa

Tabell 1: Identitetstyveri trinn I og trinn II.

Prosessen:	Personopplysninger på avveie: Registerdata	Navn, adresse, personnummer, selvangivelse	Fiktive person-opplysninger	Pass førerkort koder	Bankkort	
Uautorisert tilegning	ID-tyveri Trinn I	ID-tyveri Trinn I	Prod. ID-papirer Forfalskning	ID-tyveri trinn I	ID-tyveri trinn I	
Misbruk & svindel	ID-tyveri Trinn II	ID-tyveri Trinn II	Svindel	ID-tyveri trinn II	Idtyv trinnII	Kort-svindel

Det vi regner inn under identitetstyveri er i tabell1 markert med grønt. Vi skiller mellom trinn I; uautorisert tilegning av andres persondata, og trinn II; misbruk av andres persondata for vinningskriminalitet eller for å skade andres omdømme. Videre skiller vi mellom fem typer av personopplysninger.

I følge Finanstilsynet og de store talls lov er det tyveri av registerdata – masseidentitetstyveri - som i dag utgjør den største trusselen. Med registerdata menes her personidentifiserbare registre, fra kunderegistre til bankenes registre over finansielle transaksjoner. I slike tilfeller – f. eks. det rapporterte tilfellet med tapping av personopplysninger fra rundt 100.000 bankkort i Spania 2009 – er ofrene ofte ikke klar over at deres personopplysninger er på avveie. Lister med slike personopplysninger kan selges videre, gjerne oppstykket og over lang tid, og trinn II – selve misbruket og svindelen - kan utføres lenge etter at trinn I-hendelsen skjedde.

I tabell 1 har vi også skilt mellom identifiserende og autentiserende personopplysninger. Både *identifiserende* personopplysninger (navn, adresse, fødsel- og personnummer) og *autentiserende* dokumenter som bekrefter identitet er viktige ingredienser i identitetstyveri. De viktigste autentiserende dokumenter i Norge er pass og førerkort. Norsk pass og førerkort inneholder både bilde, navn, fødsel og personnummer. Med andre ord gir de tilgang på både de viktigste identifiserende personopplysningene, samtidig som de er autentiserende. Det samme gjelder bankkort med bilde. I tillegg til autentiserende dokumenter har vi autentiserende koder som passord til bankkort (BankID) og passord for å komme inn på forskjellige nettsteder; herunder personlig nettbutikk-konto og egne nettsider som Facebook. Personlige koder som gir adgang til lokaler og bygninger kan også regnes som autentiserende koder.

Den som har tilgang på både identifiserende og autentiserende dokumenter, kan gjennomføre økonomiske transaksjoner i en annens navn. Ved å få tilgang på en annens pass eller førerkort kan ID-tyven opprette kontoer med fiktive adresser, og slik tappe offeret for penger. For eksempel gjennom å oppta lån i den andres navn, eller ved kjøp av varer og tjenester som sendes til en fiktiv adresse.

På den ene siden, som det illustreres i tabell 1, fjerde kolonne, kan stjålne pass og førerkort også misbrukes til forfalskninger med fiktive persondata og faller da utenfor vår avgrensning. På den andre siden kan identitetstyven som har identifiserende personopplysninger (navn, adresse, personnummer, inntekt og formue), kjøpe falske autentiserende dokumenter til bruk i identitetstyveriet.

Det er uenighet om stjålne bankkort skal regnes som identitetstyveri. Fordi bankkort med bilde regnes som autentiserende legitimasjonsdokument i Norge er det uproblematisk å regne tyveri av bankkort som identitetstyveri trinn I. Men på trinn II er det, som illustrert i tabell 1, likevel hensiktsmessig å skille mellom simpel kortsvindel og tilfeller der stjålne (stengte) kort blir ytterligere misbrukt som identifikasjonsbevis knyttet til nye kjøp. Som det vil framgå av neste kapittel er det vanlig å skille ut simpel kortsvindel i offerstatistikken.

4 Omfanget av identitetstyverier basert på offerstudier

TNS-Gallup har på oppdrag fra NorSIS undersøkt omfanget av identitetstyveri i Norge 2009 i aldersgruppene 15 - 90 år. Gjennom telefonintervjuer (CATI) ble til sammen 1000 landsrepresentative respondenter spurt om de hadde vært utsatt for identitetstyveri. Spørsmålet de ble stilt var:

Identitetstyveri og identitetssvindel er misbruk av din identitet. Dette kan være alt fra å oppgi andres identitet for å slippe bot for sniking på trikken til opprettelse av ulike abonnement og grov svindel med store beløp. Har du blitt utsatt for noen form for identitetstyveri noen gang?

Basert på dette spørsmålet var det omtrent én av tyve, eller 5 prosent, som svarte bekreftende på at de en eller annen gang har vært utsatt for identitetstyveri.

Når vi sammenligner offertall, er det viktig å skille mellom studier som kartlegger omfanget siste tolv måneder, i forhold til om man har vært utsatt en eller annen gang i ubestemt fortid. I tillegg gir det store utslag om simpel kortsvindel er med i beregningene eller ikke.

4.1 USA

På vegne av Handelskommisjonen i USA (Federal Trade Commision) samler og administrer Consumer Senteniel Network hvert år en form for kriminalitetsstatistikk basert på innklagde forbrukerklager til et nasjonalt register. Hvis vi ser på antall forbrukerklagesaker knyttet til identitetstyveri, får vi inntrykk av at det har vært en sterk økning i antall bedragerier siden år 2000. I år 2000 mottok Consumer Senteniel Network 31.100 meldinger om bedragerier knyttet til identitetstyveri, i 2004 var antallet steget til 247.000 og i 2008 til 314.000 (Federal Trade Commision 2009:5). Klagesakene er imidlertid verken verifiserte eller basert på representative surveyer. Økningen kan dermed i prinsippet skyldes større oppmerksomhet om fenomenet og at flere bedragerier blir rapportert inn.

I en representativ studie finner Javelin Strategy & Reseach (Monahan & Kim 2009)[6] at så mange som hver tiende amerikaner (487 av 4.800) en eller annen gang har vært utsatt for identitetstyveri (tall fra 2008). Respondentene besvarte spørsmålet:

Has anyone ever misused any of your own existing accounts such as a credit or debit card, bank or utility account, or used your own personal information to create unauthorized new accounts or commit a crime in your name? Og: What is the approximate value of what the person obtained while misusing your information?

[6] Vi baserer oss her på en oppsummerende nett-versjon: www.javelinstrategy.com. Hele rapporten koster 3000 $.

Javelin Strategy & Research har overvåket utbredelsen av identitetstyveri (de bruker benevnelsen Identity Fraud) siden 2002. De har også informasjon om identitetstyveri siste tolv måneder, slik at utviklingen kan sammenlignes over tid[7]:

Tabell 2: Andeler i USA som har vært utsatt for identitetstyveri siste tolv måneder fra 2002 – 2008. Prosent. (N basert på ca. 5000 telefonintervjuer pr. år)

	2002	2004	2005	2006	2007	2008
ID-svindlet siste 12 måneder	4,70%	4,25%	4,00%	3,74%	3,58%	4,32%
Gj.sn. svindel beløp pr. offer	5.503$	$6.203	$6.497	$5.920	$5.574	$
Median svindel beløp	$750	$750	$750	$750	$750	$
Gj.sn. økonomisk tap pr. offer	$582	$711	$446	$554	$691	$500*
Median økonomisk tap	0	0	0	0	0	
Gj.sn. tidstap pr. Offer	33t	28t	40t	25t	26t	
Median tidstap	5t	5t	5t	5t	5t	

Kilde: Javelin Strategy & Research 2009 Identity Fraud Survey Report:
Syndicated Report Brochure/2008 Identity Fraud Survey Report:5. *=tall funnet på nettet www.spendonlife.com/guide/identity-theft-statistics

I 2007 var det 3,6 prosent og i 2008 var det 4,3 prosent som oppga at de hadde vært utsatt for identitetstyveri *i løpet av de siste tolv månedene*. Hovedbudskapet I 2007 var:'*Identity Fraud Continues to Decline, But Criminals More Effective at Using All Channels'*. Hovedbudskapet i 2008 var: '*Identity Fraud on the Rise, But consumer Costs Plummet as Protection Increase*.' (Identity Fraud Survey Report 2008, Identity Fraud Survey Report 2009). I følge Javelins' direktør James Van Dyke er det finanskrisen som ligger bak økningen i antall rammede.

Hvis vi tar hensyn til utvalgenes størrelser og feilmarginer[8], er det kanskje likevel riktigere å beskrive situasjonen som relativt stabil.

Javelin Strategy & Resarch (referert SpendOnLife 2009) har også spurt ofrene og hvordan deres persondata ble stjålet:

- 43 prosent har blitt frastjålet personopplysninger gjennom tyveri av lommebok
- 11 prosent har blitt frastjålet personopplysninger på nettet

I følge ofrene av 2008 er det altså stjålet lommebok som oftest var opphav til identitetstyveriet, mens det å bli frastjålet personopplysninger på nettet forekommer langt sjeldnere. Det er viktig å merke seg at mange ikke vet hvordan ID-tyvene har fått fatt i deres persondata. Opplysningene fra Javelin Strategy & Research (referert SpendOnLife 2009) viste videre at:

- 38 prosent har blitt frastjålet kredit- eller debetkort.
- 37 prosent har blitt frastjålet sitt Social Security Number (SSN)
- 36 prosent har fått misbrukt sitt navn og telefonnummer

En som har vært utsatt for identitetstyveri har ofte vært rammet på flere måter. En person som er rammet på flere områder blir i statistikken kategorisert for groveste metode, der opprettelse av nye kontoer regnes som mer alvorlig enn kortsvindel basert på eksisterende kort.
I sin kategorisering av identitetsvindel skiller Javelin Strategy (Kim & Monahan 2008: 53) mellom:

[7] 2008-data er innsamlet av Discovery Research group. De foregående årene er data innsamlet av Synovate, men Javelin valgte å skifte byrå fordi Synovate gikk fra et utvalg basert på RDD (random digit dialing) over til panel utvalg (remunerated opt-in panel).
[8] I et utvalg på 5000 personer, med prosentfordeling tilnærmet 5/95 er feilmarginen +/- 0,6% (95%-konfidens intervall). I et utvalg på 500 identitetstyveri utsatte, med prosentfordeling 50/50 er feilmarginen +/- 4,5% (95%-konfidens intervall).

i) Existing Card Accounts: Svindel av både eksisterende kreditt- og debet-kort.
ii) Existing Non-Card Accounts: Svindel av eksisterende sparekontoer, lån, forsikring, telefon og brukskontoer.
iii) New Accounts and Other Frauds: Nyopprettede kontoer eller lån, eller annen kriminalitet, ved bruk av ofrenes personopplysninger.

I følge Kim & Monahan i Javelin Strategy (2008) rammer de mest alvorlige tilfellene - der det opprettes nye kontoer i ofrenes navn – årlig rundt én prosent av den voksne befolkningen i USA. Svindel av eksisterende kreditt- og debet kort – omfatter årlig rundt to prosent av den voksne befolkningen, mens litt over en halv prosent utsettes for svindel av andre eksisterende kontoer:

Tabell 3: Svindel gjennom: opprettelse av nye kontoer, eksisterende ikke-kort kontoer og eksisterende bankkort i USA. Tall innsamlet 2007 (N=5075/ca.400)

	Det skilles mellom tre identitetstyverityper:		
	Opprettelse av nye kontoer	Misbruk av eksisterende ikke-kort-kontoer	Misbruk av eksisterende bankkort
Prosentandel svindlet siste 12 mnd.	0,95%	0,65%	1,97%
Gj.sn. svindel beløp pr. offer	$8.071	$9.848	$4.885
Median svindel beløp	$3.000	$3.000	$750
Gj.sn. økonomisk tap pr. offer	$1.066	$1.646	$632
Median økonomisk tap	$0	$0	$0
Gj.sn. tidstap pr. Offer	49timer	46timer	23timer
Median tidstap	25timer	25timer	5timer

Kilde: Javelin Strategy & Research 2008 Identity Fraud Survey Report.

Grovt regnet halvparten (1,97% mot (0,95 + 0,65)%) av identitetstyveritilfellene i USA er simpel kortsvindel (misbruk av eksisterende bankkort). Målt gjennom svindelbeløp, ofrenes økonomiske tap og tidstap, viser også tabell 3 at svindel av eksisterende bankkort er mindre alvorlig enn identitetstyveri som omfatter opprettelse av nye kontoer og/eller tapping av andre eksisterende kontoer. Uansett om vi sammenligner gjennomsnitt eller medianen, er tidstapet langt mindre for de som utsettes for simpel kortsvindel, enn for de to andre gruppene. Svindelbeløpet er også lavere. Til slutt viser tabell 3 at medianen – det økonomiske tapet til den midterste respondenten ordnet etter størrelsen på tapet - er lik null for alle tre kategorier. Det er rimelig å anta at noen svært få personer (på intervjutidspunktet) har tapt svært mye penger, mens de fleste er økonomisk skadefrie.

4.2 Canada

Sproule & Archer (2008) har i en studie basert på panelutvalg med 3018 respondenter undersøkt utbredelsen av identitetstyveri i Canada. De finner at 6,5 prosent har vært utsatt for identitetstyveri i løpet av det siste året, hvorav halvparten er kortsvindel. Over halvparten visste ikke hvordan deres personopplysninger var kommet på avveie. De oppgir også at bare syv prosent, mot tidligere 25 prosent, av identitetstyveriene var utført av familiemedlemmer eller bekjente.

Hver tredje forbruker i Canada oppgir at de har blitt mer bekymret for identitetstyveri enn de var tidligere. Sproule & Archer (2008) finner imidlertid at dette *ikke* gjelder de som kun har vært utsatt for kortsvindel. Tvert imot er disse mindre bekymret enn andre. I følge Sproule & Archer (2008) skyldes dette at kredittkortsvindel – i motsetning til annen ID-svindel - løses enkelt og rutinert og har små omkostninger for de som er rammet. De mener dette funnet innebærer at kortsvindel og ID-svindel bør kategoriseres og diskuteres separat.

4.3 Danmark

Justisministeriet i Danmark har også stilt spørsmål om identitetstyveri i sin Offerundersøkelse. Til sammen 1853 landsrepresentative danske respondenter i alderen 16 – 74 år har i løpet av henholdsvis mars og juni 2009 besvart spørsmål om identitetstyveri i telefonintervjuer:

Har du inden for de seneste 12 måneder været udsat for misbrug af personoplysninger eller identitetsbeviser?

Tyve personer, eller bare rundt én prosent, svarte bekreftende. Av disse (20) var flesteparten utsatt for misbruk av sitt Dankort (9) eller kredittkort (5). (Kruize 2009:18-19). Respondentene ble også spurt om hvordan ID-tyven hadde fått tilgang på deres personopplysninger. Syv av de tyve hadde blitt frastjålet personopplysninger på nettet, ti var frastjålet personopplysninger på annen måte, og bare fire respondenter visste ikke hvordan personopplysningene var kommet på avveie. (Kruize 2009:20)

4.4 Norge

Det norske materialet, bestilt av NorSIS og innsamlet av TNS Gallup, gjør det mulig å belyse hvem som kan være mest utsatt for identitetstyveri i Norge. Tallene er basert på spørsmålet: *Har du blitt utsatt for noen form for identitetstyveri noen gang?* De bekreftende svarene omfatter høyst sannsynlig også kortsvindel.

Tabell 4: Hvem er mest utsatt for identitetstyveri i Norge? Prosent[9]. (N=989)

Kategori (andel av alle)	Utsatt for identitetstyveri
Alle (100%)	5,4
Kvinner (52%)	5,6
Menn (48%)	5.1
15-29 år (16%)	8,4**
30-44år (24%)	8,6**
45-59år (29%)	4,2**
60- 90år (32%)	2,5**
Gift Samboer (63%)	5,3
Enslig/mambo (37%)	5,5
Ikke i jobb (41%)	4,2
Yrkesaktiv ansatt (54%)	6,2
Selvstendig næringsdrivende (6%)	5,4
Lavere utdanning (51%)	4,5
Høyere utdanning (49%)	6,2
StorOslo (27%)	6,7
Østlandet ellers (25%)	4,8
Sør/Vestlandet (28%)	3,5
Trøndelag/NordNorge	6,8
Bykommune (48%)	6,6
Landkommune (52%)	4,3
Inntekt under 150.000 (16%)	4,8
Inntekt 150-299 (18%)	7,2
Inntekt 300-399 (19%)	3,7
Inntekt 400+ (39%)	6,3

Kilde: NorSIS ** = Sig. P>.01

[9] I et utvalg på 1000 personer med ca. 5/95 prosent fordeling er feilmarginen +/- 1,4%

Etter måten spørsmålet er stilt i Norge, skulle man anta at eldre personer hadde vært oftere utsatt enn yngre (som har kortere tid de har vært eksponert for tyveri). Det er derfor kanskje uventet at det faktisk er de to eldste aldersgruppene som sjeldnest har vært utsatt for identitetstyveri. Det er kun alder som slår ut signifikant. Et større utvalg ville sannsynligvis gitt flere signifikante utslag. Vi kan reise spørsmål om det er slik at de som bor i byer er mer utsatt enn de som bor på landet? Er de fra storbyer mer utsatt enn andre? Er kvinner mer utsatt enn menn? Er de med høyere utdanning mer utsatt enn de uten høyere utdanning – også hvis vi kontrollerer for alder?

4.5 Sammenlignende statistikk

Forskjeller mellom land i utbredelsen av identitetstyveri kan skyldes landenes ulike rammebetingelser. Men omfanget av identitetstyveri avhenger naturligvis også av hva vi teller. I neste tabell har vi sammenstilt utbredelsen av identitetstyveri slik det er målt i Norge, Danmark, Canada og USA. Hensikten med tabellen er å vise hvor viktig det er å skille mellom ulike tidshorisonter og hvorvidt man – ut fra spørsmålsstillingen - kan anta om simpel kortsvindel er inkludert i estimatene eller ikke:

Tabell 5: Estimert omfang av identitetstyveri/svindel i Norge, Danmark, Canada og USA, basert på ulike operasjonaliseringer av begrepet:

	Norge 2009 (N=1000)	Danmark 2009 (N=1853)	Canada 2008 (N=3018)	USA 2007 (N=4800)
Noen gang utsatt for identitetstyveri	5,4%			10%
Utsatt for identitetstyveri siste 12 mnd.		1%	6,5%	3,5%*
Utsatt siste 12 mnd, unntatt kortsvindel		(0,3%)	3,2%	1,6%

*økt til 4,2% i 2008.

Tabell 5 viser tre ulike måter å avgrense og måle fenomenet identitetstyveri på. Det er kun fra USA vi har estimater for alle de tre avgrensningsmåtene. Det norske estimatet i tabell 5 er ikke tidsavgrenset, og det er sannsynlig at kortsvindel er regnet med av respondentene. Dersom vi – rent hypotetisk - forutsetter at forholdstallet mellom kategoriene i Norge tilsvarer forholdstallet mellom kategoriene i USA, vil det være 5,4/(10/1,6)= 0,9 prosent som er ofre for identitetstyverier (unntatt kortsvindel) årlig i Norge[10]. Dette tilsvarer grovt regnet (0,9 * 3,5 millioner i alderen 18-80) mer enn tretti tusen årlige tilfeller i denne aldersgruppen. Dette tallet er imidlertid rent hypotetisk, og for å få troverdige tall er det nødvendig med en mer robust og detaljert kartlegging.

4.6 Følgene av å få misbrukt sin identitet

The Identity Theft Resource Center (ITRC) i USA gjennomfører årlig en studie blant ofre for identitetstyveri. Utvalget er selvselektert og dermed ikke representativt. I *Identity Theft: The Aftermath 2008* kommer de 100 respondentene fra 30 ulike stater i USA. Identitetstyveri unntatt kortsvindel er overrepresentert i utvalget fra 2008, der hele to av tre sier de ble utsatt for at en annen åpnet kredittkonto i deres navn. Andelen som oppgir at identitetssvindelen er utført av venn eller familiemedlem er også høyere enn i de representative studiene (19% slektinger, 14% venner). Oppgitt tap er også høyere enn tallene fra Javelin Strategy and Research (tabell 3). Utvalget består med andre ord av de mer alvorlige tilfellene av identitetstyveri.

[10] Andelen i Norge som er utsatt totalt, divideres på forholdstallet beregnet etter anslagene fra USA

Uansett kan studien si noe om hvordan identitetstyveri påvirker offeret: På spørsmål om hvordan identitetstyveriet påvirker situasjon i dag, svarte:

- 70% at de ble nektet kredit
- 45% at det var vanskeligere å få lån eller kreditt
- 39% blir fortsatt oppringt av inkassobyråer
- 34% har fått kansellert sine egne kredittkort
- 33% har fått økte kredittkortrenter
- 23% sier det påvirker jobbmulighetene
- 20% har fått høyere forsikringspremier
- 6% sliter fortsatt med å få slettet kriminalitet fra sitt rulleblad
- 5% sier identitetstyveriet har ført til at de mistet jobben sin

Det rapporteres oftest om økonomirelaterte konsekvenser. Ved siden av at svært mange oppgir at de blir nektet ny kreditt, ser vi også – i denne selvrekruttert gruppen av identitetstyveriofre – at så mange som hver tredje har fått økte kredittkortrenter, hver femte har fått økte forsikringspremier, nesten hver fjerde oppgir at tyveriet har påvirket jobbmulighetene og fem prosent sier tyveriet førte til at de mistet jobben sin. I denne gruppen, som vi må anta er spesielt hardt rammet, var det fortsatt seks prosent som slet med å få slettet ID-tyvens kriminalitet fra sitt rulleblad.

Ikke uventet kan grove identitetstyverier få følelsesmessige langtidskonsekvenser. Undersøkelsen som er utført av ressurssenteret for identitetstyveriofre (ITRC) viste videre at i denne selvselekterte gruppen var:

- 51% blitt engstelig for egen økonomi
- 49% følte seg frustrerte
- 41% følte seg sviktet
- 37% sliter med maktesløshet
- 33% sliter med sinne
- 30% hadde mistet tillit til folk generelt
- 30% følte seg utmattet
- 30% var engstelig for familiens finansielle sikkerhet
- 25% var utslitt etter mistenkeliggjøring/kamp mot systemet
- 24% følte seg ubeskyttet av politi
- 24% hadde fått søvnforstyrrelser
- 22% sliter med feilplassering av sinne
- 19% sliter med overveldende tristhet
- 17% hadde fått konsentrasjonsvansker
- 14% isolering
- 11% føler skam
- 10% mener de har mistet alt
- 2% sier de er suicidale

Prosentene i listen over er neppe representative for alle identitetstyveriofre, men får stå som en illustrasjon på at identitetstyveri kan få svært alvorlige og langtrekkende konsekvenser for de som rammes.

5 Omfang av identitetstyveri basert på registerdata

En av årsakene til at det er vanskelig å danne seg et bilde av omfanget av identitetstyveri i Norge er at begrepet ikke en del av den operative terminologien i datasystemene som brukes i kriminalitetsbekjempelsen. Identitetstyverier vil kunne ansees som flere straffbare forhold, som simpelt tyveri (stjele kort og PIN-kode) og bedrageri (opprette kredittkort ved misbruk av annens ID-kort) (Torbjørn Nagelhus, Justisdepartementet)[11]. I seksjon for analyse og forebygging hos Politidirektoratet blir det sagt at identitetstyveri ikke er et kurant begrep og at det derfor er vanskelig å si noe om omfanget. Identitetstyverier utgjør kun en liten brøkdel av registrete tyverier og bedragerier, og i mange statistikker vil de ikke telles opp separat.

Som tidligere vist i tabell 1 kjennetegnes trinn I i identitetstyveriprosessen av uautorisert tilegning av persondokumenter. Vi skal i det følgende – så godt vi kan - både presentere de tallene vi har om identitetstyveri, samt tall fra omfanget av ulike dokumenter som er på avveier, og som derfor kan benyttes i identitetstyverier.

5.1 Pass

Passet er vårt fremste ID-dokument og inneholder blant annet den enkeltes fødselsnummer som brukes som en inngangsport for å verifisere vedkommende. Årlig forsvinner tusener av pass, de fleste blir stjålet eller mistet, men det er også en del som forsvinner i postgangen. Under vises en tabell over tapte/stjålne pass i perioden 2004-2009. (Det gjøres oppmerksom på at tallene fra 2004 kan være mangelfulle). Antall tapte pass har holdt seg på et jevnt nivå i perioden 2006 til 2009. Andelen som kommer bort i posten er liten, men andelen har økt jevnt siden 2004. Pr. i dag er det mulig å hente passet på den lokale politistasjonen, men beslutningen er overlatt til passinnehaveren. Det er imidlertid ikke sikkert at det er i postgangen at passene forsvinner. Det er også mulig at noen sier at de har blitt borte i posten og dermed klarer å skaffe seg et ekstra pass. Men når dette er sagt så er potensialet for å begå identitetstyveri betydelig større når det gjelder de vel 20.000 bortkomne og stjålne passene som er på avveier hvert år.

Tabell 6: Oversikt over tapte/stjålne pass i perioden 2004-2009.

	2004	2005	2006	2007	2008	2009
Mistet i posten	25	90	210	272	253	325
Frastjålet	349	1.258	1.302	1.107	971	1.768
Tapt/mistet	12.495	19.722	21.643	22.442	24.477	20.475
Ukjent	3.055	104	83	53	106	1.044
SUM	15.924	21.174	23.238	23.874	25.804	23.612

Kilde: Kommunikasjonsavdelingen Politidirektoratet

[11] I brev fra riksadvokaten 12.12.06 står det at "i Politi- og påtalemyndigheten vil saker som omhandler angivelig "identitetstyveri" bli etterforsket som bedrageri mot selskapet, jfr. Straffeloven §270 og §271".

Et annet problem i tilknytning til pass er opprettelsen av falske identiteter. Dette er et tiltagende problem. Kripos-leder Atle Roll-Mathisen kommenterer økningen av falske pass og sier at falsk identitet er en gjenganger i krimsaker og at det er vanskelig for politiet å oppklare slike saker, og at man bør styrke kontrollen av slike dokumenter. Med et falskt pass får man tilgang til konto i banken og lån. Straffesakregisteret hadde bare i første halvår i fjor 200 kriminalsaker hvor det var brukt falsk identitet og i halvparten av sakene var det snakk om falskt pass. I 2008 ble rundt 400 personer anmeldt, siktet og anmeldt for bruk av falsk ID (Aftenposten 19.1.2010). Også førerkort forfalskes og det er en økning av falske førerkort. I 2007 ble det avdekket rundt 100 falske førerkort (http://www.nettavisen.no/motor/article2442244.ece). Forfalskninger er imidlertid ikke identitetstyveri men kan være et redskap i samme type kriminalitet.

Det er nå utviklet nye pass som skal hindre misbruk. Bestiller du pass fra og med 1. oktober 2010, vil du få de nye, biometriske passene der et digitalt foto av ansiktet ditt lagres i en liten brikke som kan leses av fra passet. Dette biometriske bildet kan leses av i nærheten av grensekontrollen. Ansiktsformen til innehaveren av passet kan scannes på grensekontrollen, og kontrolleres opp mot det biometriske bildet og det tradisjonelle passbildet. Utlendingspass, reisebevis for flyktninger og statens tjenestepass vil også bli biometriske fra samme dato.

5.2 Førerkort

Førerkort inneholder bilde og fødselsnummer og dette er ofte tilstrekkelig for å opprette kreditt i eierens navn. Statens Vegvesen utsteder førerkort, men fører ikke statistikk over bortkomne eller stjålne førerkort. Det er en del førerkort som blir borte hvert år. Tapt/stjålet førerkort blir registrert i førerkortregisteret i Autosys. Det er kun SVV og politiet som har tilgang til å registrere dette i førerkortregisteret. Totalt antall tapte førerkort i 2008 som ikke er merket gjenfunnet er 57.796. For 2009 er tallet 55.796. (Kilde: Daltveit ved Statens Vegvesen 11.03.2003)

Vi blir også fortalt at førerkort ikke bare gir muligheter til økonomisk vinning. Det er også et problem at noen er ”stand-in” for andre og låner bort sin identitet og kompetanse slik at en annen får førerkort og kjøreseddel og godkjent en kompetanse som vedkommende ikke har. Dette betyr at det finnes en del sjåfører som ikke har den kompetansen som kreves. Samme problemstilling gjelder for falske førerkort fra andre land. Dette er et fenomen som har økt betydelig, og det jobbes mye for å avdekke dette.

Det har vært et stigende antall falske førerkort i løpet av de to siste årene sier Dagny Daltveit ved trafikantavdelingen i Statens Vegvesen til Nettavisen 2. desember 2008. I 2007 hadde de rundt 1000 anmeldte tilfeller. Hovedsakelige fra øst-europeiske land. En telefonsamtale bekrefter at dette fortsatt er et problem, men tall foreligger ikke på nåværende tidspunkt. Hun forteller videre at politiet har begynt å ta disse sakene meget alvorlig, og de tiltalte får strengere straffer enn tidligere. Dette er dokumentfalsk, og i tilegg er Vegvesenet bekymret for trafikksikkerheten.

5.3 Banker og bankkort

Mange bankkort har bilde og fødselsnummer. Og i tillegg kontonummer. Dette gir muligheter både for identitetstyveri og alminnelig tyveri.. Gjennom flere henvendelser til bankene viser det seg å være vanskelig å få tall om identitetstyverier fra den enkelte bank. Finansnæringens fellesorganisasjon har imidlertid sammen med Sparebankforeningen laget et notat over mislighetsstatistikk 2003-2008. Denne statistikken samler inn og viderefører informasjon om

interne og eksterne misligheter som tidligere er blitt innhentet av Bankenes Standardiseringskontor. I notatet pekes det på at det er noen svakheter ved den første presentasjonene av den nye statistikken, men det konkluderes med at den foreliggende statistikk vil kunne gi et anvendbart bilde av situasjonene på mislighetsområdet selv om den er preget av en del overgangssva-kheter. (Finansnæringens fellesorganisasjon 2009: 2). Rapporten gjennomgår statistikk og utvikling på en rekke områder som bedrageri av sjekker, debetkort, kreditkort, giro osv. For å synliggjøre omfanget av identitetstyverier har de også innhentet data for identitetstyverier som separat serie. Identitetstyveri defineres i statistikken som "forhold der et individ urettmessig kopierer en reell persons personalia, eller gjennom forfalskede dokumenter utgir seg for å være en bemyndiget representant for et firma og gjennomfører handlinger (ofte bedrageri) i vedkommendes eller firmaets navn". Men en rekke andre hendelser her kan gi et mulighetsgrunnlag for identitetstyverier. Vi gjengir derfor statistikken over omfanget av ulike bedragerier i 2003 til 2008:

Tabell 7: Oversikt over antall rapporterte misligheter 2003- 2008 fra Finansnæringens fellesorganisasjon.

Bedrageri:	**2003**	**2004**	**2005**	**2006**	**2007**	**2008**
Sjekker	95	129	186	119	100	107
Debetkort	5.444*	12.248*	9.394*	7.352	6.134	10.552
Kredittkort	*	*	*	3.126	3.554	4.594
Giro/overførsel	146	175	246	118	110	100
Kreditt	80	56	67	72	117	138
Hacking, phising etc.**	-	-	-	-	-	7
IKT-kriminalitet for øvrig	36	148	165	878	1.031	979
Urettmessige uttak	527	604	769	631	778	1.079

* For årene 2003- 2005 er tallene samlet for debet og kredittkort.
** Ny serie fra og med 2. halvår 2008

Det opplyses at flere av disse postene kan være saker som er å betrakte som identitetstyverier. Derfor har de gjort dette om til en separat serie. "*Identitetstyverier defineres i statistikken som et forhold der et individ urettmessig kopierer en reel persons personalia, eller gjennom forfalskede dokumenter utgir seg for å være en bemyndiget representant fore t firma og gjennomfører handlinger (ofte bedragerier) i vedkommendes eller firmaets navn.*" (Finansnæringens fellesorganisasjon 2009: 11). Her er det kun statistikk for 2. halvår i 2008 og antallet identitetstyverier er 96. Disse hadde et bruttotap på 5 241 298 kroner. (Det vil si de totale beløp som er utbetalt i hver enkelt sak. Egenandeler og refusjoner samt eventuelle senere innbetalinger fra gjerningsperson holdes utenom).

Tabell 7 illustrer at identitetstyverier er en liten del av de bedrageriene som er nevnt ovenfor. Heller ikke vet vi hvem disse er knyttet til, om de er privatpersoner eller mindre firmaer. Det bør også nevnes at noen av disse sakene eller tilfellene kan inngå i flere statistikker. Når dette er sagt så ser vi av tabellen at det er en jevn økning i de fleste misligheter fra 2003 og frem til 2008.

5.4 Teleselskaper

Teleselskaper opplever at det opprettes abonnement i andres navn. Vi har fått tall og kommentarer til forekommende identitetstyverier hos følgende selskaper:

- **Chess** forteller at de i 2009 har avsluttet 2.411 kundeforhold som følge av identitetstyveri. Av dette er 2.142 knyttet til kontantkort, mens 269 er knyttet til etterskuddsfakturerte abonnement, (Mail fra Økonomidirektør Arild Christiansen Chess). Han skriver også at de dessverre ikke har tall for 2008.

- **Telenor**: 1395 mobilabonnement bestilt med falsk ID i 2009, mot 1361 i 2008. Totalt tap 8,2 mill NOK i 2008. Kilde:http://www.idtyveri.info/index.php?option=com_content&view=category&layout=blog&id=4&Itemid=25. Antall identitetstyverier har hatt en svak nedgang i 2008. Tatt i betraktning den totale omsetning og antall abonnenter er antallet ikke så stort.
- Fra **Lebara** fikk vi følgende mail: "*Av og til blir vi kontaktet av folk som melder fra om ID-misbruk i forbindelse med opprettelse av kontantkort. Vi har registrert 166 henvendelser i fjor (dette tallet inkluderer kun folk som ønsket å fylle ut et sperreskjema mot fremtidige registreringer). Det skjer at noen ikke ønsker å gjøre dette, de vil bare stenge det nummeret som var registrert i deres navn - vi har ikke oversikt over disse henvendelser. Dette tallet er nok mye høyere enn 166. Vi leverer ingen rapporter på dette til noen.*"
- Om tallene over kun refererer til identitetstyverier er imidlertid noe usikkert. Tallene kan også omfatte fiktive identiteter. Heller ikke her har vi klart å avdekke det totale bildet av identitetstyverier. I telefonsamtaler med flere teleselskaper antydes det imidlertid at identitetstyveri helt klart forekommer, og at det er en viss økning. Men mange aktører ønsker ikke å få sitt navn eller teleselskap nevnt.

Internett- og telebransjen gikk i 1999 sammen om å opprette en egen bransjeforening (ITAKT) for å bekjempe svindel og misbruk av infrastruktur og teletjenester. Dette behovet for samarbeid kom, i følge bransjen selv, i forbindelse med liberaliseringen av telemarkedet. Tiltaket har fått større relevans i de senere år i og med den teknologiske utviklingen og globaliseringen av tjenester. ITAKT jobber for å heve medlemmenes kompetanse på området, utarbeide retningslinjer for "best practice", og for mottiltak mot svindel (se www.itakt.no). Sett i forhold til bedriftenes omsetning, ser det ikke ut til at identitetstyveri utgjør noen stor økonomisk trussel.

5.5 Skattelister

Skattelistene er offentlige og har blitt en lett tilgjengelig informasjonskilde som kan hjelpe ID-tyven til å blinke ut sine ofre. Representanter for banker i Norge forteller at de merker en større pågang av forsøk på å opprette kontoer med en annen ID etter at selvangivelsen er kommet i posten. Christian Meyer i Norsk Senter for informasjonssikring (NorSIS) sier i et intervju med DinSide: "*Jeg har selv snakket med ID-tyver som synes vi har en fantastisk ordning her i landet. Offentliggjøringen av skattelistene, krydret med nordmenns naivitet i slike saker, er et veldig godt utgangspunkt for å drive kriminell virksomhet.*"

Skatteetaten tar nå sine forholdsregler for å redusere risikoen for Identitetstyveri, samtidig som de sparer miljøet for papir. For skatteoppgjøret 2009 er det mulig for lønnstakere og pensjonister å reservere seg mot selvangivelse og skatteoppgjør på papir. De må selv gjøre operasjonen og sende inn mobil og e-postadresse. Her krever e-forvaltningsforskriften av man går inn og ser på det mottatte dokumentet innen 7 dager etter mottagelse. Hvis ikke er Skatteetaten forpliktet til å sende skatteyter en papirkopi. (www.skatteetaten.no/eaktør).

5.6 Melding om flytting

I forbindelse med identitetstyverier inngår ofte en melding om flytting til Folkeregisteret. Det har også vært noen innvendinger fra andre kommersielle aktører om at det er for lett for uvedkommende å etablere seg på ny adresse som gjør det mulig å få tilsendt varer og lignende som man har bestilt i en annens navn til den nye adressen. Jan Fredrik Karlsen oppdaget at noen hadde stjålet hans identitet da han skulle opprette en ny bankkonto og ble bedt om å sjekke at banken hadde hans riktige adresse. Det hadde de ikke. Folkeregisteret bekreftet

overfor Karlsen at de hadde mottatt en skriftlig adresseendring, og at den falske adressen dernest automatisk ble registrert av både banken hans og av forsikringsselskapet. Hvor ID-tyvene hadde fått tak i hans personnummer viste han ikke (Dagbladet 27.11.2007). I dag kan man sende skriftlig melding om flytting, men i tillegg til personnummer må man også vedlegge en kopi av legitimasjon. Det er imidlertid ingen meldeplikt tilbake om at flytting er registrert.

Melding av flytting innenlands kan også utføres på internett av alle som er bosatt i Norge. Det kan gjøres gjennom MinID eller min private innlogging til offentlige tjenester,. Ved bruk av pin-koder og selvvalgt passord er dette en tjeneste som identifiserer den enkelte. Alle over 13 år kan opprett MinID. Pr. oktober 2009 er 1,5 millioner nordmenn registert. MinID kan brukes på over 50 tjenester på nett fra statlig og kommunal sekstor, som NAV, skatteetaten og lånekassen. Behandlingsansvarlig for personopplysninger er Direktoratet for forvaltning og ikt. Minside lagrer bare de data som trengs for at man skal kunne opprette sin egen personlige side. På Minside kan man få innsyn i opplysninger som er lagret om deg i ulike offentlige registre. Opplysningene blir hentet fra de aktuelle registrene. De blir ikke lagret på Minside. For eksempel ligger alle skattedataene dine fremdeles i Skatteetatens registre. Kilde: http://www.norge.no/minside/ 22.2.2010.

5.7 Kredittopplysninger

Et viktig hjelpemiddel for ID-tyven er tilgang til mulige ofres kredittverdighet. Det har liten hensikt å stjele identiteten til en gjeldsslave. Det er nok å oppgi fødselsnummer eller kortnummer for å handle på postordre eller kjøpe telefonabonnement. Ved å varsle et kredittopplysningsselskap når man mister slik informasjon, kan man forhindre identitetssvindel, sier salgs- og markedsdirektør Frode Berg i Dun & Bradstreet (D&B), Norges ledende kredittopplysningsselskap. Fra 2000 til 2005 har antall sperringer hos Dun & Bradstreet mer enn doblet seg. Menn er langt flinkere enn kvinner til å sikre seg slik, og 21 prosent flere menn enn kvinner har registrert frivillig sperre hos Dun & Bradstreet de siste fem årene.
http://www.db24.no/DB/Nyheter/+Ikke+nok+%C3%A5+sperre+kontoen.b7C_wtvW2d.ips

Å sperre innsynet for kredittvurdering kan også være en måte å stoppe identitetstyveri. Antall personer som har valgt å sperre muligheten for kredittvurdering er vokst betraktelig. Vi vet ikke om dette skyldes økning i antall identitetstyverier, flere gjeldsofre etter finanskrisen, eller andre forhold. Det er likevel sannsynlig at i hvert fall deler av økningen kan knyttes til identitetstyverier. D&B har nå kontaktet Finansnæringens fellesorganisasjon (FNH) og Næringslivets Hovedorganisasjon (NHO) for å få til et enda tettere samarbeid mellom kredittgiverne og kredittopplysningsselskapene. Målsettingen er at man i fremtiden skal kunne formidle sperringer mellom kredittopplysningsselskapene og kredittgiverne dersom kundene ønsker dette.

5.8 Internett[12]

Økningen i identitetstyveri har en sterk tilknytning til utviklingen og alminneliggjøringen av internett, og tilgang til nettbaserte tjenester for enkeltindividet. De fleste husstander har i dag tilgang til internett, og husstandsmedlemmene foretar søk, nedlastinger, netthandel, offentlig tjenestehåndtering, nettbanktransaksjoner, deltar i sosiale medier, etc, i større og større grad. I Norge har over 90 prosent av befolkningen tilgang til internett. Hele ni av ti av disse har slik tilgang hjemme, mens 65 prosent (også) har slik tilgang på jobb. Rundt tre av fire sier de har handlet på nettet (Slettemeås 2009).

[12] Dette avsnittet er forfattet av Dag Slettemeås, SIFO

Sikkerhet, trygghet og risiko er elementer som inngår i den elektroniske hverdagen. Håndtering av sikkerhet er en grunnleggende forutsetning for all annen aktivitet på nettet og ellers i en digital hverdag. Sikkerhet kan avhenge av både menneskelige og teknologiske faktorer – og oftest en kombinasjon av begge. Sikkerhetskjeden er gjerne ikke sterkere enn det svakeste ledd, og ofte er dette forbrukeren fordi han/hun er uforutsigbar i sin atferd (Slettemeås 2007: 74).

Det er nå langt mer penger og persondata i sirkulasjon i digitale kanaler enn tidligere, noe som gjør nettarenaen svært attraktiv for profesjonelle kriminelle. Betaling over internett og nettbanktransaksjoner åpner for å angripe spesielt forbrukere, ettersom dette er langt lettere enn å gå rett på virksomheten eller banken. Det viser seg at norske nettbrukere er svært utsatt for svindel fordi nettbruken er omfattende, mens sikkerhetsrutinene er svake (eks. knyttet til bruk av brannmur, oppdatert antivirus, kryptering av trådløst nettverk, etc).

Den omfattende bruken av både kommersielle og offentlige tjenester på internett medfører mange påloggingsgrensesnitt for forbrukerne. Ofte må man lage nye brukernavn og passord og kravene til lengde og tegn på disse varierer. En konsekvens er at man gjerne gjenbruker samme pinkode på mange tjenester. Dette forenkler hverdagen, men gjør brukeren mer sårbar dersom pinkoden stjeles. Da ligger veien åpen for både grov svindel og identitetstyveri (Slettemeås 2007).

En måte myndighetene har tilnærmet seg denne problemstillingen på er å støtte utviklingen av teknologi og systemer for sikker autentifisering, verifisering og signering, blant annet gjennom arbeidet i PKI-forum (se bla. Slettemeås 2004), som er blitt videreført i strategien for elektronisk ID[13]. Norske innbyggere har de siste årene fått tilgang til MinSide (http://www.norge.no/minside/), og kan logge seg på med *MinID*, som er den enkeltes private innlogging til offentlige tjenester. Videre har man gjennom *BankID*-samarbeidet (www.bankid.no) i lenger tid gitt forbrukere mulighet til elektronisk legitimasjon og sikker identifisering og signering på nett. Disse tiltakene bidrar til å redusere risikoen for at enkeltpersoner blir svindlet gjennom nettbaserte tjenester.

5.9 Netthandel

Mange av dagens økonomiske transaksjoner er internasjonale i karakter, og foregår i økende grad på nett. Økonomiske transaksjoner som krysser landegrenser skyldes ikke lenger bare nordmenn som bruker kortet i utlandet. I dag handles det over landegrensene hjemme fra de tusen hjem. Å handle på nettet betyr at du etterlater deg elektroniske spor som igjen kan føre til identitetstyveri.

Vi skal se noe nærmere på netthandlerne og tar utgangspunkt i en rapport utført for Forbrukerrådet i slutten av 2007. Undersøkelsen er landsrepresentativ og dataene er samlet inn av TNS Gallup. Undersøkelsen omfatter kun de som har handlet på nettet siste år. 95 prosent av respondentene brukte datamaskin som plattform for handelen, men 11 prosent e-handlere hadde også brukt mobilen som plattform. De fleste handler 1-5 ganger i måneden, mens 9 prosent oppgir at de handler 6 ganger eller oftere i måneden.

De fleste betaler netthandlene med kredittkort (58 %) og 22 % med giro/oppkrav og 8 % med debetkort og 8 % på andre måter. En noe større andel menn enn kvinner (66 % av mennene mot 51 % av kvinnene) betaler oftere med giro/oppkrav. Omtrent halvparten (45 %) hadde e-handlet på et utenlandsk nettsted i løpet av siste året. Menn (52 %) oftere enn kvinner (38 %). Andelen faller med økende alder. De som ikke handlet på utenlandsk nettsted oppgir sikkerhet, dårlig forbrukerbeskyttelse og toll/moms som grunn for at de ikke gjør det.

[13] Se FAD: http://www.regjeringen.no/nb/dep/fad/tema/ikt-politikk/esignatur.html?id=457129

Et mindretall (15 %) hadde opplevd problemer i forbindelse med sin e-handel siste året. Problemene gjaldt i hovedsak forsinket levering og at bestilt vare ikke ble levert. Her var det ingen store forskjeller mellom kjønnene. Mer enn halvparten (54 %) svarer at de kommer til å e-handle mer i fremtiden enn de har gjort frem til nå. Dette gjelder flere menn enn kvinner, og særlig aldersgruppen 30-44 år.

Ifølge Sifo-surveyen 2009 svarte mer enn halvparten av de som hadde handlet på internett at de hadde mottatt svindelbrev - f.eks. store lotterigevinster- på e-mail[14]. Denne type e-mail er altså så vanlige at de fleste gjenkjenner slike brev. Men når slike brev fortsatt strømmer på, er det sannsynligvis noen som fortsatt biter på. Slik phishing[15] etter finans- og identitetsopplysninger på nettet har til hensikt å gi ID-tyvene informasjoner som senere kan utnyttes til økonomisk tapping av ofrene (Slettemeås 2009).

Mye av dette er internasjonal svindel, og det norske folk er fortsatt noe beskyttet fordi norsk er et lite språk. Det finnes oversettelsesprogrammer, men det er fortsatt lett å gjennomskue et automatisk oversatt brev, med alle absurditeter og feil det medfører. Ifølge ØKOKRIM sendes det årlig 100 millioner kroner ut av landet, fordi enkelte lar seg friste av framtidige, store gevinster som naturligvis aldri kommer. (http://www.teknofil.no/wip4/derfor-virker-nigeria-brev/d.epl?id=28477).

5.10 Manglende registre og statistikk

I sin kronikk "Å bli frastjålet identiteten" av fornyingsminister Rigmor Aasrud 19.12.09 kan vi lese at regjeringen støtter arbeidet mot identitetstyveri på flere måter, blant annet gjennom dette prosjektet som skal skaffe egne tall til veie. Å skaffe faktiske tall har imidlertid vist seg å være komplisert fordi mange offentlige kontorer og organisasjoner ikke samler inn tall systematisk. For eksempel vil identitetstyveri anmeldes hos de lokale politikontor. Her blir det skrevet en rapport som igjen sendes til politiet sentralt. Men hvordan ganske like hendelser blir rapportert kan variere sterkt, ofte er identitetstyveriet en av flere hendelser og dette betyr igjen at hvor man velger å kategorisere denne hendelsen vil variere.

Pr. i dag (primo 2010) føres det ingen samlet statistikk over id-kriminalitet i Norge. Det er også mulig at slik statistikk ikke vil fange opp hele omfanget, både fordi offeret noen ganger ikke er klar over at hans eller hennes identitet er misbrukt, og fordi de unnlater å melde tyveriet til politiet, eller at hendelsen blir kategorisert under en annen rubrikk. Ved henvendelse til ØKOKRIM får vi vite at politiet ennå ikke har gode nok statistikker for identitetstyveri, men dette er noe det jobbes med. I mars 2010 har ikke politiet noen grupper som jobber spesielt med identitetstyverier. Heller ikke Brønnøysundregisterne registrerer ID-tyverier.

Under arbeidet med dette prosjektet fant vi at mange bedrifter og organisasjoner er berørt av identitetstyverier, men de fører ikke slik statistikk, og andre ønsker ikke offentliggjøre slike tall. Dette fordi det erfaringsmessig vil skape en del ekstrahenvendelser, og ikke minst frykter kommersielle bedrifter - som banker og teleoperatører - at slik offentliggjøring kan skade deres omdømme. Et annet problem er at det ligger ulike definisjoner av identitetstyveri til grunn. Det kan virke som noe av statistikken over identitetstyverier inneholder beslektede former for kriminalitet som for eksempel fiktive identiteter, falske pass osv. Alle vi har henvendt oss til er imidlertid oppmerksomme på fenomenet og er urolige over en eventuell øk-

[14] Blant de som hadde handlet på internett var det fem prosent som oppga at de hadde blitt svindlet på nettet. Bare 40 prosent sa at de leste hele eller mesteparten av kjøpsbetingelsene når de handlet i ny nettbutikk. Kvinner er i følge dem selv noe mer forsiktig enn mennene, og opplever sjeldnere å bli svindlet (Sifo-surveyen 2009)

[15] *Phishing* er en betegnelse på digital snoking eller fisking etter sensitiv informasjon, som passord eller kredittkortnummer. Ref: http://no.wikipedia.org/wiki/Phishing

ning, og de uttrykker et sterkt ønske om at kartlegging og statistikk blir samlet. Et omfattende rapporteringssystem over identitetstyverier vil kunne si noe om utbredelsen, men også om hvilke kanaler som har vært anvendt i hvert enkelt tyveri, og dermed noe om hvor sårbare de ulike systemene er. Dette vil igjen gjøre det lettere for både bedrifter og personer å beskytte seg mot dette.

6 Bedrifter som tredjepart

Bedrifter kan også bli utsatt for identitetstyveri. I slike tilfeller vil ID-tyven foreta disposisjoner i bedriftenes navn, som kan ramme både bedriftenes omdømme og økonomi. I denne rapporten har vi imidlertid kun fokusert på identitetstyveri rettet mot fysiske personer. Men som det blant annet framgår av intervjuene med identitetstyveriofrene i denne rapporten, vil bedrifter ofte bli økonomisk skadelidende som tredjepart: Når en ID-tyv for eksempel bestiller varer på stjålen identitet og oppgir en fiktiv adresse, kan ikke bedriften fakturere identitetstyveriofferet, men må bære tapet selv. Selv om det kan være slitsomt og tar tid, vil offeret i regelen klare å bevise at det ikke er han eller henne som har bestilt varene eller tatt ut kreditt.

Det er viktig å merke seg at *ett* identitetstyveri kan resulterer i *mange* bedragerier. Et identitetstyverioffer regnet ut at han gjennom til sammen 13 bedragerier ble frastjålet rundt 500.000,- kroner. Han måtte bære omkostningene ved å rydde opp i de mange kravene identitetstyveriet resulterte i, men det var bedriftene som til syvende og sist måtte ta det økonomiske ansvaret (Se referert SIFO-intervju i kapittel 2). Vi skal ikke se bort fra at det blir en del oppryddingsarbeide i bedriftene også.

Når man beregner omfanget av identitetstyveri, er det uenighet om simpel kortsvindel skal inkluderes. Dersom simpel kortsvindel – dvs at noen har stjålet et bankkort og tar ut penger eller varer på dette kortet – skal regnes som identitetstyveri, tyder tall fra USA og Canada på at antallet dobles. Dette betyr at alvorlig identitetstyveri ser ut til å være like utbredt som simpel kortsvindel. Men fordi hvert enkelt identitetstyveri gjerne resulterer i mange bedragerier, er identitetstyveri langt mer alvorlig. Simpel kortsvindel utgjør i dag en mindre trussel, sett både fra bank, bedrift og kortkunde.

For å begrense skadeomfanget av simpel kortsvindel har banknæringen utviklet et svært velfungerende kontrollsystem. I store deler av verden har ned til den minste lille butikk i dag betalingsterminaler som vil avvise stjålne kort, og kundene må identifisere seg med personlige koder. Dette representerer et svært godt system som begrenser skadevirkningene av kortsvindelen. *De med sterke insentiver mot tap, lager gode systemer*. I tilfellet med bankene er det tydelig at dersom forbrukerne hadde måttet bære tapene, ville institusjonene mistet insitamentet til å lage dette godt fungerende kontrollsystemet. Tidligere direktør for Forbrukerrådet Stalheims lov lyder: *For å få gode systemer må man plassere ansvaret for at noe kan gå galt hos den aktør som kan påvirke risikoen.*

Bankenes praksis med utstedelse av bankkort med bilde, som gjelder som legitimasjonsbevis på lik linje med pass og førerkort, er ofte benyttet i identitetstyverier. Selv om bankkort rapporteres som stjålet, kan ID-tyven fortsatt benytte slike bankkort som legitimasjon ved for eksempel opprettelse av kreditt. Bildene på bankkortene er små og ofte dårlige. Dette gjør det enkelt å bruke dem av en av samme kjønn og omtrent samme alder. I våre intervjuer med identitetstyveriofre var det gjerne bankkort med bilde med i spillet. Vi forstår ikke helt hensikten med bankenes praksis med å utstede bankkort med bilde, fødsel- og personnummer, nå

som personlige koder og kortterminaler er tilgjengelig nesten over alt. Det bør reises spørsmål ved om bankkort med bilde skal kunne brukes som legitimasjonsbevis.

Brønnøysundregistrene er en forvaltningsetat med ansvar for en rekke nasjonale kontroll- og registreringsordninger for næringslivet. Det overordnede mål er å bidra til økt økonomisk trygghet og effektivitet både for næringslivet og i samfunnet generelt. Brønnøysundregistrene fører ingen statistikk over identitetstyverier. Sikkerhetsansvarlig Olav Melteig sier at "I forhold til våre tjenester og løsninger, så er det mest aktuelt i forbindelse med stjeling av firma, avarter av "companies hijacking", gjennom misbruk og stjeling av organisasjonsnummer.
Vi har noen tilfeller av dette pr år, anslagsvis 2-3 pr år." Selv om de ikke fører statistikk over identitetstyverier er de oppmerksom på dette og følger med. De deltar blant annet i ID-tyveriprosjektet som kjøres i regi av NorSIS. I en pressemelding 27.oktober 2009 fra Brønnøysundregistrene opplyses det at det settes i verk nye tiltak mot identitetstyveri. Når det meldes om omfattende endringer i et selskap, for eksempel at hele styret er endret i tillegg til forretningsadresse eller postadresse, vil det tidligere styret straks bli varslet. Videre kan vi lese at "Når Foretakregisteret får henvendelser hvor det er mistanke om falske dokumenter, falsk underskrift eller andre straffbare handlinger, oppfordrer vi om at forholdet blir politianmeldt og at det blir vurdert å begjære midlertidig forføyning overfor registreringsvedtaket.

Et sentralt problem i forhold til utbredelsen av identitetstyveri, er dilemmaet mellom *trygghet* og *effektivitet*. Det ser ut til å være vanskelig å forene enkle, effektive systemer med høy brukervennlighet og lønnsomhet på den ene siden, med trygge, vanntette systemer som stopper misbruk og avslører kriminalitet på den andre siden. Det er for eksempel fortsatt relativt lett for en ID-tyv å bestille mobiltelefoner og opprette telefonabonnementer i falskt navn, sannsynligvis fordi teleselskapene ikke finner det lønnsomt å håndholde strenge kontrollrutiner som ville forhindret dette.

Men som bankenes betalingsterminaler viser, er det mulig å lage gode systemer som fremmer både effektivitet og trygghet. En større aktsomhet blant bedrifter mot ID-tyveri vil være fordelaktig for både bedrifter og personer som rammes av dette fenomenet. Det er bedriftene som bærer det økonomiske tapet, men det er ikke alltid at de involverte personene melder identitetstyveriet til politiet. Riksadvokaten har tatt opp med bransjeforeningen for internett- og telefonleverandører at bransjene selv bør vurdere å anmelde forhold, istedenfor å overlate dette til de personer som er utsatt for misbruk av sin identitet (brev av 19.12.06).

7 Ulike typer risiko og utsatthet for identitetstyveri

Identitetstyveri foregår på mange måter. Muligheten for at en person skal oppleve at hun eller han skal bli utsatt for identitetstyveri kan noe forenklet sies å være et resultat av risikoer den enkelte utsetter seg for eller risikoer i systemet. *Personrisiko* henviser til muligheten for å bli frastjålet identiteten for eksempel ved at man ukritisk gir fra seg personlige opplysninger, er uforsiktige med hvordan posten håndteres, ikke skjuler pinkoden når man tar ut penger, mister passet osv. I et intervju på Norgesglasset juli 2009 sier Trude Talberg Furulund som jobber i Datatilsynet at *" i Norge har vi tradisjon for å stole på hverandre. Den høye tilliten er et godt samfunnstrekk, men baksiden er at mange av oss har litt for lett for å gi fra oss personopplysninger*".

Vi har ikke noen opplysninger om hvor tillitsfulle det norske folk er i så henseende. Under er gjengitt resultater fra en kanadisk survey. Vi ser her at for eksempel 41 prosent har åpen postboks, 21 prosent river ikke i stykker dokumenter før de kastes osv.

- 92 prosent sier de aldri eller sjelden gir fra seg personlig informasjon på telefon
- 88 prosent sier de sjekker at ingen ser når de taster inn kode i kortterminal eller minibank
- 79 prosent river vanligvis i stykker dokumenter med finansielle- eller viktige person-opplysninger før de kaster dem.
- 59 prosent har låst postboks
- 57 prosent oppbevarer som regel sensitiv informasjon på et låst sted (skuff, boks)
- 50 prosent er mer forsiktige med hva slags – og hvor mange – identitets dokumenter de bærer med seg.
- De fleste oppgir at de skifter viktige passord i hvert fall hvert 2-5 år, mens 30 prosent sier de aldri skifter slike passord.
- 20 prosent sier de har sluttet helt, eller redusert, netthandel fordi de er bekymret for identitetstyveri.
- 9 prosent sier de har sluttet helt, eller redusert, bruk av nettbank fordi de er bekymret for identitetstyveri.
  Kilde: Sproule & Archer (2008)

Om det er slik i Norge vet vi ikke. Det er imidlertid liten grunn til å tro at nordmenn er mer påpasselige enn kanadiere, noe som igjen skulle tilsi at muligheten for at noen skal kunne stjele identiteten deres så absolutt er tilstede.

Ved *systemrisiko* skjer identitetstyveriet fordi det er manglende kontroll og rutiner i systemet. To typer av systemsvakhet er mulig. For det første; der en ID-tyv har tilegnet seg en annens identitet og lykkes i å bruke denne til identitetstyveri fordi det er huller eller svakheter i kontrollsystemene. Hovedproblemet her er at det ikke finnes noe system for å sjekke om autentiserende dokumenter som pass, sertifikat og bankkort med bilde er gyldige. Her ønsker NorSIS å etablere en felles database på linje med sjekk av heftelser på kjøretøy. Datatilsynet har godkjent dette i brevs form med kopi til FAD, og NorSIS har sendt henvendelse til Kripos og

Vegdirektoratet for videre dialog med tanke på felles database for tapte pass og førerkort (Christian Meyer, NorSIS). Et system som ser ut til å virke bra, er bankenes system for å avvise ugyldige bankkort for betaling.

For det andre kan hele systemer blir angrepet, for eksempel ved hacking eller ved at man får plantet en trojaner. Episoden i Spania er et eksempel på dette, der tusenvis ble tappet for kreditt- og personopplysninger. Konsekvensene her kan tenkes å få et langt større omfang enn der et enkelt svindelforsøk lykkes i møtet med systemet fordi det her er mulig å rette massive angrep mot bedrifter og organisasjoner. I grunnleggende forstand er begrepet 'hacking' knyttet til spredning av en krise til hele det finansielle systemet, fra det nasjonale finansielle systemet til det internasjonale finansielle systemet. For eksempel kan vi lese hos Norges Bank:

Systemrisiko er risikoen for at soliditets- og likviditetsrisikoen i en bank skal spre seg og medføre insolvens eller illikviditet hos andre finansielle institusjoner. Dette vil svekke bankenes evne til å formidle kreditt og kapital, og kan i verste fall svekke bankenes mulighet til å tilby betalingstjenester. De totale samfunnsmessige kostnadene i slike tilfeller kan overstige bankens kostnader, noe som tilsier at banken ikke har gode nok incentiver til å begrense denne risikoen (Norges Bank, 2004).

Våre informanter uttrykker en bekymring over en mulig økning av identitetstyverier i Norge. Finansnæringens fellesorganisasjon nevner følgende faktorer som kan være medvirkende årsaker til en økning på kriminalitetsområdet:

- Det foreligger et økende behov for "rene identiteter" fra personer knyttet til organiserte kriminelle grupperinger.
- Denne type kriminalitet har ikke spesielt fokus hos politi og påtalemyndighet, pg prioritert saksområde som for eksempel vold må gå foran når ressurser skal fordeles.
- Det er relativt lave strafferammer for å bruke, og selge slike falske dokumenter, til tross for store muligheter for økonomisk vinning.
- Det er juridiske mangler i form av at det i Norge ikke er ulovlig å være i besittelse av forfalskede dokument.
- Risikoen for oppdagelse er relativt liten, grunnet manglende kompetanse hos de som utøver kontrollfunksjonen.
- Personen utsatt for identitetstyveri er ofte ikke klart over forholdet på det tidspunktet identiteten blir brukt. Offeret oppdager normalt ikke problemet for han/hun blir konfrontert med fakta som den "nye brukeren" står for. Dermed forsvinner og "ferske spor"

(Kilde: Felles utfordringer knyttet til identitetsmisbruk. Finansnæringens fellesorganisasjon 2008).

Det er gjort en del for å tette huller som har vært utnyttet til identitetstyverier. Det er utviklet nye pass med biometiske data (fra og med 1.1.2010), og det er utviklet en BankID som skal sikre autentisering og signering på nett. Løsningen består av en sentral infrastruktur driftet av BBS. Løsningen er basert på utstedelse av kvalifiserte sertifikater og er registrert hos Post- og teletilsynet, på linje med BuyPass. Den elektroniske signaturen kan brukes til avtaleinngåelse. Med BankID kan du også inngå avtale om BankAxess til bruk ved kjøp på internett. Å minne nordmenn om å passe på sine identifikasjonspapirer og ikke å gi fra seg fødselsnummer til alle som ber om det, kan også redusere risikoen for identitetstyveri.

En interdepartemental arbeidsgruppe ledet av Justisdepartementet (JD), med representanter fra Fornyings-, administrasjons- og kirkedepartementet (FAD), Samferdselsdepartementet, Arbeids- og inkluderingsdepartementet, Nærings- og handelsdepartementet og Utenriksdepartementet foreslo i 2007 innføring av et frivillig nasjonalt ID-kort for alle med fast bopel i

Norge. For norske statsborgere skal kortet dessuten kunne utstyres med funksjonalitet for reise innen Schengen området (opplysninger om norsk statsborgerskap mv). Arbeidsgruppen forslag innebærer at kortet forsynes med følgende sikkerhetselementer i henhold til internasjonale standarder:

- Bilde av og opplysninger om innehaveren
- Optisk maskinlesbar tekst som inneholder personinformasjon fra den visuelle teksten
- Kontaktløs brikke som skal inneholde persondata sammen med biometri (ansiktsfoto og fingeravtrykk)
- Kontaktbrikke for lagring av elektronisk ID (eID) og elektronisk signatur som oppfyller forvaltningsstandarder fastlagt av Fornyings-, administrasjons- og kirkedepartementet.

Hovedbegrunnelsen for forslaget om å etablere et nasjonalt ID-kort er å legge til rette for at folk har et tilbud om å kunne dokumentere sikker identitet, mao. knyttet til alminnelig behov for identifisering. Et nasjonalt ID-kort som har høy grad av tillit mht. sikkerhet vil dessuten kunne fungere som et basiskort for utstedelse av andre ID-kort, f.eks. bankkort eller førerkort. Dette vil kunne gi større sikkerhet i identifiseringsprosessen, samtidig som det vil forenkle arbeidet både for den som skal utstede nytt ID-kort og for den som skal identifisere seg.

Sikker identifisering av personer og effektivitet i samhandling representerer betydelige samfunnsinteresser. Riktig identifisering er en kjerneoppgave for myndighetene, bl.a. innenfor områder som berører samfunnssikkerhet. En av de store utfordringene er å fastslå riktig identitet ved utstedelse av et ID-kort. Offentlige myndigheter har bedre kontrollmuligheter på dette feltet enn andre aktører, bl.a. gjennom tilgang til offentlige registre og kontakt med myndighetene i andre land.

Arbeidsgruppen har også anbefalt ID-kortet skal utstyres med en elektronisk ID (eID). eIDen skal kunne benyttes til følgende formål:

- Autentisering ved pålogging av nettsider
- Digital signering av skjema på nettsider eller dokumenter i f.eks Word eller PDF-format
- Digital signering av e-post
- Dekryptering av mottatte krypterte e-post, dokumenter eller andre typer elektroniske typer meldinger.

Arbeidsgruppens forslag har vært på bred høring, og JD og FAD arbeider nå for å følge opp arbeidsgruppens forslag. Arbeidsgruppens rapport finner man her: http://www.regjeringen.no/nb/dep/jd/dok/rapporter_planer/rapporter/2007/nasjonalt-id-kort---sluttrapport-februar.html?id=457630.

Et annet tiltak som beskytter er gjenpartsplikten – det vil si at forespørsler blir tilbakemeldt. Dette vil for eksempel sikre at den som har fått forespørsler om sin økonomi hos et kredittselskap vil bli oppmerksom på dette og reagere dersom det er en annen som har bedt om kredittvurderingen. Ikke alle er pålagt meldeplikt, men i Pressemelding fra 27. oktober kan vi lese at Brønnøysundregisterne har innført meldeplikt når det meldes om omfattende endringer i et selskap.

Det kan stilles noen spørsmål ved verifisering og legitimering. Ingen sikkerhetsordning er sterkere enn det svakeste leddet. Svakhetene i systemene ved utstedelse og verifisering av legitimasjonsdokumenter gjør både folk og bedrifter sårbare for denne type kriminalitet. Det utstedes i dag en rekke dokumenter som aksepteres som bevis på identitet. Hvor egnet disse er, kan det sikkert stilles spørsmål ved.

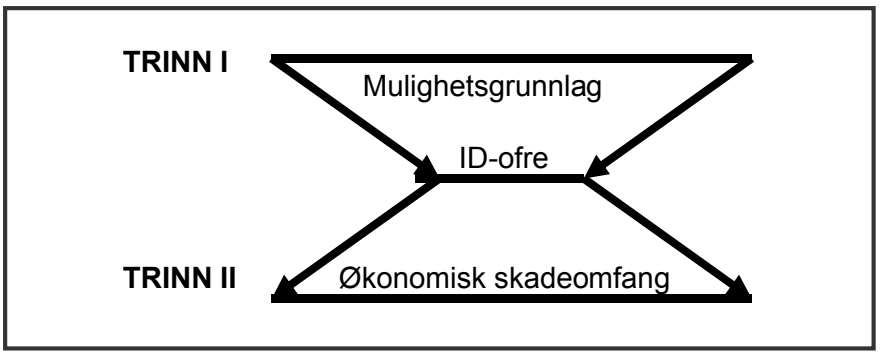
Det er et ideal at Norge skal være et åpent samfunn der man skal ha rett til å gjøre seg kjent med forvaltningens saksdokumenter. Dette kan skape problemer. Bl.a kan ID-tyver misbruke denne åpenheten til egen vinning. For eksempel er skattelistenes dypere funksjon at de gir en transparens i samfunnet som gjør det vanskeligere å unndra skatt. De er et massivt datagrunnlag for å si noe om landet vi bor i. Samtidig er det klart at disse blir brukt av andre som har mindre hederlige hensikter. Kanskje hadde det vært mulig med en offentlig skatteliste hos Skatteetaten, som man må benytte MinID for å få tilgang til, og som registrerer alle som benytter tjenesten, og lar deg se, eller gir melding om, hvem som har søkt opp dine detaljer? Banker som opplever at deres server har blitt utsatt for hacking, burde kanskje også hatt meldeplikt til kunder som kan være berørt?

8 Konklusjon

Det finnes ikke god statistikk i Norge som kan si noe sikkert om omfanget av identitetstyveri. Men uansett hvor stort eller lite omfanget av identitetstyveri skulle være, er det å bli utsatt for identitetstyveri alvorlig for de som rammes.

Identitetstyveri er et komplekst fenomen, og det er ikke enighet om hvordan begrepet skal forstås, eller hva som skal regnes inn under identitetstyveri. I hovedsak handler identitetstyveri om ulovlige handlinger begått i en annens navn, uten at den det gjelder har gitt tillatelse til dette. Vinningskriminalitet gjennom identitetstyveri starter gjerne med tyveri av persondata, for eksempel tyveri av lommebok med førerkort og bankkort med bilde. Vi har derfor funnet det hensiktsmessig å skille mellom identitetstyveri trinn I: Uautorisert tilegning av persondata, og identitetstyveri trinn II: selve misbruket eller svindelen begått i en annens navn.

Tallfesting på trinn I sier noe om mulighetsgrunnlaget for identitetstyveri – for eksempel antall stjålne pass, eller personopplysninger på avveie, mens tallfesting på trinn II sier noe om skadeomfanget etter identitetstyveriet - for eksempel antall telefonabonnementer eller forbrukslån som er opprettet på stjålen identitet. Et tredje måte å måle på er såkalt offerstatistikk, dvs. antall personer som er rammet av identitetstyveri. Det er denne tredje måten som vanligvis søkes estimert for å si noe om omfanget av identitetstyveri. Men det er viktig å huske at ett identitetstyveri gjerne resulterer i mange bedragerier.



Identitetstyveri kan både ramme økonomi og omdømme. Men det er særlig økonomiske bedragerier og svindel som har vært viet oppmerksomhet. Blant de som har beregnet omfanget av identitetstyveri, er det uenighet om simpel kortsvindel skal inkluderes. Dersom simpel kortsvindel – dvs at noen har stjålet et bankkort og tar ut penger eller varer på dette kortet – skal regnes som identitetstyveri, tyder tall fra Danmark, USA og Canada på at antallet dobles. Med andre ord kan alvorlig identitetstyveri være like utbredt som simpel kortsvindel. Men fordi hvert enkelt identitetstyveri gjerne resulterer i mange bedragerier, er identitetstyveri langt mer alvorlig. Selv om antallet identitetstyveriofre fortsatt skulle være relativt lavt i Norge, er likevel skadene hvert enkelt offer utsettes for alvorlige målt i psykiske belastninger knyttet til engstelse, bekymringer og oppryddingsarbeide. I de mange tilfellene der ID-tyvene ikke blir tatt, kan misbruket av en annens identitet strekke seg over flere år.

I Identitetstyveri-prosjektet kan vi lese at de har som mål å få etablert et nasjonalt kompetansesenter som skal levere opplæringsstøtte, statistikk og en hjelpelinje for ofre. Videre at det er ønskelig at disse tjenestene blir et spleiselag mellom myndighetene og næringslivet. (NorSIS 2009:19).

Tidsperspektivet er også problematisk når omfanget av identitetstyveri skal estimeres. Noen ofre opplever gjentatte misbruk av sin identitet over år, og noen ofre vil ikke være klar over at de er rammet før lang tid har gått, fordi ID-tyvene gjerne oppretter fiktive adresser som gjør at det kan ta lang tid før offeret blir klar over at han eller hun er rammet. Mange identitetstyveriofre vet ikke hvordan ID-tyven har fått fatt i personopplysningene om dem. Stjålne persondata fra registre kan omfatte viktige opplysninger om hundre tusener av personer. Slike personopplysninger kan selges videre puljevis over lang tid. Det kan altså gå lang tid fra identitetstyveri trinn I til identitetstyveri trinn II finner sted, og enda noe tid før offeret blir oppmerksom på tyveriet.

Et mandat i dette prosjektet var å kartlegge hvilke data som foreligger om identitetstyverier i Norge, og hvor tilgjengelige disse er. Konklusjonen er at det pr. i dag ikke finnes offentlig statistikk som kan si noe om alvorligheten og den totale utbredelsen av identitetstyveri i Norge. Det finnes heller ikke samlet statistikk over antall bedragerier som belastes bedrifter og institusjoner. Svært mange bedrifter og organisasjoner fører ikke slik statistikk, mens noen oppgir at de ikke ønsker å knytte sin bedrift til offentliggjøring av slike tall. Dette fordi det erfaringsmessig vil skape en del ekstrahenvendelser, og ikke minst frykter kommersielle bedrifter - som banker og teleoperatører - at slik offentliggjøring kan skade deres omdømme.

I flere land har det vært gjennomført landsrepresentative offerstudier for å overvåke og estimere omfanget av identitetstyveri. Tallet de kommer fram til, avhenger i stor grad av hvordan fenomenet identitetstyveri operasjonaliseres; om man regner siste år eller overhodet, og om kortsvindel inkluderes eller ikke. Studier fra USA og Canada tyder på at det særlig er tredjepart, bedriftene som har gitt kreditt eller solgt varer og tjenester til en ID-tyv, som i siste instans må ta de økonomiske tapene.

I Norge har TNS Gallup på vegne av NorSIS gjennomført en landsrepresentativ telefonsurvey med 1000 respondenter, der de stilte spørsmål om respondenten hadde blitt utsatt for noen form for identitetstyveri *noen gang*. Omtrent en av tjue, 5,4 prosent, svarte bekreftende. I en tilsvarende undersøkelse i Danmark, men da avgrenset til *siste år*, svarte bare én prosent bekreftende, og enda færre; under en halv prosent, når simpel kortsvindel ble holdt utenfor. Det finnes altså ingen sikre tall over hvor mange som årlig utsettes for alvorlig identitetstyveri i Norge pr. i dag. Flere av våre informanter var engstelige for at fenomenet skulle øke og spesielt gjennom 'hacking' av store dataregistre med relevante personopplysninger.

For å få et bedre bilde av omfang av identitetstyveri i Norge, bør det gjennomføres en grundig og mer detaljert undersøkelse. Ved å gjennomføre en offerstudie, kan man i tillegg til å beregne antall ofre stille spørsmål og samle informasjon om det vi har kalt trinn I og trinn II i identitetstyveriprosessen. Viktige problemstillinger kan være: Hvor mange rammes; hvem er det som i størst grad rammes; hva vet offeret om hvilke personopplysninger som er på avveie og eventuelt hvordan ID-tyven har tilranet seg identiteten; hvor mange bedragerier og omtrent hvor mye har ID-tyven svindlet til seg; hvorvidt offeret selv er økonomisk/omdømmemessig skadelidende og hvor mye tid offeret har brukt på å rydde opp etter identitetstyveriet. I tillegg kan det være interessant å få innsyn i hvilken grad ikke-ofre beskytter opplysninger om seg selv og egen økonomi. Passer det norske folk på sine autentiserende papirer, har de lås på postkassen osv. For å få informasjon om utvikling over tid, vil det være nyttig å komme fram til noen kjernespørsmål som kan gjentas regelmessig over tid. I tillegg til disse offerstudiene bør det arbeides med å innføre et pre-kodet system for registrering av felles statistikk.

Under arbeidet med identitetstyveri har dilemmaet mellom trygghet og effektivitet vært et stadig tilbakevendende tema. Det oppfattes å være vanskelig å forene enkle, effektive systemer med høy brukervennlighet på den ene siden, med trygge, vanntette systemer som stopper misbruk og avslører kriminalitet på den andre siden. Det er for eksempel fortsatt relativt lett for en ID-tyv å bestille mobiltelefoner og opprette telefonabonnementer i falskt navn, sannsynligvis fordi teleselskapene ikke finner det lønnsomt å håndholde strenge kontrollrutiner som ville forhindret dette. Motsatt ser vi at bankene i fellesskap har utviklet et svært godt system for å begrense kortsvindel: For å begrense skadeomfanget av simpel kortsvindel har banknæringen utviklet et svært velfungerende kontrollsystem. I store deler av verden har den minste lille butikk i dag betalingsterminaler som vil avvise stjålne kort, og kundene må identifisere seg med personlige koder. Dette representerer et globalt godt system som *både* fremmer effektivitet og begrenser skadevirkningene av kortsvindelen. *De med sterke insentiver lager gode systemer*. I tilfellet med bankene er det sannsynlig at dersom forbrukerne hadde måttet bære tapene, ville institusjonene mistet mye av insitamentet til å lage dette godt fungerende kontrollsystemet. Eller som tidligere direktør for Forbrukerrådet Stalheims lov lyder: *For å få gode systemer må man plassere ansvaret for at noe kan gå galt hos den aktør som kan påvirke risikoen.*

En rekke tiltak er gjort for å tette huller og redusere muligheten for at identitetstyveri skal finne sted. Det er lite som tyder på at forsøk på identitetstyveri vil avta. Det er derfor nødvendig å fortsette dette arbeidet og å utvikle gode systemer for å redusere både den personlige risikoen og systemrisikoen. Ulike aktører har ansvar her. Folk må bli flinke til å passe på sine identifikasjonspapirer. Og både personer og bedrifter må utvikle gode rutiner og kontrollsystemer. Her vil meldeplikt, statistikkføring og rutiner for håndtering av personlige opplysninger være gode midler i kampen. Sist, men ikke minst, må muligheten for at finansielle systemer kan angripes forebygges. Ansvaret for å lykkes ligger både på den enkelte, på det offentlige og på bedriftene.

Vi har kalt utredningen 'Identitetstyveri i tillitsfulle systemer'. Dette peker tilbake til mange av våre informanters beskrivelse av systemene. Norge kjennetegnes av en tillitsfull befolkning og et åpent samfunn der befolkningen har tilgang til mange av forvaltningens saksdokumenter. Brukervennlige, lønnsomme og effektive systemer bygd på åpenhet og tillit fortrekkes framfor beskyttelse og sikkerhetskontrollerende systemer. Ulempen er at tilliten og åpenheten kan misbrukes. Men er det slik at valget står mellom enkle, effektive, men risikable systemer – mot tunge, trege og trygge systemer?

Litteratur

Angell, Arnt (2009): Nordmenn er spesielt lettlurte. NTB, DN.no: http://www.dn.no/forsiden/politikkSamfunn/article1661937.ece Nedlastet 23.desember 2009.

Arendt (2009): Identitetstyverier og andre e-forbrytelser. *Computerworld* www.idg.no/computerworld/tema/sikkerhet/article149809.ece?mode=print Nedlastet 12.11.2009

CBS News (2009): *60 minutes,* CBS News, 25. oktober 2009 http://www.cbsnews.com/video/watch/?id=5419958n&tag=contentMain;contentBody

CIPPIC (2009): Canadian Internet Policy and Public Interest Clinic, University of Ottawa, Canada. http://www.cippic.ca/identity-theft-2/

Datatilsynet (2009) *Identitetstyveri*. En utredning gjennomført av Datatilsynet for Fornyings-, administrasjons- og kirkedepartementet. datatilsy-net.no/upload/Dokumenter/utredninger%20av%20Datatilsynet/Utredning%20om%20ID-tyveri.pdf Nedlastet 2. desember 2009.

Dow,J. (2000) What is systemic Risk?. Moral Hazard, Initial Shocks and Propagation. I *Monetary and Economic Studies*, December 2000.

Elster, J (2000): Trust and emotions. *Sociologi i dag* – Tillit, no 3/2000. Novus forlag, Oslo

ESS (European Social Survey) (2009): Komparative resultater fra tretti land: «folk flest er til å stole på, eller om en ikke kan være forsiktig nok i møte med andre mennesker». Referert i *Aftenposten* 15.10.09: Sødal, H. & P.A. Johansen (2009): Nordmenn er Europas mest naïve.

Federal Trade Commission (2010): Fighting back against identity theft. http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html Nedlastet 19,02.2009

Federal Trade Commission (2009): Consumer Sentinel Network: DATA BOOK for January – December 2008. (Consumer Complaint-rapport fra februar 2009): http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2008.pdf Nedlastet 19.02.2009

Finansnæringens fellesorganisasjon *Mislighetsstatistikk* 2003-2008.

Fjellheim, H.K. & I. Andersen: Skattelistene er en gave til skurkene. *VGNett* 20.10.2009 http://www.vg.no/nyheter/innenriks/artikkel.php?artid=575485

Gustad, R. (2009): Stjal identitet for å beholde baby. *Nordlys* http://www.nordlys.no/nyheter/article4648442.ece Nedlastet 1.desember 2009

Haakaas, E. (2009): Vil skjerpe sjekk av pass. Falske pass er verktøy for kriminalitet. *Aftenposten* 18.01.2009

Haver, Cecilie K., I, Skaugrud, A.K. Bakker, A. Birkeland og E.A. Eriksen (2009): *"Vennligst ikke stjel meg"*. Prosjektoppgave i MSA 115 Risiko og Samfunnssikkerhet, Universitetet i Stavanger.

Identitetstyveriprosjektet (2009): Se NorSIS.

ITRC (2008): Identity Theft Resource Center: Identity Theft: The Aftermath 2009. www.idtheftcenter.org

Javelin Strategy & Resarch (2008, 2009): Identity Fraud Survey Report. www.javelinstrategy.com/research

Kim, Rachel (2008) *Identity Fraud Survey Report, Consumer Version. How Consumers can protect themselves*. Nettversjon. Javelin Strategy & Research, California. www.javelinstrategy.com/research

Kim, R & M.T. Monahan (2008): *Identity Fraud Survey Report: Identity Fraud Continues to Decline, But Criminals More Effective Using All Channels.* Javelin Strategy & Research, California www.javelinstrategy.com/research

Knudsen (2009): Norske bankkort rammet i innbrudd. *NRK.no* www.nrk.no/nyheter/okonomi/1.6816620 nedlastet 01.12.2009

Kruize, P. (2009): *Identitetstyveri*. Københavns Universitet. Det Juridiske Fakultet.

McNally, M.M. & G. R. Newman (2008): Charting the Conceptual Landscape of Identity Theft. In: McNally & Newman (2008): *Perspectives on Identity Theft.* Crime Prevention Studies. Vol.23, Monsey: Criminal Justice Press; Devon: Willan Publishing Cullompton, pp.33-55.

Monahan, M. & R. Kim (2009): *Identity Fraud Survey Report. Identity Fraud on the Rise. But Consumer Costs Plummet as Protections Increases.* Javelin Strategy & Research, California www.javelinstrategy.com/research

NorSIS (2009): *Identitetstyveri- Strategi og tiltaksplan for identitetstyveriprosjektet*. Godkjent av styringsgruppen 19. november 2009. www.idtyveri.info

OECD (2009): *Online Identity Theft*. www.sourceoecd.org/governance/9789264056589

Slettemeås, D. (2004): Grunnlagsdokument. Forbrukervinkling på Public Key Infrastructure (PKI). SIFO oppdragsrapport nr. 8 – 2004.

Slettemeås, D. (2007): Forbrukernes stilling i informasjonssamfunnet. SIFO oppdragsrapport nr. 15 - 2007

Slettemeås, D. (2009): Forbrukernes digitale mestring. SIFO prosjektnotat nr. 10-2009. SIFO, Oslo.

SpendOnLife (2009): Child Identity Theft. www.spendonlife.com/guide/child-identity-theft

SpendOnLife (2009): Identity Theft Statistics. www.spendonlife.com/guide/identity-theft-statistics

Sproule, S. & N. Archer (2008): Measuring Identity Theft in Canada 2008: Consumer Survey – Working Paper #23, www.merc-mcmaster.ca/working-papers/measuring-identity-theft-in-canada-2008-consumer-survey, McMaster University, Ontario, Canada. Nedlastet 15.12.2009

Sødal, H. & P.A. Johansen (2009): Nordmenn er Europas mest naïve. *Aftenposten* 15.10.09. http://www.aftenposten.no/nyheter/iriks/article3321677.ece/
Nedlastet 23. desember 2009

Task Force Report (2008): *The President's Identity Theft Task Report* September 2008 (2008): http://www.identitytheftlabs.com/identity-theft/heartland-hackers-largest-id-theft-case-in-history-sees-perpetrators-indicted/ http://breachalerts.trustedid.com/?p=230 Accessed on 08.12.2009)

Uncletaz.com (2009): Forfalsking: Kripos offisielle hjemmeside.
http://uncletaz.com/norsktaz/kripos/