

Identitetstyveri



Strategi og tiltaksplan for identitetstyveriprojektet

Prosjekteier: Norsk Senter for Informasjonssikring - NorSIS

Godkjent av styringsgruppen 19.november 2009

Innhold

1	Innledning.....	3
2	Oppbygging av dokumentet.....	4
3	Presentasjon av prosjektet.....	4
3.1	Om initiativtagerne, Security Valley og NorSIS.....	4
3.2	Formålet med prosjektet.....	4
3.3	Prosjekt mål	5
3.4	Aktører	5
4	Definisjoner	6
4.1	Prosjektets definisjoner	6
4.2	Andre relevante definisjoner	7
5	Forslag til tiltak.....	8
5.1	Forebygging	9
5.2	Assistanse til ofre og tilbakeføring til normalt tilstand	9
5.3	Lovhåndhevelse	10
6	Drøfting om og begrunnelse av forslag	11
6.1	Tiltak 1 – fødselsnummer og organisasjonsnummer	11
6.1.1	eID og Borgerkort.....	11
6.1.2	Felles infrastruktur for eID i offentlig sektor.....	11
6.1.3	Organisasjonsnummer	12
6.2	Tiltak 2 – ansvar.....	12
6.3	Tiltak 3 – valideringskrav	13
6.4	Tiltak 4 – kredittopplysning	14
6.4.1	Sperretjeneste.....	14
6.4.2	”Rødt flagg”	15
6.4.3	Tiltak og fremdriftsplan.....	15
6.5	Tiltak 5 - Oversikt over hvor det er stiftet gjeld.....	16
6.5.1	Tiltak og fremdriftsplan.....	17
6.6	Tiltak 6 – informasjonstiltak til virksomheter.....	17
6.7	Tiltak 7 – generell offentlighet og skatteopplysninger	18
6.8	Tiltak 8 – informasjonstiltak til befolkningen.....	18
6.9	Tiltak 9 – hjelpelinje	19
6.9.1	ID-tyveriforsikring.....	19
6.10	Tiltak 10 – kompensasjon	20
6.11	Tiltak 11 – statistikk.....	21
6.12	Tiltak 12 – opplæring og dialog.....	22
6.13	Tiltak 13 – oppfølgingsansvar.....	22
6.14	Tiltak 14 – etterforskning.....	22
6.15	Tiltak 15 – tiltaksplan	22
7	Om identitetstyveri og utviklingstrekk	23
7.1	Hvorfor oppstår identitetstyveri?	23
7.2	Hvordan velges offeret ut?.....	23
7.3	Hvem er aktørene?	24
7.4	Kilder til objektiv informasjon.....	24
7.5	Hvor utsatt er norske borgere?.....	25
7.6	Utviklingen i andre land.....	26
8	Det emosjonelle og samfunnsøkonomiske aspekt	27
9	Konklusjon.....	29
10	Kilder	30

1 Innledning

Identitetstyveri er en av verdens sterkeste voksende kriminalitetsformer. Utviklingen skjøt fart ved årtusenskiftet, ledet an av utviklingen i USA. Den sterkeste utviklingen er påvist i engelskspråklige land. Det kan også skyldes at disse landene har bedre statistisk underlag. I Norge må man basere seg på antagelser, da tilsvarende statistisk underlag ikke er å oppdrive. Det synes likevel å være en utbredt oppfatning at identitetstyveri er økende, men foreløpig holder seg på et moderat nivå. Det skremmende er likevel hvor rask utviklingen økte i USA. Hele tusen prosent i løpet av en femårs periode.

Innledningsvis presiseres det at begrepet "identitetstyveri" kan være noe misvisende. Strengt tatt kan man ikke stjele andres identitet, men man forleder en tredjepart til å tro at man besitter en annens aktiva, rettigheter og plikter. I denne prosessen gir man seg ut for å være vedkommende. Fornærmede er i de fleste tilfeller helt ukjent for gjerningsmannen og er således kun et "relé" for gjennomføring av kriminelle handlinger. Offeret er valgt ut av kriminelle som gjennom kyniske handlinger ønsker å skaffe seg kontroll over vedkommendes aktiva eller ubenyttet kredittverdighet. I andre tilfeller kan handlingene ta sikte på å skaffe kontroll over immaterielle verdier.

Identitetstyven utnytter svakheter i vår sosiale infrastruktur. Vedkommende tar utgangspunkt i en normal forventning om tillit og troverdighet. En person som ønsker å få gjennomført en handling eller en økonomisk transaksjon, forventes å ha rettighet til det. Det er også grunnen til at kreditor har presumpsjon for at det faktisk er offeret som har gjennomført en handling, det være seg bruk av kredittkort, opptak av kreditt eller liknende.

De ofre ID-tyveriprojektet og dets deltagende aktører har vært i kontakt med, forteller om en følelse av sterk mistillit fra kreditors side. Det er videre tilfeldigheter som avgjør om saken deres får prioritering hos politiet. Hvis en sak likevel får nødvendig oppmerksomhet, er offeret i beste fall redusert til et vitne. De får gjennomgående et inntrykk av at det har lite hensikt å gå til egne, rettslige skritt mot gjerningsmann. I de tilfellene politiet har etterforsket saken og gjerningsmann er kjent, kan kreditorene sjelden gjøre annet enn å akseptere at det er de som er blitt lurt. De velger derfor stort sett å dekke de direkte økonomiske tapene. De dekker likevel ikke offers indirekte kostnader - tiden vedkommende har brukt til å rydde opp, og tap av økonomisk omdømme. Flere år etter slike hendelser kan ofre slite med sin kredittverdighet.

Den 26. september 2008 undertegnet President Bush en lov som kriminaliserer flere former for identitetstyveri samt gir ofre et betydelig bedre rettsvern. Blant annet kan ofre kreve erstatning for tiden vedkommende har brukt på å rydde opp i sin kredittverdighet. Lovprosessen har vært lang og gjenstand for flere runder hvor et økende antall politikere har tatt til orde for et sterkere vern av ofrene.

Historiene rundt identitetstyveri er ikke avgrenset til private forhold. Også næringsvirksomheter rammes av dette fenomenet. I slike sammenhenger benyttes ofte firmaattester og virksomheten settes i urettmessig gjeld. Likeledes er problematikken relevant i forhold til ikke økonomiske forhold som industrispionasje, korrupsjon og informasjonstyveri. Sistnevnte problemstillinger krever en annen analytisk tilnærning. Dette dokument er avgrenset til private rettssubjekter.

2 Oppbygging av dokumentet

I kapittel 3 presenteres ID-tyveriprojektet, dets deltagende aktører og prosjektets mandat via prosjekteier NorSIS.

I kapittel 4 defineres identitetstyveri og identitetssvindel.

I kapittel 5 fremsettes et forslag til en helhetlig tiltakspakke. Forslagene er hentet fra en prosess gjennomført i ID-tyveriprojektets regi våren 2009 samt et grundig utredningsarbeid som er gjennomført i USA på oppdrag fra presidenten.

I påfølgende kapittel 6 underbygges forslagene.

I kapittel 7 gis en nærmere presentasjon av hva identitetstyveri er, hvordan det oppstår og hvilke trender man ser. Kapittel 8 drøfter emosjonelle og samfunnsøkonomiske aspekter rundt identitetstyveri.

Kapitlene 7-8 er ment for lesere som har lite kjennskap til identitetstyveri, dets historikk, utviklingstrekk, sosiale og sosialøkonomiske virkninger, hvordan og hvorfor slik kriminalitet oppstår.

3 Presentasjon av prosjektet

3.1 Om initiativtagerne, Security Valley og NorSIS

Det har i perioden fra 2001 og frem til i dag vært jobbet systematisk på Gjøvik med å bygge et sammensatt og komplett sikkerhetsmiljø med bedrifter, offentlige aktører og utdannings-/FoU-aktører innen informasjonssikkerhet.

Norsk Senter for Informasjonssikring, ([NorSIS](#)) er en del av regjeringens helhetlig satsing på informasjonssikkerhet i Norge. NorSIS jobber for at informasjonssikkerhet skal bli en naturlig del av hverdagen.

Målgruppen er norske virksomheter i privat og offentlig sektor herunder kommunene. NorSIS skal så langt som mulig også imøtekomme innbyggernes behov. Alle samfunnsgrupper skal kunne dra nytte av NorSIS sine tjenester.

NorSIS bygger informasjonssikkerhet ved å:

- Bevisstgjøre om trusler og sårbarheter
- Opplyse om konkrete tiltak gjennom nyheter, råd og veiledninger
- Påvirke til gode holdninger

[Security Valley](#) og NorSIS tok initiativet til å samle nødvendige ressurspersoner for å begynne kampen mot den nye kriminalitetsformen, identitetstyveri og svindel. NorSIS er prosjekteier og jobber ut fra tilsagnsbrev fra Fornyings- og administrasjonsdepartementet (FAD) og har således mandat til å etablere denne type prosjekter.

3.2 Formålet med prosjektet

Formålet med prosjektet er å redusere/bremse omfanget og konsekvensene av identitetstyverier og misbruk av personopplysninger.

3.3 Prosjektmål

Definere tiltak og virkemidler som forebygger og reagerer på identitetstyverier og svindel som følge av slike tyverier.

3.4 Aktører

Aktive deltagere	Andre interessenter
Affinion International	Abelia
Apropos Internett	Barne- og likestillingsdep. (BLD)
Brønnøysundregistrene	Data-Secure
Datatilsynet	Fornyings- adm og kirkedep. (FAD)
DnB NOR	Handel og Servicenæringens Hovedorganisasjon (HSH)
Dun & Bradstreet	Internett- og Telebransjens Anti-Kriminalitets Tiltak (ITAKT)
Experian (tidl. Credit Inform)	Justis- og politidepartementet
Finansmarkedsfondet	Kripos
Finansnæringens Hovedorganisasjon	Norsk Arbeids og Velferdsetat (NAV)
Fokus Bank	Politidirektoratet (POD)
Folkeregisteret (Skattedirektoratet)	Post og Teletilsynet (Nettvett)
Forbrukerombudet	Skandiabanken
Gjøvik kunnskapspark	Sparebankforeningen
Help Forsikring	
Høgskolen i Gjøvik	
IKT-Norge (NorTib)	
Lindorff	
Lindorff Decission	
Norsk Senter for Informasjonssikring	
Næringslivets sikkerhetsråd	
Posten Norge	
Security Valley	
Skattedirektoratet	
Steria	
Universitetet i Oslo (UiO)	
Veolia Miljø – Sikkerhetsservice	
Økokrim	

4 Definisjoner

4.1 Prosjektets definisjoner

Prosjektet la seg på følgende definisjon etter flere gjennomganger i forprosjektfasen i 2008:

Identitetstyveri

Innsamling, besittelse, overføring, reproduksjon eller annen manipulering av 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.

Definisjonene fra identitetstyveriprojektet bygger i all hovedsak på arbeidet til CIPPIC¹, og er ment som et utgangspunkt snarere enn endelig.

¹ www.cippic.ca/identity-theft-2/ (Det kanadiske prosjektet)

4.2 Andre relevante definisjoner

I 2007 gjennomførte CIPPIC et større forskningsprosjekt knyttet til identitetstyveri. CIPPIC² valgte da å splitte begrepet i identitetstyveri og identitetssvindel. (Sproule & Archer 2007)

Med identitetstyveri menes:

“The unauthorized collection, possession, transfer, replication or other manipulation of another person’s personal information for the purpose of committing fraud or other crimes that involve the use of a false identity.”

Med identitetssvindel menes:

“The gaining of money, goods, services, other benefits, or the avoidance of obligations, through the use of a false identity.”

Datatilsynet definerte sommeren 2007 identitetstyveri som:

Alle situasjoner “(...) hvor en person, uten samtykke fra rette vedkommende, enten: helt eller delvis er i stand til å utføre en eller annen form for uønsket transaksjon i annen persons navn, eller skaffer seg tilgang til ressurser tilhørende andre, eller urettmessig tilegner seg rettigheter som tilhører andre vil være identitetstyveri.”

Tilsynet la seg bevisst på en vid definisjon, selv om de erkjente at den verken var særlig presis eller entydig. (Datatilsynet 2009, side 19)

I definisjonen ligger det at det må foreligge en eller annen vinning for gjerningsmannen. Vinningen ser ikke ut til å trenge å være av ren økonomisk karakter, men det må være i form av noe som denne personen ikke ville fått tilgang til med sin reelle identitet. Definisjonen sier videre at det er tilstrekkelig å være i besittelse av en annens identitet for at det skal kunne kalles et identitetstyveri.

En arbeidsgruppe ledet av Finansnæringens Hovedorganisasjon leverte en rapport i oktober 2008, der de definerte identitetstyveri på følgende måte:

Med identitetsmisbruk menes uberettiget bruk av personlige opplysninger. Arbeidsgruppen legger videre til grunn følgende definisjoner:

1) Misbruk av reell identitet: Urettmessig tilegnelse av et individs personopplysninger eller et foretaks firmaopplysninger, som så misbrukes. Dette skjer gjerne ved:

- Identitetstyveri/ stjålet identitet: Dette er forhold der ett individ urettmessig kopierer en reell persons personalia, eller gjennom forfalskede dokumenter klarer å utgi seg for å være en bemyndiget representant for et firma og gjennomfører handlinger (ofte bedragerier) i vedkommendes eller firmaets navn. Arbeidsgruppen er ikke kjent med at det eksisterer klare, entydige eller anerkjente definisjoner av begrepet identitetstyveri, verken nasjonale eller internasjonalt.
- Forfalsket identitet: Dette er forhold der en person har endret et eller flere opprinnelige reelle dokument/ personalia for å tilpasse dette til egen person eller firma.

2) Fiktiv identitet:

- Dette er forhold der en person har opprettet en ny identitet, basert på fullstendig falske personalia. En slik identitet kan bygge på dokumentasjon som er vanskelig å verifisere, eks. utenlandske dokumenter som ikke er lett gjenkjennelige av norske offentlige myndigheter. Identiteten kan være opprettet ved å fremvise et forfalsket dokument eller den kan være registrert i et offentlig register. Dersom den fiktive identiteten er registrert inn i folkeregisteret, vil andre offentlige myndigheter lett utstede ekte identitetsdokumentasjon basert på den ukorrekte informasjon som ligger i registeret.
- Det samme kan gjelde firmaer som registreres i Brønnøysund, også der er man avhengig av at opplysningen innregistreringen bygger på er korrekte, for at man kan være sikker på at firmaet eksisterer.

5 Forslag til tiltak

ID-tyveri-prosjektet presenterer her en helhetlig tiltakspakke. Av pedagogiske hensyn er forslagene presentert først, mens begrunnelsene kommer i påfølgende kapittel. Forslagene er organisert i tre tiltaksområder:

- Forebygging
- Bistand til fornærmede og tilbakeføring til normaltilstand
- Lovhåndhevelse

Oppbyggingen er basert på modellen til den amerikanske "Identity Theft Task Force Members" nedsatt av President Georg W. Bush i 2006. Gruppen har i en rapport³ oppsummert sine forslag, i alt 31 anbefalinger. Flere av disse er allerede satt i verk. Prosjektet har trukket veksler på en rekke av de forslag gruppen har fremmet.

Prosjektet vil føre egen argumentasjon for forslagene, men vil også vise til kildedokumentene for ytterlig underbygging av forslagene. Den amerikanske gruppen, som har bestått av ledere på høyt nivå hos i alt 15 departement, direktorat og andre forvaltningsenheter, har gjort et meget grundig arbeid. Problemstillingene det tas utgangspunkt i er de samme, selv om rammebetingelsene er noe ulik. Prosjektet mener at det foreligger en del særnorske problemstillinger som må vurderes. Etter prosjektets vurdering trekker de norske rammebetingelsene i skjerpene retning. Eksempler på dette er kravet om offentliggjøring av skatteinformasjon på individnivå og at bruk av fødselsnummer som en bekreftelse på identitet har blitt sedvane flere steder. I tillegg vises det til at vi har en høy andel nettbank kunder og 1,5 millioner norske brukere registrert på Facebook. Ingen stoler mer på andre personer eller er mindre skeptiske i møte med andre mennesker enn nordmenn, ifølge tall fra European Social Survey (ESS) som ble publisert i oktober 2009. Legge inn link

Det henledes spesielt til de foreslåtte tiltak 2 og 3. Disse er meget viktige elementer for å sikre en tilstrekkelig motivasjon hos næringslivet til å balansere hensyn. I økonomisk terminologi vil tiltakene bidra til å inkorporere de *eksterne kostnadene* ved mangelfull sikkerhet i virksomhetens egne regnskaper. Dersom dette ikke gjøres, vil rasjonelle beslutningstakere ikke ta hensyn til eksternaliteter⁴ virksomheten burde bære ansvaret for.

Utover det vil alle de foreslåtte tiltak kunne bidra til å redusere risikoen for at identitetstyveri utvikler seg til å bli et alvorlig problem i Norge. Prosjektet har merket seg endringene i straffeloven av 19. desember 2008⁵, hvor kriminalisering av identitetstyveri tydeliggjøres. Etter prosjektets oppfatning er denne lovendringen et viktig bidrag i forhold til adekvat lovhåndhevelse.

³ Rapporten "The President's Identity theft Task force report", publisert september 2008. Link gov.

⁴ Eksternaliteter - er innen samfunnsøkonomi en betegnelse på samfunnsøkonomiske gevinster eller kostnader ved produksjon eller konsum som enkeltaktørene ikke blir godskrevet/belastet økonomisk for i markedet, og som de dermed heller ikke tar hensyn til.

⁵ Den nye bestemmelsen om identitetskrenkelse, § 202 Identitetskrenkelse, vil gi straff for den som tar en annens identitet, opptrer med en annens identitet eller opptrer med en identitet som er lett å forveksle med en annens. I tillegg omfattes det å sette seg i besittelse av en annens identitetsbevis. Identitet kan omfatte navn, fødselsnummer, organisasjonsnummer, e-postadresse eller andre opplysninger som alene eller sammen med annen informasjon kan identifisere en fysisk eller juridisk person.

5.1 Forebygging

Tiltak 1 – fødselsnummer

En kritisk gjennomgang og reduksjon i unødvendig bruk av fødselsnummer i offentlig og privat sektor.

Tiltak 2 – ansvar

Påvirke regelverket slik at det til enhver tid er tidsriktig i forhold til problemstillingen. Klargjøre hvilke krav som stilles til debitor og kreditor i en prosess der det oppstår tvist om krav grunnet påstand om ID-tyveri.

Tiltak 3 – valideringskrav

Sørge for plikt til legitimering og at det gjennomføres validering (eksempelvis innføring av Borgerkortet) av identifikasjonspapir dersom gjeld, kreditt eller andre fordringer skal stiftes (Registeroppslag).

Tiltak 4 – kredittopplysning

På virke myndighetene til å stille krav om at det må tilbys to tjenester for den registrerte som et ledd i kredittopplysningsvirksomheten: "Rødt flagg" og felles sperretjeneste.

Tiltak 5 – oversikt over hvor det er stiftet gjeld

Vurdere en mer effektiv bruk av eksisterende systemer framfor å etablere en egen oversikt

Tiltak 6 – informasjonstiltak til virksomheter (private og offentlige)

Bevisstgjøre om ansvar, beskrive trusler og opplyse om viktige sikringstiltak for å sikre personopplysninger som behandles av virksomhetene.

Tiltak 7 – generell offentlighet og skatteopplysninger

Innføre plikt til å fjerne navn eller andre direkte identifiserende elementer ved publisering av dokumenter etter offentlighetsloven. Innskerpe eller begrense offentliggjøring av inntekts- og formuesopplysninger direkte på individnivå.

Tiltak 8 – informasjonstiltak til befolkningen

Gi allmenn informasjon til befolkningen om hvordan forebygge identitetstyveri og behov for aktsomhet ved indikasjoner på identitetstyveri.

5.2 Assistanse til ofre og tilbakeføring til normalt tilstand

Tiltak 9 – hjelpelinje

Opprette en hjelpelinje for ofre som kan assistere med råd og veiledning. Veilederne bør ha spesialopplæring i håndtering av slike saker og et bredt kontaktnett mot politi, næringsliv og andre relevante enheter.

Tiltak 10 – kompensasjon

Utvikle regelverk som gir offeret full kompensasjon for påført skade, herunder også brukt tid samt få slettet urettmessige fordringer.

5.3 Lovhåndhevelse

Tiltak 11 – statistikk

Etablere en enhetlig statistikk for identitetstyveri. Innføre supplerende meldeplikt for finanssektoren, hjelpetelefon og andre instanser som mottar henvendelse ved identitetstyveri.

Tiltak 12 – opplæring og dialog

Bidra til systematisk opplæring av ansatte i politiet til å håndtere identitetstyveri. Bidra til opplæring av IKT personell til å forhindre uautorisert utlevering av personopplysninger. Økt deling av informasjon mellom næringslivet, forvaltningen og politiet.

Tiltak 13 – oppfølgingsansvar

Tildele ansvar for oppfølging av identitetstyveri til et organ i statsforvaltningen (etter den amerikanske modellen).

Tiltak 14 – etterforskning

Henstille Justisdepartementet å utrede organisering vedr. etterforskning av identitetstyveri. politiet. Problemstillingen er spesielt relevant hva gjelder organisert kriminelle som opererer i flere politidistrikt. Det bør vurderes et formalisert samarbeid med private virksomheter som har ekspertise vedrørende dataetterforskning.

Tiltak 15 – tiltaksplan

Henstille Justisdepartementet om å få utarbeidet en tiltaksplan for justissektoren som bidrar til at identitetstyveri stanses, avverges, etterforskes og dømmes. En tiltaksplan bør omfatte nødvendige tiltak hos politiet, domstolene og kriminalomsorgen, slik som lovverk og strafferammer tilpasset dagens kriminalitetstyper

6 Drøfting om og begrunnelse av forslag

6.1 Tiltak 1 – fødselsnummer og organisasjonsnummer

Ukontrollert spredning og tilhørende uautorisert innhøsting av personopplysninger representerer den viktigste enkeltrussel i risikobildet. Personopplysninger vil først ha verdi når disse er systematisert i forhold til identitetstyvens behov. I likhet med preferansen for de fleste andre som behandler personopplysninger, vil innsamling og systematisering av informasjonen på en tverrsektoriell unik identifikator være å foretrekke. Det er derfor fødselsnummer er så attraktivt for identitetstyven. Kjenner han dette nummeret er det enklere å skaffe nye, supplerende opplysninger. Det er også lettere å systematisere og bearbeide ny illegalt tilegnet informasjon dersom han får tilgang til det. Man må huske på at kjøp og salg av personopplysninger utgjør en viktig del av disse kriminelle aktiviteter. Samarbeid med utro tjenere både i offentlig sektor og privat næringsliv kan utgjøre en del av disse aktivitetene. Identitetstyveri er fremfor alt en kriminalitetsform som kan ha elementer av langsiktige perspektiver. De kriminelle kan sitte med et stort utvalg av mulige ofre og slår kun til når forholdene ligger til rette for det.

Fødselsnummeret er en statsautorisert, varig og entydig identifikator. Det er beskrevet tidligere i dokumentet hvorfor unødvendig bruk og spredning av dette nummeret representerer et problem. Prosjektet har merket seg at den amerikanske gruppen har foreslått og fått gjennomslag for betydelige reformer i USA hva gjelder bruk av amerikanernes fødselsnummer (Social Security Number). Det har vært gjennomført endringer innen skattemyndighetenes bruk, helsesektoren, forsvaret, privat næringsliv, lokale myndigheter med videre.

6.1.1 eID og Borgerkort

En rekke offentlige elektroniske tjenester på Internett krever innlogging i form av en elektronisk identitet (eID). Direktoratet for forvaltning og IKT (Difi) har ansvaret for å forvalte og videreutvikle MinID, og for å etablere en felles infrastruktur for eID i offentlig sektor.

MinID er en offentlig eID som allerede i dag kan brukes for å logge inn på nærmere 50 tjenester fra statlige etater, for eksempel Minside og Altinn. For å bruke MinID trenger du et PIN-kodekort. Rundt fire millioner innbyggere mottok PIN-kodekort i begynnelsen av desember 2008.

6.1.2 Felles infrastruktur for eID i offentlig sektor

Torsdag 26. november 2009 ble den nye versjonen av MinID lansert, som den første elektroniske ID (eID) som benytter seg av ID-porten - den nye, felles plattformen for eID i offentlig sektor. Dette er et viktig skritt for å redusere risiko for å bli utsatt for ID-tyveri.

Innloggingen med MinID har fått et bedre brukergrensesnitt med mer hjelpeinformasjon. En rekke nye detaljer er forbedret, som forenklede prosedyrer ved tap av passord og bestilling av PIN-koder.

– MinID er blitt sikrere ved at brukerne nå får tilsendt brev ved opprettelse av ny bruker og SMS-varslings ved endringer i brukerprofilen. Dette skal gjøre det lettere å avdekke forsøk på ID-tyveri, forteller Hans Christian Holte, direktør i Difi.

ID-tyveriprojektet er meget positivt til det arbeidet som er gjort i DIFI. Det er positivt at flerfaktorautentisering nå er tilbudt. Ved rebestilling av passord når dette er glemt, sendes det nå en engangskode på sms til forhåndsdefinert mobilnummer. Ved innlogging med denne koden går det en epost til definert epostadresse (det står anbefalt på nettsiden at man ikke bør benytte en epostadresse som kan nås fra mobiltelefonen). Når denne engangskoden, som har ti minutters varighet, tastes inn, får man mulighet for å registrere nytt permanent passord samt tilgang til egen profil og tjenester.

Vi forventer nå en videre satsing som omfatter innlemming av alle andre offentlige enheter som håndterer personsensitiv informasjon slik at vi ikke blir sittende igjen med åpenbare hull i denne nye infrastrukturen.

6.1.3 Organisasjonsnummer

Organisasjonsnummer er og skal være en offentlig opplysning. Organisasjonsnummeret er en unik identifikator for det enkelte selskap i næringslivet. Flere tilfeller har vist at det er varierende grad av kontroll med både person- og selskapsopplysninger før inngåelse av kreditt. Ofte er kjennskap til dette nummeret nok til å sikre seg kredittverdighet i selskapets navn. Med en kopi av firmaattesten stiller man enda sterkere. På lik linje med fødselsnummeret må det gjøres en grundig vurdering av håndteringen når det gjelder organisasjonsnummer samt se på opplysningstiltak for å redusere omfanget av svindel med disse.

Det bør vurderes et virksomhetssertifikat med eID på lik linje med det planlagte borgerkortet. Oppdatering, roller, definert tidsperioder, automatisk utløpsdato etc. er elementer som må vurderes lagt inn i dette kortet.

6.2 Tiltak 2 – ansvar

Hvem har eierskap til problemet når en handling eller disposisjon bestrides? Sagt på en annen måte, hvem bør bære ansvaret hvis noen utnytter en annens identitet? De kriminelle har utnyttet fornærmedes identitet til å skaffe seg selv verdier og påfører samtidig langsiktig skade på fornærmedes troverdighet og kredittverdighet.

De fleste vil sikkert konkludere med at dette avhenger av om offeret kan lastes for forholdet. Dersom vedkommende har delt koder, påloggingsinformasjon eller andre hemmeligheter bærer offeret et ansvar. Men gitt at vedkommende ikke har det, stiller saken seg i et annet perspektiv. Prosjektet erfarer at man trekker det individuelle ansvaret vel langt når det kreves at en fordring som er offeret uvedkommende, blir vedkommendes problem. At noen har skaffet seg urettmessig tilgang til varer eller tjenester ved å manipulere tredjeperson bør ikke medføre at offeret eier problemet.

Av markedsføringsloven § 11 følger et generelt prinsipp om at det er den som har et krav som må dokumentere at det foreligger en gyldig avtale med den som kravet rettes mot. Bestemmelsen gjelder både for krav som rettes mot forbrukere og til næringsdrivende, organisasjoner eller offentlige myndigheter. Så lenge den kravet rettes mot kan vise til forhold som sannsynliggjør at vedkommende ikke har inngått en gyldig avtale med kravshaver, kan ikke kravet drives inn. Utfordringene i denne forbindelse vil i stor grad være knyttet til fremskaffelse og vurdering av bevis for at avtaler som er inngått med en næringsdrivende er en følge av id-tyveri. Her kommer det også inn spørsmål om hvilke rutiner den næringsdrivende bør ha for å minske risikoen for at ID-tyver inngår ugyldige avtaler.

Etter prosjektets syn er det ikke unaturlig at det er sterk korrelasjon mellom hvem som bærer et ansvar og hvem som sikrer seg. Hvis ansvaret i stor grad legges på offeret, vil næringslivet ha få insentiver til å sikre seg. Hvis den enkelte bærer ansvaret, vil vedkommende måtte sikre seg ekstremt godt. På tross av det, vil man altså ikke være trygg. Det sørger blant annet de andre spillerne for: Staten, kommunene og næringslivet. De sørger alle for både legale og tilfeller av utilsiktede lekkasjer av personopplysninger. Selv om dette i seg selv er kritikkverdig, må vi i hvert fall stramme til når det gjelder mulighetene for å benytte opplysningene, som gjøres tilgjengelig.

Ansvaret bør tydeligere plasseres hos fordringshaverne. Først da vil disse ha bedriftsøkonomiske insentiv til å sikre transaksjonene bedre. Det er her sakens kjerne ligger. Ligger bevisbyrden hos fordringshaver må vedkommende forsikre seg om at transaksjonen på forsvarlig måte kan knyttes mot debitor. Fordringshaverne har videre muligheter til å begrense eget ansvar om andre virksomheter kan lastes for forholdet.

Prosjektet ser at en fordring kan være omstridt ved at en debitor ikke har til hensikt å betale sin gjeld. Tydeliggjøring av ansvaret vil samtidig binde rettmessig debitor tettere til kravet, spesielt dersom plikten til validering av identifikasjonsdokument realiseres (se tiltak 3).

6.3 Tiltak 3 – valideringskrav

Identifikasjonsdokumenter på avveie representerer en viktig faktor i trusselbildet. Dersom identitetstyven har uautorisert tilgang til personopplysninger og uautorisert tilgang til instrumenter (pass, førerkort og tilsvarende dokumenter) representerer det en betydelig utfordring. Det trenger likevel ikke å bety at identitetstyven kan nyttiggjøre seg disse til egen vinning. Selv om de dyktigste kriminelle evner å manipulere tredjepart uten tilgang til identitetspapirer, vil som hovedregel slike instrumenter være involvert.

Offentliggjøring av skatteinformasjon på individnivå samt en utvidelse av offentlighetsloven, legger ikke forholdene til rette for beskyttelse av personsensitiv informasjon. Videre, en rekke virksomheter har mangelfull kontroll over opplysningene de forvalter.

Gitt de vanskelige rammebetingelsene som skisseres ovenfor, synes det mest rasjonelt å gjøre det vanskeligere å nyttiggjøre seg personopplysningene. Selv om ulovlig innsamling og foredling av personopplysninger krenker offerets personvern, er det likevel verre om opplysningene kan misbrukes til å kompromittere vedkommende ytterligere. Dersom identitetstyver ikke kan nyttiggjøre seg personopplysninger, vil det svekke både verdien av illegalt innsamlede opplysninger og aktørens interesse for å samle disse inn.

Prosjektet er opptatt av å gi rett aktør insentiv til handling. Dersom bevisbyrden i større grad forskyves vil insentiv utløses hos den som har mulighetene for å løse problemet.

En samhandling som innebærer inngrep i økonomiske rettigheter og plikter forutsetter normalt en form for identifisering, enten ved fysisk legitimasjon eller ved en egnet elektronisk ID (eID). Etter prosjektets syn bør kreditor ha et ansvar for å sjekke om legitimasjonen er gyldig. Når det gjelder fullverdig eID, er det allerede på plass egnede løsninger (valideringsløsninger). Prosjektet legger til grunn at de midlertidige løsningene på nivå⁶ 1-3 fases ut. I prinsippet er det derfor behov for å etablere tilsvarende for fysiske identitetsbevis. Prosjektet foreslår imidlertid at valideringen snus på hodet, ved at det er ugyldige fysiske identifikasjonsdokumenter som registreres.

Det kan etableres et oppslag i register over identifikasjonsdokumenter som er meldt tapt eller stjålet. Kun identifikasjonsdokumentets løpenummer skal sendes over til registeret. Det etableres mulighet for kontroll via telefon, via elektroniske oppslag eller strekkode.

ID-tyveriprojektet har mottatt et svar fra Datatilsynet om at dette ikke strider mot POL §8. Det er videre sendt forespørsel til politidirektoratet og Vegdirektoratet om dette.

En validering vil si at man bekrefter ekthet og at identitetsbeviset ikke er meldt tapt av rettmessig innehaver. Slike tjenester vil likevel ikke bli benyttet om ikke ansvaret plasseres tydeligere der det hører hjemme. Nå er det vanskelig å fange alle ønskede aspekter i forhold til fysiske identitetsbevis. Dersom ekthet skal slås fast, krever det langt mer inngripende og kostnadsdrivende løsninger enn kun kontroll av om dokumentet er meldt tapt. Prosjektet foreslår at man avgrenser seg til en kontroll om et konkret identitetsbevis er meldt tapt eller stjålet. En slik løsning vil ikke fange opp falske identitetsbevis, men vil uansett være et vesentlig bidrag. Kvalitetssikring/kontroll ved innmelding må tydeliggjøres.

⁶ Det vises til kravspesifikasjonene for eID og eSignatur utarbeidet i regi av Fornyings- og administrasjonsdepartementet.

6.4 Tiltak 4 – kredittopplysning

Forslaget til tiltak er todelt, henholdsvis en fullstendig sperring av kreditt hos kredittopplysningsselskapene samt en modus som gir informasjon om at den registrerte anser seg særlig utsatt for identitetstyveri. Sistnevnte bør administreres hos Folkeregisteret. Et ”rødt flagg” innebærer at det kommer opp varsel hos kredittopplysningsbyråene og andre behandlere av personopplysninger. Det innebærer en særskilt og mer inngående verifisering ved økonomiske transaksjoner. Prosjektet kan ikke på det nåværende tidspunkt spesifisere hva en slik inngående verifisering bør bestå i, men viser til at slike tiltak allerede er implementert i Canada. Det bør kunne trekkes vekslers på disse erfaringene. Tilbudet om ”rødt flagg” bør være et godt supplement til sperring av kreditt.

Prosjektet slutter seg til FAD sitt forslag om en tjeneste hvor byråenes aktiviteter samordnes.

Det er sterke signaler om en samordnet sperretjeneste som kredittopplysningsbyråene nå har tatt initiativ til å drøfte.

6.4.1 Sperretjeneste

Prosjektet er av den oppfatning at det vil føles gunstig for borgeren å kunne henvende seg ett sted for å sperre for tilgang til kredittopplysninger. Slik situasjonen er i dag må man kontakte de tre store aktørene. Ifølge Datatilsynets oversikt er det ytterligere fem virksomheter som har konsesjon, men disse har liten markedsandel.

Det ligger i sakens natur at om den registrerte ønsker å sperre utlevering av opplysninger fra et byrå, vil ønsket trolig gjelde generelt. Det finnes likevel unntak. Datatilsynet har hatt tilfeller hvor den registrerte vil la seg sperre hos en virksomhet, men ikke hos øvrige. Det kan f. eks. skyldes at vedkommende er misfornøyd med selskapets håndtering av innsyn, retting og sletting av opplysninger.

Få er klar over hvordan kredittopplysningsbransjen er organisert, hvilke aktører som er på markedet og hvilke tjenester de enkelte tilbyr. Med mindre den registrerte er gjort oppmerksom på hvilke aktører som er operative i markedet, vil det ikke være intuitivt hvem som bør kontaktes.

Sperring av kredittopplysning er ikke uten praktiske utfordringer. Få er klar over hvor ofte slike opplysninger faktisk utleveres. Prosjektet har heller ikke eksakte tall, men har gjennom Datatilsynets kontrollvirksomhet fått antydninger om at antall utleveringer ligger i størrelsesorden 20 millioner⁷ hvert år. Denne kontrollvirksomheten avdekker også at terskelen for å be om kredittvurdering blir stadig lavere. I noen tilfeller er det avdekket at det bes om kredittvurdering for nye kundeforhold, uavhengig av om det skal gis kreditt eller ikke. Det er da naturlig å anta at kredittvurderingen benyttes til å sile ut uønskede kunder.

Det er tre sentrale aktører i forhold til kredittvurdering: Kredittopplysningsbyrået, kunden (den som ber om kredittvurdering) og den omspurte (den registrerte).

En trend de siste årene er at de praktiske vurderingene rundt saklighet nå foretas av kunden, ikke kredittopplysningsbyråene slik det var tidligere. De fleste kundene har online tilgang og forespør kredittvurdering etter behov. Selv om prosjektet har tatt fatt i de mest ekstreme utslagene av den nye praksisen, vil denne være utbredt i overskuelig fremtid.

Selv om det er mulig å foreta en midlertidig oppheving av sperringen, er trolig få klar over hvor ofte det kan være påkrevd. Dersom en registrert har satt sperre på utlevering, vil de kunne bli avvist som kunde hos teleselskaper, forsikringsselskaper, netthandel og som innskuddskunde i bank. Manglende utlevering kan av praktiske grunner tolkes til at den registrerte har anmerkninger, selv om det er spesifisert at sperring er iverksatt. Vedkommende kan da bli avvist på feilaktig grunnlag.

⁷ Opplysningene er gitt fra de tre store kredittopplysningsbyråene, men er beheftet med usikkerhet.

Omfanget av sperringer har økt jevnt de siste årene:

Dun & Bradstreet	Lindorff Decision	Experian
2007: 1 049		2007: 447
2008: 1 842		2008: 1 591
2009: 1 808 (pr. 26.08)		2009: 1 706 (pr. 10.09)
Totalt: 4 886	Totalt: 4 739	Totalt: 4 937

Sperring av anledning til å utlevere kredittopplysning må ses i sammenheng med muligheter for å åpne for kredittvurdering i konkrete situasjoner. Kredittopplysningsbyråene har allerede i dag løsninger for dette. Løsningene er ikke optimale, men i følge byråene fungerer de tilfredsstillende. Normalt får den som sperrer egne opplysninger en kode som må oppgis ved senere midlertidig oppheving. Det er ikke til å komme bort fra at sperring og oppheving vil være beheftet med mye plunder for den registrerte.

Prosjektet mener det foreligger to likeverdige alternativer:

1. At det opprettes felles mottakssted for sperring og midlertidig oppheving hos kredittopplysningsbyråene.
2. At kredittopplysningsbyråene, etter samtykke fra registrerte, utveksler ønsket om sperring og oppheving til øvrige byråer.

I et felles møte blant kredittopplysningsbyråene den 4. november d.a. var det enighet om å utrede alternativ 1. Det var ønske om å se på mulighet for å legge denne tjenesten på nettsiden www.idtyveri.info. I forhold til eksisterende regelverk og spesielt i forhold til personopplysningsforskriftens § 4-2 må det avklares om hvordan dette skal gjennomføres. Datatilsynet er ikke uvillige til å vurdere behovet for justering av denne om dette alternativet velges, og det skulle vise seg at en endring er nødvendig.

6.4.2 ”Rødt flagg”

Prosjektet vil for øvrig vise til Datatilsynets forslag om alternativt supplement til sperring, nemlig innføring av såkalt ”rødt flagg”. Det vil være en mildere variant. Det er dog innsigelser på denne løsningen. Bank og finans, som er de absolutt største brukerne av kredittvurderingstjenesten og de det vil være mest aktuelt for, ønsker minst mulig manuell behandling og har derfor på forhånd tatt en beslutning om hva de skal gjøre dersom de støter på en person med et slikt merke. De fleste bruker scoretjenester som en del av sitt beslutningsgrunnlag. Merkingen må derfor på en eller annen måte påvirke score slik at bruker blir gjort oppmerksom på merkingen. Kredittopplysningsselskapene er derfor av den oppfatning at en slik merking vil avvike lite fra dagens løsning med sperring. Løsningen har dog vært testet ut i Canada, angivelig med gode resultater.

6.4.3 Tiltak og fremdriftsplan

Av ovennevnte fremgår at det er hensiktsmessig å se sperring og åpning av sperring under ett. Etter prosjektets vurdering taler mye for at det vil være hensiktsmessig at henholdsvis sperring, midlertidig oppheving og mer oppheving samordnes. Slik samordning må være basert på samtykke fra den registrerte. Prosjektet mener at man vil være tjent med at byråene slutter seg til en permanent frivillig ordning. For alle praktiske formål snakkes det om tre aktører. Et drøftelsesmøte med disse byråene gjennomføres i løpet av 2009, med sikte på igangsetting ved inngangen til 2010. Fremdriften vil være avhengig av velvilje hos byråene. De har imidlertid vist fleksibilitet og velvilje ved tidligere anledninger.

6.5 Tiltak 5 - Oversikt over hvor det er stiftet gjeld

Kredittopplysningsbyråene er normalt involvert i de tilfeller det foreligger et kreditlement av en viss størrelse. Det innebærer at det ikke bare er ved etablering av gjeldsbrev at byråene blir forespurt. Tilsvarende kan byråene forespørres ved etablering av nye kundeforhold, tegning av telefonabonnement, kjøp av varer og tjenester på kreditt, etablering av nye kundeforhold med videre. Byråenes tjenester er også i bruk i forbindelse med inkassovirksomhet, sikkerhetsklarering og andre mer perifere aktiviteter. Datatilsynet har lagt seg på en relativ liberal forvaltningspraksis hva gjelder utlevering av kredittopplysning. Forespørsel om kredittopplysning har vært akseptert ved kredittkjøp helt ned mot kr. 200,-⁸.

Kredittopplysningsbyråene fører en oversikt over hvem som har bedt om utlevering av kredittopplysninger. De vet likevel ikke hvem som har gitt kunden kreditt. Oversikten vil normalt være tilgjengelig i et halvt år, og kan på forespørsel forelegges den omspurte. Datatilsynet er i tvil om det vil være en god løsning om kredittopplysningsbyråene skal føre oversikt over formålet kunden har med sin forespørsel. De har riktignok et ansvar i forhold til å vurdere saklighet, men ikke på det nivået Fornyings- og administrasjonsdepartementet etterlyste i sin henvendelse til Datatilsynet høsten 2008.

ID-tyveriprojektet viser til gjenpartsplikten som pålegger byråene å underrette den registrerte i forbindelse med utlevering av kredittopplysninger. Dette er et meget viktig institutt for å sette den registrerte i stand til å reagere. For mange ofre vil nettopp gjenpartsbrevet være første indikasjon på et identitetstyveri. Tiltaket har sin begrensning fordi postgangen til offeret er blant de faktorer identitetstyven vil forsøke å skaffe seg kontroll over. Slik kontroll har tradisjonelt blitt ervervet ved å endre adresse, eller å overvåke postkassen. Det er lett for trenede kriminelle å se forskjell på interessant og uinteressant post.

Etter prosjektets vurdering er det ikke, etter gjeldende rett, anledning til å pålegge kredittopplysningsbyråene å supplere nevnte oversikt med hvilke formål det bes om kredittvurdering for. Det er heller ikke registrering av om gjeld eller kreditt blir innvilget. I praksis ville en slik registrering innebære en utvidelse til en form for lavkvalitets gjeldsregister. Det høye antall årlige kredittvurderinger, som antydte tidligere, underbygger videre prosjektets skepsis.

ID-tyveriprojektet vil dessuten påpeke at det kan stiftes ny gjeld eller kreditt innen allerede etablerte kundeforhold. For eksisterende kunder er det mindre vanlig at det bes om ny vurdering, siden virksomheten allerede kjenner kunden. Identitetstyvene er godt kjent med at eksisterende kunder behandles annerledes enn nye og at det ofte er en lavere terskel å manipulere virksomheter som offeret allerede har relasjon til. Byråene vil, etter prosjektets vurdering, ha mangelfull oversikt og gjennomgående lav opplysningskvalitet i et eventuelt utvidet register.

Utover ovennevnte vil prosjektet trekke frem det faktum at det ofte bes om kredittvurdering som ikke etterfølges av en økonomisk transaksjon. Kredittopplysningene er kun et av flere beslutningskriterier. Det er heller ikke gitt at tilbyder av kreditt faktisk får realisert sitt tilbud. Forholdet kan illustreres med et eksempel: Ved finansiering av bil vil en kunde kunne forespørre flere selskaper om finansiering. Alle som forespørres vil kunne ha et saklig behov for å innhente kredittopplysninger, mens kun en av dem blir reell kreditor. Kredittopplysningsbyrået vil ikke ha noen informasjon om hvem som faktisk inngikk avtale med kunden, med mindre de innføres nye plikter for aktørene.

Prosjektet mener derfor at netto bidrag fra en slik løsning vil være marginal. Prosjektet viser dog til at byråene har en oversikt over hvem som har spurt om kredittopplysning og at det kan være en hjelp i oppnøstingsarbeidet til politiet, offer eller andre som bistår offeret.

I et av prosjektets forslag senere i dokumentet fremholdes opplæring av polititjenestemenn som et viktig tiltak. Kunnskap om byråenes rolle og deres oversikt vil være blant de forhold det er viktig å

⁸ Forvaltningspraksisen er vurdert skjerpet inn. I forbindelse med planlagt revisjon av regelverket vil Datatilsynet vurdere å fremme forslag om innstramming av praksis.

formidle til etterforskere. Tilsvarende vises det også til forslaget om hjelpelinjen som vil kunne veilede offeret, blant annet til å skaffe seg tilgang til listene som byråene besitter.

En del amerikanske foredragsholdere og skribenter⁹ har hevdet at det i gjennomsnitt tar 11-13 måneder før et identitetstyveri oppdages av offeret. Selv om prosjektet ikke kan stå inne for dette tallet, indikerer det dog et lagringsbehov som sett fra prosjektets ståsted ville innebære en uønsket utvikling.

Av ovennevnte følger at prosjektet vurderer kost / nytte ved en utvidelse av pliktene til aktørene å være negativ. Det anbefales at man begrenser seg til at allerede eksisterende oversikt hos byråene benyttes som hjelpemiddel. Selv om det vil være mye overskuddsinformasjon i forhold til hvor kreditt eller gjeld faktisk er stiftet, vil oversikten gi et bidrag til å indikere hvor dette kan ha skjedd.

6.5.1 Tiltak og fremdriftsplan

Etter prosjektets vurdering vil det ikke være mulig innen gjeldende rett å få etablert et kvalitativt register over hvor gjeld er stiftet hos byråene. Det vil kreves endring i personopplysningsforskriften og i konsesjonene til byråene. Datatilsynet mener dessuten at tiltakets effektivitet foreløpig ikke er tilstrekkelig godtgjort til å forsvare en regelverksendring og justering i konsesjon. Prosjektet viser likevel til at kombinasjon av eksisterende register og gjenpartsplikten er gode instrumenter. Disse kan trolig utnyttes mer effektivt ved tilstrekkelig opplæring av etterforskere i politiet.

6.6 Tiltak 6 – informasjonstiltak til virksomheter

Målet med tiltaket er å forebygge at virksomhetene mister kontrollen over personopplysninger som siden kan misbrukes av identitetstyven. Personopplysninger kan være tilgjengelig både for ansatte og samarbeidspartnere. I mange tilfeller er ikke virksomhetene bevisst de forventninger samfunnet har satt til ansvarlig forvaltning, herunder hvilke sikringstiltak som kreves ved behandling av slik informasjon.

Det handles hvert år for store summer i norske virksomheter. Det er innkjøpsansvarlig som har fullmakter til slik handel. Det handles på nettet, hos leverandører og hos detaljister. Ved eksempelvis å forfalske eller skaffe seg tilgang til en ekte firmaattest, har svindlere klart å tilegne seg kreditt eller andre fordeler på vegne av virksomheten. Slike handlinger kan både ramme enkeltpersoner i virksomhetene, ved at de stilles til ansvar for kjøp de ikke har foretatt eller det kan ramme enkeltpersonforetak.

Det er behov for en styrking av informasjonsarbeidet mot virksomhetene slik at de i større grad er klar over truslene og sitt ansvar. De bør gjøres kjent med forventninger om sikringstiltak, at de til enhver tid vet hva slags beskyttelsesverdige opplysninger de forvalter og hvordan dette realiseres.

I tillegg til generelle informasjonstiltak vil spesialisert opplæring av nøkkelpersonell i virksomheter være effektive tiltak mot identitetstyveri.

⁹ Kilde til informasjonen er primært ved søk på nettet. Ingen kilder er spesifikt nevnt da disse anses usikre.

6.7 Tiltak 7 – generell offentlighet og skatteopplysninger

Ukritisk publisering av personopplysninger i regi av offentlig sektor på nettet kan ha negative virkninger. Det kan faktisk hjelpe kriminelle i deres arbeid med innhøsting av personopplysninger. Situasjonen er ikke mindre kritisk sett i lys av den nye offentlighetsloven som legger opp til en ytterligere liberalisering i forhold til gjeldende rett. Datatilsynet er også bekymret over utviklingen og har tatt dette opp i et eget brev¹⁰ til regjeringen. Datatilsynets bekymring ble drøftet i et tilsvarende fra Justisdepartementet hvor man mente at man holdt seg innenfor gjeldende rett. Departementet tilsvarte gjorde tydelig at man ikke delte disse bekymringene. Tvert imot viser siste tids utvikling på lovområdet at departementer går enda lenger i liberaliseringen.

Prosjektet presiserer at det er koblingen mellom sak og person ved publisering¹¹ på nettet som kan gi utilsiktede skadevirkninger. Det er en kjent sak at det skjer systematisk innhøsting av personopplysninger fra nettet, med sikte på senere kommersialisering. Dette gjøres av selskaper som ligger utenfor norsk og europeisk jurisdiksjon. Hvorvidt slik innsamling skjer fra norske domener er imidlertid uklart på det nåværende tidspunkt. Etter prosjektets vurdering kunne en interesseavveining tilsi at man burde aidentifiserte en sak før publisering. Først på konkret forespørsel burde den supplerende opplysning om hvem saken gjelder vært utlevert. Sett i lys av nylig vedtatt offentlighetslov, må prosjektet erkjenne at sistnevnte forslag neppe er innenfor realistiske rammer.

Prosjektet har registrert at enkelte har tatt til orde for at offentliggjøringen bør skje fra skattemyndighetenes nettsider, slik at man unngår en fullstendig ukontrollert spredningen av opplysningene. Skattemyndighetene kan i det minste sette i verk tiltak mot massiv innhøsting av opplysningene. Slik situasjonen er i dag, hvor det sendes ut fullstendige datasett til rundt 150 redaksjoner er det fare for at bruken av opplysningene kan gå på tvers av lovgivers intensjoner.

6.8 Tiltak 8 – informasjonstiltak til befolkningen

I USA og Storbritannia er det gjennomført vellykkede informasjonskampanjer rettet mot befolkningen for å øke aktsomheten overfor identitetstyveri. Prosjektet er opptatt av at informasjonen mot forbrukeren må være relevant. Man bør være bevisst på hva som bør være forbrukerens ansvar og hva som påligger andre aktører. Etter prosjektets oppfatning vil et hovedfokus mot forbruker være å:

- Forhindre at forbruker bidrar til unødvendig spredning av egne personopplysninger, herunder at beskyttelsesverdig informasjon destrueres på behørig måte før den kastes.
- Vurdere tiltak som strengt tatt går utover eget ansvar, for eksempel låsing av postkasse for å hindre at beskyttelsesverdig informasjon kommer på avveie.
- Gi opplæring i generelle aktsomhetsregler i den fysiske verden og på Internett.
- Gi opplæring i hvordan sikre egen datamaskin for å hindre datainnbrudd eller at personlig informasjon på datamaskinen kommer på avveie.
- Skape bevissthet om å reagere raskt på tegn til identitetstyveri.
- Sette forbruker i stand til å oppdage pågående identitetstyveri.
- Det må fokuseres på opplæring av de unge gjennom målrettede kampanjer/kurs i skolen og andre fora der ungdom møtes.

¹⁰ Brev fra Datatilsynet til FAD 31.8.2007.

¹¹ Med publisering menes i dette tilfellet en allmenn tilgjengeliggjøring på nettsider – uten noen form for tilgangskontroll.

6.9 Tiltak 9 – hjelpelinje

De som er utsatt for identitetstyveri trenger ofte bistand. Få har opplevd slike situasjoner tidligere og er rådvile. Siden tidsaspektet er viktig for å begrense skade, er det viktig at offeret får raskt assistanse fra profesjonelle veiledere.

Finansnæringens Hovedorganisasjon (FNH) og kredittopplysningsselskapene uttalte allerede i 2008 at det var behov for en hjelpelinje der ofre for identitetstyveri kan henvende seg og få hjelp. Det er i dag en tydelig økning i antall henvendelser mot førstelinjetjenestene i finanssektoren.

Nå vil en hjelpelinje ikke bare begunstige offeret, men også næringslivet. Det er de som normalt vil bære de direkte kostnadene. En hjelpelinje vil således også gi en netto gevinst i de bedriftsøkonomiske og samfunnsøkonomiske regnskapene.

Myndighetene utsteder borgerne med en statsautorisert, varig og entydig identifikator, og bør således bidra til å sikre denne når rettmessig individ opplever problemer som følge av at denne identifikatoren er stjålet og/eller misbrukt.

Basert på overnevnte argumentasjon mener prosjektet at dette initiativet må samfinansieres av næringslivet og norske myndigheter.

Det blir viktig med spesialiserte veiledere, gjerne med samme type opplæring som foreslås ovenfor tjenestemenn i politiet. Det er likevel viktig at en slik hjelpelinje ikke gjør typiske politioppgaver, det bør forbeholdes politiet.

6.9.1 ID-tyveriforsikring

Det siste året har stadig flere forsikringstilbud kommet på markedet.

ID-tyveriprojektet er i utgangspunktet positiv til ID-tyveriforsikring – i mangel av noe bedre.

All den tid vi ikke har tilbud om et støtteapparat fra myndighetene, er det positivt at kommersielle krefter kommer på banen. Dog er det synd at det ender opp med at forbrukerne må betale for å sikre sin egen identitet, da dette burde være et myndighetsansvar.

ID-tyveriprojektet håper forsikringene, slik de fremstår i dag, blir overflødig en gang i fremtiden.

Prosjektet har som mål å få etablert et nasjonalt kompetansesenter, som skal levere opplæringsstøtte, statistikk og en hjelpelinje. Det er ønskelig at disse tjenestene blir et spleiselag mellom myndighetene og næringslivet.

Ved at noen nå bygger kompetanse på deler av hjelpelinjefunksjonen har vi mer kompetente aktører å diskutere outsourcing av elementer i denne hjelpelinjen med, den dagen dette skal etableres som en samfinansiert tjeneste mellom næringslivet og myndighetene.

6.10 Tiltak 10 – kompensasjon

Identitetstyveri innebærer samfunnsøkonomiske tap. Staten må, i motsetning til næringslivet, legge til grunn samfunnsøkonomiske vurderinger i sine beslutningsprosesser. Identitetstyveri har en rekke eksterne virkninger. De eksterne virkningene påvirker det samfunnsøkonomiske regnestykket¹². Prosjektet vil primært trekke frem følgende komponenter, sett i forhold til offeret:

- Eventuelt direkte økonomisk tap.
- Offerets tidskostnad.
- Reduksjon av livskvalitet hos offeret i relevant periode.
- Svekket allmenn tillit og tilhørende økning i transaksjonskostnader.
- Generell mistro til bruk av elektroniske løsninger.

Den amerikanske lovgivningen som ble vedtatt i september 2008 tok i seg noen av de ovennevnte komponentene. Lovgiver erkjente at offeret vil bruke tid og kostnader på å rydde opp i forhold som i prinsippet er offeret uvedkommende. Dette kan offeret kreve kompensasjon for.

Prosjektet mener det er riktig å anta samme resonnement i Norge. Negative økonomiske eksternaliteter er viktig å kanalisere til rette pliktsubjekt. Det er ikke rimelig at offeret skal bære kostnader om en virksomhet eller offentlig forvaltningsenhet har håndtert sitt ansvar på en uforsvarlig måte. Datatilsynet tilrår at nevnte problemstilling kanaliseres til rette departement for videre utredning.

¹² Samfunnsøkonomiske virkninger blir grundigere behandlet i kapittel 8.

6.11 Tiltak 11 – statistikk

Sammen med TNS-Gallups Catiavdeling har vi intervjuet et representativt utvalg på 1000 respondenter via telefon. Undersøkelsen viser at 5,4 % av den norske befolkning mener de har blitt utsatt for Identitetstyveri.

Definisjonen som ble brukt:

“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.”

Spørsmålet som ble stilt: “Har du blitt utsatt for noen form for identitetstyveri noen gang?”

Prosjektet vil fortsette med slike målinger for å kunne følge med på utviklingen, og samtidig få et inntrykk av om de ulike tiltakene vi initierer faktisk har noen effekt.

Identitetstyveriprojektet har videre skaffet til veie statistikk fra noen enkeltaktører (DnB NOR, Telenor, Sparebank 1), som sier noe om hvordan fenomenet identitetstyveri utvikler seg i Norge. Den rådende oppfatning er at problemet foreløpig er moderat, men sterkt økende. Flere av prosjektaktørene synes å dele oppfatningen om at man raskt kan stå ovenfor en situasjon hvor økningen kommer ut av kontroll. Samtidig viser man til at mye kan gjøres preventivt for å forebygge tilstander man har hatt i USA. I følge de føderale myndigheter ble 10 millioner, eller rundt 4 % av befolkningen, rammet i 2006. Tallet er meget høyt, men dannet samtidig et godt beslutningsgrunnlag for handling. Innsatsen som amerikanerne har foretatt er imponerende, og har gitt konkrete resultater. Det viser at det nytter. I Norge kan ingen si noe mer vedrørende omfang, variasjon i type tyveri og svindelmetoder eller utvikling. Dette er meget uheldig og bør tas fatt i snarlig. Prosjektet har vært i dialog med politidirektoratet og utalt sine ønsker om at det settes i verk tiltak for å få en mer entydig registrering av de tilfeller som tross alt anmeldes.

Amerikanerne har utviklet standard skjema som skal sendes et av de føderale byråer. Slik fanger man opp et bredere spekter av identitetstyveri. Mange tilfeller anmeldes ikke. Man ønsker trolig ikke den negative oppmerksomhet en anmeldelse gir og kompenserer offeret de direkte kostnadene.

Prosjektet mener at vårt forslag til politidirektoratet må tas med inn i planene om oppgradering/overgang til nytt straffesaksregister, og at dette implementeres så raskt som mulig. Samtidig bør alle aktører i dialogen mot forbruker oppfordre til å anmelde slike saker, selv om næringsvirksomheten påtar seg de direkte økonomiske tap. Vider må politiet pålegges å ta i mot alle anmeldelser, selv om det ikke er ressurser til å etterforske disse. Kopi av anmeldelse er ofte den eneste dokumentasjonen et offer har for å bekrefte sin situasjon.

6.12 Tiltak 12 – opplæring og dialog

Næringslivet er de som raskest vil oppfatte trender innen kriminalitetsutviklingen. I de aller fleste tilfeller vil et tilslag innbefatte aktiviteter mot finansindustrien eller andre som gir kreditt. Denne sektoren peker seg derfor ut som spesielt interessant hva gjelder informasjonsutveksling med politiet. Sektoren bør også være en viktig bidragsyter i forbindelse med kompetanseoppbygging i politiet.

Prosjektet foreslår at det etableres et opplæringstiltak for tjenestemenn om identitetstyveri og hvordan dette kan bekjempes. Det er høstet mye erfaring i andre land som norske politimyndigheter kan dra veksler på. Manglende kunnskap kan bidra til at de kriminelle får en for lett jobb, til stor skade for den økonomiske tilliten i samfunnet vårt. Prosjektet vil i kapitlet om samfunnsøkonomiske virkninger komme inn på hvordan svekket tillit kan føre til økte transaksjonskostnader og en nedkjøling av omsetning.

Datatilsynet har uttalt at erfaringsutveksling fint kan skje uten omtale av konkrete gjerningspersoner. politiet bør få informasjon om trender, nye måter å utnytte svakheter på og en åpen drøftelse om innslag av organiserte kriminelle.

6.13 Tiltak 13 – oppfølgingsansvar

I USA har Federal Trade Commission (FTC) det overordnede ansvar for oppfølging av omtalte problematikk. Dersom det skal trekkes parallell til norsk forvaltning ville det peke i retning av Forbrukerrådet. Forbrukerrådet har selv uttalt at denne form for kriminalitet ikke bør legges under dem.

Forbrukerrådet har imidlertid ikke signalisert noen interesse for å ha en rolle i forhold til id-tyveri problematikk.

Forbrukerombudet har på sin side uttalt at NorSIS bør ha en rolle i forhold til et slikt overordnet ansvar. NorSIS har allerede en rolle som formidler av sikkerhetskultur på nasjonalt nivå samt tett kobling til et av landets sterkeste miljøer i forhold til informasjonssikkerhet med Høgskolen i Gjøvik som en vesentlig aktør.

Prosjektet er omforent rundt etableringen av et nasjonalt kompetansesenter som også skal ha ansvar for hjelpelinjen. Det vil således være formålstjenlig å samle all aktivitet i dette senteret.

6.14 Tiltak 14 – etterforskning

Identitetstyveri kan være knyttet til organisert kriminalitet. I slike tilfeller kan kriminelle gjerne forsøke å utnytte mulige svakheter i politiets organisering. Organiserte kriminelle jobber ofte på tvers av politidistriktene, og det kan ta tid før distriktene blir enige om en koordinert etterforskning. Dette er til de kriminelles fordel. Dess raskere en operativ etterforskning tar til, dess høyere er mulighetene til å begrense skadene og gripe gjerningsmennene.

Prosjektet mener det kunne være hensiktsmessig å vurdere å legge det overordnede ansvar for denne kriminalitetsformen til en sentral politienhet. Prosjektet anbefaler Justisdepartementet å få dette forholdet nærmere belyst.

6.15 Tiltak 15 – tiltaksplan

Det synes nærliggende å peke på fravær av konkrete planer for å møte utfordringene man står ovenfor. Prosjektet mener det er nærliggende å peke i retning av Justisdepartementet når det gjelder ansvaret for dette. Dersom man skal være rustet til å møte utfordringene mange mener vil komme, må politi, statsadvokatene, domstoler og Kriminalomsorgen trekkes inn som elementer i planleggingen.

politi, statsadvokatene og domstolenes medvirkning er viktig for å få de kriminelle tiltalt og dømt for de straffbare forholdene. Dette er viktig både ut fra allmennpreventive hensyn og for å stanse videre kriminalitet fra slike, ofte notoriske, kriminelle.

7 Om identitetstyveri og utviklingstrekk

7.1 Hvorfor oppstår identitetstyveri?

Identitetstyveriet består av en forberedelsesfase, hvor innhøsting av personopplysninger er sentralt, samt en gjennomføringsfase hvor ulike instrumenter får større betydning. Råstoffene en identitetstyv bruker er altså:

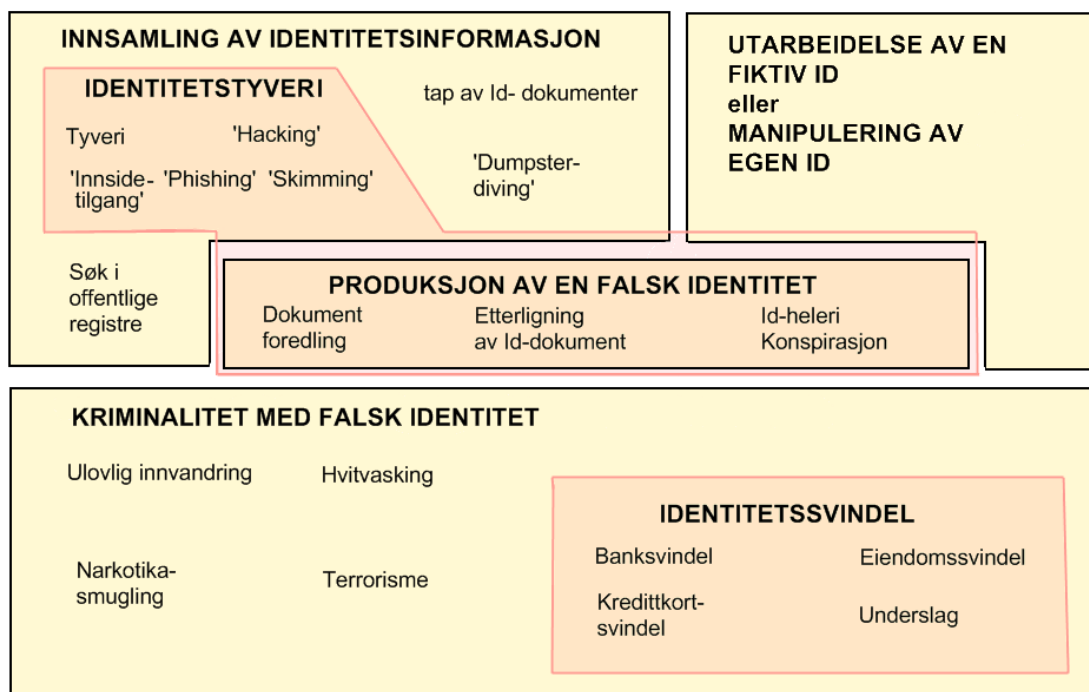
- Personopplysninger, og
- instrumenter¹³

Den første komponenten benyttes for å selektere ut ofre og som inngangsport til ny, supplerende informasjon. Den andre komponenten benyttes i forbindelse med gjennomføring.

7.2 Hvordan velges offeret ut?

I de fleste tilfeller vil det ligge økonomiske motiver bak et identitetstyveri. Det er offerets aktiva eller kredittverdighet som identitetstyvrene er ute etter. Med aktiva menes personlige eiendeler, herunder eventuell formue. Med kredittverdighet menes muligheter for låneopptak eller kredittkjøp som ikke er utnyttet.

Før ett konkret offer velges ut foretas det, i hvert fall blant organisert kriminelle, en seleksjon. Det samles eller kjøpes inn informasjon om et større antall personer. Ut fra gitte kriterier selekteres de mest attraktive ut. I noen tilfeller innhentes supplerende informasjon og det søkes tilgang til instrumenter¹⁴. Når disse er i hende starter normalt aktivitetene som rammer offeret. Vi har hentet en skisse fra identitetstyveriprojektet i Canada som gir en god illustrasjon av prosessen:



Kilde: Sproule, CIPPIC, Canada 2007

¹³ For eksempel identitetsbevis eller andre dokumenter som brukes til å manipulere en tredjepart.

¹⁴ Med instrumenter menes identitetsbevis eller liknende

7.3 Hvem er aktørene?

De sentrale aktørene når det gjelder identitetstyveri og identitetssvindel er:

- Den som gir tilgang til informasjon eller instrumenter (kilde)
- Den som samler, bearbeider informasjon og instrumenter (innhøster/identitetstyven)
- Den som gjennomfører svindelen (identitetssvindleren)
- Den som gir uautorisert tilgang til andres aktiva eller rettigheter (virksomheten)
- Den som misbrukes av identitetstyven (fornærmede/offer)

Mange virksomheter i offentlig og privat sektor ”lekker” personopplysninger. Ikke i den forstand at det er en planlagt eller tilsiktet prosess. Praksisen trenger ikke en gang å være i strid med gjeldende rett. Likevel, når relativt triviell informasjon innhøstes og settes i system, representerer det et meget potent verktøy. Informasjon er makt, også hva gjelder identitetstyveri. Personopplysninger kan sette identitetstyven i stand til å manipulere tredjepart. Kunnskap om, selv trivielle forhold, utnyttes til å overbevise motpart om ønsket identitet.

Flere har tatt til orde for at det er manglende sikkerhet hos virksomhetene som utgjør en sentral del av problemet. Det er for så vidt en korrekt observasjon, men man må samtidig forstå at man her beveger seg inn på identitetstyvens spesialfelt – nemlig det å manipulere. De utvikler sine metoder, ofte med inngående kjennskap til styrker og svakheter i virksomhetenes rutiner.

Det finnes mange kilder til personopplysninger. Det mest fremtredende eksemplet er de tidligere nevnte særnorske skattelistene, som er søkbare på nettet. Bedre blir det ikke av at den svært detaljerte selvangivelsen sendes ut i åpne postkasser i et nærmere bestemt tidsrom. Høyverdige identitetsbevis, som pass, sendes tilsvarende ut i ubeskyttet postgang. Videre har store reformer innen helse, sosial og omsorg gjort at stadig flere mennesker har tilgang til flere opplysninger, over lenger tid. Det synes uthensiktsmessig å liste opp alle kildene, her spiller både kommunene og næringslivet en rolle. Deler av næringslivet har lagt listen så lavt for etablering av nye kundeforhold, at hvem som helst som har tilgangen til fødselsnummer og adresse kan ta seg til rette.

Spredning av personopplysninger er et personvernproblem, men trenger ikke å være det i forhold til identitetstyveri. Ofte er personopplysninger sentrale i en innledende fase: Selekttering, supplering og bearbeiding av potensielle ofre. Det at noen vet mye om offeret burde likevel ikke være tilstrekkelig til å utgi seg for vedkommende. Det er her argumentet om å sikre kontroll på instrumentene kommer inn i bildet. Identitetsbevis på avveie er den mest kritiske faktoren. Et tappt førerkort kan benyttes i årevis av kriminelle. Likeledes med bankkort med identitetsbevis på baksiden. Verst er det imidlertid med pass på avveie. Mellom 100-200 norske pass kommer på avveie mellom passprodusent og innehaver - hvert eneste år. Hvor disse havner er det få som vet. Regningen havner sannsynligvis hos deler av de 100-200 som aldri mottar passet sitt. I tillegg til de som kommer bort i postgangen mistes eller gjenglemmes det store mengder identitetsdokumenter, telefoner, lommebøker og liknende i taxi, på flyplasser og andre tilsvarende steder.

7.4 Kilder til objektiv informasjon

En naturlig kilde til informasjon burde vært politiet. De har imidlertid hatt en uensartet registrering av fenomenet. I praksis må man inn i hver enkelt sak i relevante saksfelt for å avdekke om hendelsen kan defineres som identitetstyveri. Forholdet er imidlertid i ferd med å bedres, etter at politidirektoratet ble bedt om å foreta seg noe i saken. De har foreslått endringer i politiets saksbehandlingssystem, slik at det legges inn koder for identitetstyveri. Det gjør at man vil få noe bedre statistikk på sikt hva gjelder de tilfeller som faktisk anmeldes.

Når det gjelder svindel med kredittkort og urettmessig opptak av kreditt så er det mange av disse tilfellene som ikke anmeldes til politiet. Etter hva Datatilsynet erfarer, kan en årsak til dette ha med tilliten til finansindustrien å gjøre. I mange tilfeller kompenseres finansinstitusjonene tapene uten å

anmelde slike forhold. Slik sett opprettholdes det et kunstig høyt tillitsnivå til for eksempel elektroniske betalingskort.

Etter prosjektets vurdering bør det arbeides for større åpenhet omkring identitetstyverier som innbefatter bruk av finansielle instrumenter. I motsatt fall er det vanskelig å kartlegge de samlede samfunnsøkonomiske kostnadene ved denne formen for kriminalitet.

7.5 Hvor utsatt er norske borgere?

Datatilsynet har ved flere anledning uttrykt bekymring om det norske samfunnets robusthet i forhold til identitetstyveri. Det norske samfunnet er preget av en utstrakt grad av åpenhet, tillit og modernisert samhandling. Dette er positive karakteristika, men kan samtidig trekkes så langt at det slår tilbake ved å gi borgeren økt sårbarhet. Informasjon er en viktig maktfaktor, så også hva gjelder personopplysninger. Ved å gjøre tilgangen til personopplysninger enklere for allmennheten, men også for identitetstyven, svekkes samtidig borgerens evne til å beskytte seg.

Utfordringen er ikke åpenheten i forvaltningen. Det er den internettbaserte, personifiserte åpenheten. Offentlighetsloven er tuftet på prinsippet om at borgeren skal settes i stand til å kontrollere forvaltningen. Det er relevant å stille spørsmål om det er selve saken som er kjernen i denne kontrollmekanismen eller om det er personifiseringen. Dette spørsmål må vurderes i lys av hvilke andre hensyn som står i fare for å forvitte. Den som ønsker å stille kritiske spørsmål til forvaltningen og som trenger tilhørende personopplysninger bør kunne få det. Det er likevel ikke åpenbart at det fulle informasjonsbildet bør tilgjengeliggjøres uoppfordret.

Etter prosjektets vurdering er det noe mangel på kritisk sans hva gjelder hva som bør tilgjengeliggjøres. Den viktigste kanal for tilgjengeliggjøring er Internett. Ulempen med denne formidlingskanalen er at man har lite kontroll med hvem som høster informasjon og hvilke hensikter disse har. Datatilsynet erfarer i sin dialog med offentlig sektor at få tenker gjennom faren for masseinnhøsting av informasjon. Det er et formål som normalt går langt utover offentlighetslovens intensjon og vil også være i strid med personopplysningsloven. Innsamlingen kan skje i den hensikt å begå straffbare handlinger. ID-tyven / innhøster kan sitte hvor som helst i verden og omsette sitt foredlede produkt til innenlands kriminelle¹⁵. Når først informasjonen er innhøstet er det ofte svært vanskelig å få slettet materialet.

Norske borgere er sårbare i forhold til identitetstyveri. Sårbarheten gjelder både overfor individuelle kriminelle og organiserte miljøer. Basert på to enkle faktorer:

- Kontaktopplysninger og fødselsnummer, samt
- et høyverdig identifikasjonsdokument (fører kort, bankkort eller pass),

kan offeret påføres stor skade.

Førstnevnte faktor kan kjøpes eller skaffes til veie ved identitetstyvens egen bedrift, mens sistnevnte enten stjeles eller finnes i offerets postkasse.

Prosjektet har ikke holdepunkter for å hevde at norske borgere er mer utsatt enn andre europeere, men viser til at det foreligger en rekke svakheter som før eller siden vil utnyttes i større grad enn i dag.

¹⁵ De amerikanske justismyndigheter avdekket et internasjonalt nettverk som hadde samlet inn kredittkortopplysninger om 11 millioner personer. Se henvisning i kilder.

7.6 Utviklingen i andre land

Det er de engelskspråklige land som har opplevd sterkest vekst i antall tilfeller med identitetstyveri, dersom man ser på de offisielle statistikkene. I USA er det føderale byrået Federal Trade Commission (FTC) som har det overordnede ansvaret og fører statistikk.

Den sterkeste utviklingen innen identitetstyveri har man observert i USA. I en periode på 5 år (2001-2006) utviklet det seg fra ca. 750 000 tilfeller til rundt 10 millioner¹⁶. Identitetstyveri var med det en kriminalitetsform som rammet rundt 4 % av USAs befolkning i 2006. Det er et meget høyt tall.

Det kan ikke påvises samme utvikling i andre land. Det som imidlertid er påfallende er hvor sterk veksten var i USA. Fenomenet mer enn tidoblet seg i ovennevnte periode. I 2006 nedsatte president Georges Bush en såkalt "Presidential task force" som fikk iverksatt en del umiddelbare tiltak. Gruppen kom med mange forslag¹⁷ til hvordan identitetstyveri kan forebygges. Mange av forslagene vil også ha relevans for Norge.

Omsetning av personopplysninger utgjør en viktig del av identitetstyvenes virksomhet. De største hendelsene er registrert i USA. Prosjektet vil eksemplifisere problemstillingen:

- Den 5. august 2008 kunngjorde det amerikanske justisdepartement at 11 personer var tiltalt for tyveri av kredittkortopplysninger for hele 40 millioner mennesker¹⁸. Mye tyder på at de 11 sammensvorne hadde tenkt å kommersialisere materialet. I slike tilfeller stykkes gjerne datamaterialet opp og selges på det svarte marked, for eksempel i bolker på tusen poster. Hva prisen er for en slik fil på det illegale markedet skal være usagt, men det er utvilsomt lønnsomt.
- FBI arresterte en tidligere ansatt¹⁹ ved en finansinstitusjon som i hver uke over en periode på to år hadde solgt personopplysninger om 20.000 kunder for 500 dollar. Totalt utleverte mannen personopplysninger om 2 millioner kunder og oppnådde en gevinst på 50.000 dollar.

I Storbritannia er det Home Office som er ansvarlig for arbeidet med å forebygge og bekjempe identitetstyveri. Det er imidlertid et bredt samarbeid mellom myndighetene og næringslivet. Blant annet er det etablert en egen nettside²⁰ som fungerer som et felles referansepunkt for arbeidet. Siden har to målgrupper, henholdsvis privatpersoner og næringslivet.

Det er vanskelig å finne noen god statistikk for Storbritannia, utover at det hevdes å være en markant økning i problemet.

I Canada er en av femten innbyggere blitt ofre for Id-tyveri/svindel. Id-tyveri koster Canada 13,72 milliarder kroner i året. Ofrene registrerte over 197 millioner i tap i 2008. Både myndighetene og næringslivet er aktive vedrørende policy, rapportering, statistikk og holdningskampanjer.

Når det gjelder øvrige land besitter ikke prosjektet noen god statistikk.

¹⁶ Kilde: Hjemmeside til Federal Trade Commission – www.ftc.gov.

¹⁷ Forslagene er oppsummert i rapporten: <http://www.ftc.gov/opa/2008/10/idtaskforce.shtm>.

¹⁸ Kilde er US Department of Justice: www.udoj.gov, press releases.

¹⁹ Kilde: DIrekt, nummer 4/2008 .

²⁰ <http://www.identity-theft.org.uk/>.

8 Det emosjonelle og samfunnsøkonomiske aspekt

Man tar vanligvis egen identitet for gitt. Få tenker over hva det vil si å ha en konkurrent til sin troverdighet, eller sitt gode navn og rykte. Når det gjelder identitetstyveri, er det nettopp disse elementene som utnyttes. Identitetstyvene forvalter og foredler deler av offerets troverdighet for egen vinning. De utnytter forventningene om at økonomiske transaksjoner skal skje kjapt og effektivt. Denne rasjonaliteten utøves mellom mennesker som sjeldent kjenner hverandre, i noen tilfeller mellom bruker og maskin, uten medvirkning fra en kundebehandler. En sentral forutsetning for at dette skal fungere, er at man kan bevise at man er rettmessig innehaver av påberopte rettigheter.

Den tyske sosiologen Wolfgang Sofsky skriver i sin bok ”Personvern – et manifest” om hvordan invasjon i det private rom skaper en sterk avmaktsfølelse. Han setter et klart skille mellom det offentlige og det private. Det er likevel ikke tilstrekkelig at noen uønsket har skaffet seg privat kunnskap, men når man forstår at de har til hensikt å misbruke den at de sterkeste følelsene oppstår. Han fremholder personvernet som ens ”*private festning*”, som gjør oss mindre sårbare ovenfor omgivelsene. Festningen beskytter det private rom hvor individet selv bør avgjøre hvem som skal inviteres inn.

Det private rom vil være av varierende størrelse, avhengig av en rekke individuelle faktorer. Sofsky slår imidlertid fast at behovet for et privat rom uansett vil være tilstede, siden det hører til forestillinger om det å være et selvstendig menneske. I det moderne samfunnet benytter vi tjenester som gjør at deler av vår private rom, i hvert fall for et kortere tidsrom, forvaltes av virksomheter²¹. Bruk er basert på en kombinasjon av behov, beleilighet og tillit. Hvis tilliten brytes kan det skape sterke reaksjoner. Fremfor alt svekker det individets tillit til den som forvolder tillitsbruddet, men også til forvaltere for øvrig. Mennesket har presumpsjon om tillitt, hevder Sofsky, men at hvis denne brytes så kan reaksjonene ramme bredt. Vi har foreløpig ikke hatt mange alvorlige brudd som har blitt allmenn kjent, men om det skjer vil en eventuell tillitssvikt kunne ramme bredt.

Identitetstyven bryter seg inn i det private rom ved at de tilegner seg privat informasjon. Reaksjonene hos offeret vil være sterkt varierende, men henger trolig nøye sammen hvor sterk avmaktsfølelsen er. Verst er det trolig i de tilfeller hvor identitetstyveriet er omfattende, vedvarende og hvor gjerningsmann fortsatt er ukjent. Offeret vet ikke dennes motiv, videre planer og kan være redd for at krenkelsene vil utvides til også å omfatte fysiske trusler eller vold.

Til borgerens identitet kan det være knyttet eierskap til både kapital, hus, bil, båt og hytte. Eiendomsretten, står som kjent sterkt i vår vestlige kultur. Staten sørger for registrering av aktiva, minimum ved hvert årsskifte, både for å sikre borgerens eiendomsrett og for å sikre sin skattebase. Utover dette bidrar offentlighetsloven til å pålegge offentlige sektor plikt til å meddele deler av sin registerinformasjon til andre borgere som av ulike grunner krever innsyn.

Et offer trenger ikke nødvendigvis å være velstående, men må være kredittverdig. Det er nemlig det utnyttede potensialet identitetstyven normalt konsentrerer seg om. Det sies at de mest attraktive objektene for identitetstyvene i USA, er college studenter. Innen to - fem år etter at de er ferdig på college, begynner kontoen til disse studentene å fylles opp. Dermed begynner finansinstitusjonene å kaste seg over dem med tilbud – de er drømmekunder. Det er på dette tidspunkt ”lånet” av identiteten for alvor kan starte.

Ofre for identitetstyveri beskriver en sterk følelse av ubehag. De vet sjelden hvem som står bak handlingene, hvilke motiver de har, når og hvor identitetstyven slår til igjen. Videre sitter noen ofre med usikkerhet om de kan være truet på annen måte. De vil også være usikker på når det de opplever som et mareritt ender.

²¹ Eksempler på slike virksomheter kan være teleselskaper, e-post leverandører, banker, postverket.

Et offer fortalte at *”det føltes som å bokse med bind foran øynene, man vet ikke hvem motstanderen er, hvor han befinner seg, men kjenner slagene over hele kroppen”*. Utsagnet er en meget god sammenfatning av ulike historier prosjektet og dets aktører har fått presentert.

Identitetstyveri påfører samfunnet store økonomiske tap. De viktigste komponentene i dette regnskapet er:

1. Finansinstitusjonens eller andre virksomheters direkte tap
2. Finansinstitusjonenes eller andre virksomheters omdømmetap
3. Offerets direkte tap
4. Offerets indirekte tap i form av for eksempel tidskostnad
5. Offerets emosjonelle kostnader
6. Den generelle økning i transaksjonskostnader i samfunnet ved at tillit mellom individ og virksomhet svekkes

Det er ikke mulig å tallfeste de samfunnsøkonomiske kostnadene basert på det mangelfulle tallmaterialet som foreligger. Det er det også vanskelig å sette en økonomisk verdi på de emosjonelle komponenter i regnestykket. Det har vært gjort forsøk på å tallfeste kostnadene i andre land, primært i USA. Tallene er imidlertid mangelfulle og innbefatter stort sett bare et par av de ovennevnte punkter.

De tre første komponentene taler for seg selv. Når det gjelder den fjerde og femte komponenten, så er det kostnader som sjeldent synliggjøres. Det er samtidig den komponenten som mange ofre trekker frem som den viktigste. Offeret har fått seg forelagt en situasjon vedkommende føler seg helt uskyldig trukket inn i. Fra kreditorers side blir henvendelsene ofte møtt med mistenkelighet og mistro. Det kan ta lang tid og sannsynliggjøre egen uskyld ovenfor kreditorer. Ofrene peker ofte på at de sitter med bevisbyrden. Den emosjonelle belastningen varierer sterkt og henger naturlig sammen med hvor omfattende vedkommende er rammet, samt vedkommendes robusthet for slike hendelser. Det at noen man ikke vet hvem er opptretter som en selv, kan føles sterkt belastende for enkelte. De er ofte usikre på vedkommendes motiv, hvor langt krenkelsen vil strekke seg og om de også er direkte fysisk truet.

Selv om det er vanskelig å slå fast med sikkerhet, er det trolig den sjette og siste komponenten som vil utgjøre den største enkeltkostnaden i regnskapet. Dersom det skapes et inntrykk av at den enkelte lett kan kompromitteres, vil en rasjonell handling fra individets side være å øke aktsomhetsnivået, samt å sikre sine transaksjoner bedre. Den enkelte vil stille strengere krav til de virksomheter det samhandles med og vil kunne respondere negativt på det den enkelte opplever som manglende forsvarlighet. Virksomhetene på sin side vil tilpasse seg en slik virkelighet og sikre seg bedre. Det vil øke transaksjonskostnadene. Ikke mye for hver enkel transaksjon, men sett i sum kan kostnadene bli betydelig.

Det burde vært forsket mer på de samfunnsøkonomiske kostnadene ved denne form for kriminalitet. Datatilsynet er ikke kjent med, men forholder det ikke som usannsynlig, at det foreligger forskningsmaterialet innen temaet. Gitt den eksplosive utviklingen fenomenet har hatt i Nord-Amerika, ville de være underlig om ingen hadde forsket på temaet.

Id-tyveriprojektet har som nevnt hatt kontakter mot et kanadisk forskningsmiljø som har arbeidet med tematikken. Man er imidlertid ikke kjent med om det foreligger relevant materiale fra denne gruppen når det gjelder de samfunnsøkonomiske kostnadene²².

²² Prosjektet har sendt forespørsler om dette.

9 Konklusjon

Prosjektet anbefaler at det nedsettes en interdepartemental gruppe som får i oppdrag å følge opp prosjektets 14 tilrådninger i samarbeid med prosjektet. Det åpnes videre for en representant fra departementene i styringsgruppen når myndighetene bidrar med finansiering av prosjektet.

Myndighetene vil på sikt være tjent med en samfinansiering sammen med relevant næringsliv slik at flere aspekter av denne problemstillingen både bidrar med finansiering, kompetanse og annen støtte til prosjektet og dermed sikrer best mulig kvalitet og resultat ved gjennomføring av overnevnte spesifikke tiltak.

10 Kilder

Dette dokumentet har tatt utgangspunkt i utredningen om ID-tyveri som Datatilsynet sendte Fornyings- og administrasjonsdepartementet 30. Januar 2009.

Rapporter og bøker:

- The President's Identity Theft Task Force Report, Department of Justice, Oktober 2008
 - <http://www.idtheft.gov/>
- The right to Privacy, Ellen Alderman m.fl., Vintage Books 1997
- Understanding Privacy, Daniel J. Solove, Havard University Press 2008
- DIrekt, nummer 4/2008, Datainspektionen
- Verteidigung des Privaten. Eine Streitschrift, Wolfgang Sofsky, C. H. Beck 2007

Pressemeldinger:

- Federal Trade Commission / Department of Justice, 21. oktober 2008: President's Identity Task Force Report on steps Taken to Implement Strategic Plan.
- Department of Justice, 5. august 2008: Retail Hacking Ring Charged for Stealing and Distributing Credit and Debit Card Numbers from Major U.S. Retailers (08-689)

Nettsider:

- www.idtheft.cov (Den amerikanske arbeidsgruppens offisielle side)
- www.ftc.gov (Amerikanske myndigheters nettside)
- <http://www.identity-theft.org.uk> (Britiske myndigheters nettside)
- www.datatilsynet.no
- www.norsis.no (NorSIS, prosjekteier)
- www.idtyveri.info (etablert av Id-tyveriprojektet)
- www.cippic.ca/identity-theft-2/ (Det kanadiske prosjektet)
- www.phonebusters.com/english/index.html (Kanadisk hjelpelinje)
- www.idtheftcenter.org/ (Amerikansk hjelpelinje / kompetansesenter)