

# The Challenge of Countering Identity Theft: Recent Developments in the United States, the United Kingdom, and the European Union

Nicole van der Meulen  
6 September 2006  
International Victimology Institute Tilburg (INTERVICT)

Report Commissioned by the National Infrastructure Cyber Crime program (NICC)

## Table of contents

List of Abbreviations	III
Foreword	IV
1. Introduction	1
1.1 Case Justification	1
1.2 Report Outline	2
2. Identity Theft: In Search of a Definition	2
3. Identity Theft: One Concept, Many Faces	5
4. Identity Theft and Identity Fraud in Action	7
4.1 The Fight Against Identity Theft in the US	7
4.1.1 Prevalence in the US	7
4.1.2 Policy Developments	8
4.1.2.1 Criminalization	8
4.1.2.2 Increasing Organizational Responsibility	9
4.1.2.3 Use of Social Security Numbers	11
4.1.2.4 Law Enforcement Initiatives	12
4.1.2.5 Victims of Identity Theft	12
4.1.2.6 Most Recent Efforts	13
4.1.2.7 Effectiveness	14
4.1.3 Policy Conflicts and Concerns	14
4.2 The UK and Identity Fraud	15
4.2.1 Prevalence	15
4.2.2 Policy Developments	15
4.2.3 Policy Conflicts and Concerns	17
4.3 The EU and the Threat of Identity Theft	18
4.3.1 Prevalence of Identity Theft in the EU	18
4.3.2 Ideas for Prevention and Countermeasures	19
4.3.3 Policy Conflicts and Concerns	21
5. The Forgotten Face	22
6. The Netherlands	23
7. Concluding Remarks and Lessons	24
7.1 Urgency of Identity Theft	24
7.2 Cultural Differences	24
7.3 Policy Options: Criminalization	25
7.4 Raising Public Awareness	26
7.5 Identification Numbers and a Central Database	26
7.6 Biometrics	27
7.7 Conflicts of Interest: The Challenge of Coordination and Cooperation	29
7.8 Conclusion	29
Bibliography	31
About the Author	36
About INTERVICT	36

**List of Abbreviations**

BSN	Burgerservicenummer
CBP	College Bescherming Persoonsgegevens
CIFAS	Credit Industry Fraud Avoidance System
COPS	Office of Community Policing Services
CRA	Credit Reporting Agency
DG	Directorate General
EU	European Union
FACTA	Fair and Accurate Credit Transactions Act
FIDIS	Future of Identity in the Information Society
FPEG	Fraud Prevention Expert Group
FTC	Federal Trade Commission
GAO	Government Accountability Office
IFF	Identity Fraud Forum
IFSC	Identity Fraud Steering Committee
ITRC	Identity Theft Resource Center
JRC	Joint Research Center
LSE	London School of Economics and Political Science
MOB	Maatschappelijk Overleg Betalingsverkeer
NVB	Nederlandse Vereniging van Banken
SSN	Social Security Number
UK	United Kingdom
US	United States

## Foreword

Cyber Crime and identity theft are becoming more and more synonymous. This is a logical development. Most Cyber criminals only want to make money. It is easier to take money from a lot of people by using identity theft vehicles such as Phishing sites and get away with it, than to try to extort a large sum of money from a big company that has the clout to get the investigative authorities moving. When we want to combat Cyber Crime it's therefore important also to have an insight in the way identity theft is committed and the way in which it is presently combated. This study, which was commissioned by the National Infrastructure Cyber Crime program (NICC) for the Identity track of the GOVCERT.NL 2006 Conference, presents the state-of-the-art of countering identity theft in the United States, the United Kingdom and the European Union. In addition it presents relevant lessons for Dutch policymakers. The study was executed by Nicole van der Meulen of the International Victimology Institute Tilburg (INTERVICT) of Tilburg University in the Netherlands. It is the opinion of the NICC that this independent study presents a very interesting overview of the current developments and therefore can be of great value in combating identity theft related Cyber Crime.

Dr. Edwin C. Mac Gillavry  
Project leader NICC

The National Infrastructure Cyber Crime program (NICC) is a public-private initiative to develop the Dutch infrastructure to combat Cyber Crime. Its primary task is to initiate public-private cooperation, conduct experiments and develop innovative ways to enhance the awareness of Cyber Crime.

Address NICC:  
National Infrastructure Cyber Crime  
ICTU  
P.O. Box 84011  
2508 AA Den Haag  
The Netherlands  
T +31 (0)70 888 79 46  
Nicc@ictu.nl

Address author:  
Nicole van der Meulen  
INTERVICT  
Tilburg University  
PO Box 90153  
5000 LE Tilburg  
The Netherlands  
T +31 13 466 3509  
N.S.vdrMeulen@uvt.nl

## 1. Introduction

Identity theft continuously manifests itself in the media as one of the fastest growing crimes of the twenty-first century. On a daily basis, newspapers provide readers everywhere with disturbing headlines about the tremendous financial costs and the increasing rate of victims identity theft causes. The major focus for the past few years has been on the United States (US) but recent developments indicate that other countries, both inside and outside of the European Union (EU), are hardly immune to this highly complex crime. As a result, numerous policy makers acknowledge that identity theft has become a major economic and societal problem; yet, hardly anyone manages to grasp the precise scope of problems identity theft causes. As the US Department of Treasury notes, “The lack of a standard definition makes it difficult to collect comprehensive, accurate data for quantifying the costs and incidents of identity theft.”<sup>1</sup> In addition to the difficulty of assessing the financial damage identity theft causes, researchers encounter an even greater obstacle when they try to delve into the unquantifiable damages victims incur. These non-financial costs are highly problematic and at times overlooked due to the strong emphasis on the financial damages the crime causes. With regard to non-financial costs the Identity Theft Resource Center (ITRC) provides the most comprehensive overview of the traumatic impact identity theft has on the lives of numerous victims. Through the ITRC’s study *Identity Theft: The Aftermath 2003* and its follow up *The Aftermath 2004*, the overall impact of identity theft on victims becomes painfully clear. Victims describe how their lives become ‘paralyzed’ as they are unable to obtain a mortgage, continuously blame themselves, and suffer “a significant strain in the relationships with their significant others.”<sup>2</sup> In addition to the damage identity theft causes victims, businesses, and society at large, policy makers are also especially concerned with the connection between identity theft, organized crime, and terrorism. As a result, the various harms identity theft brings into society force policy makers in different countries to try to develop means to prevent, detect, and manage the occurrence of identity theft.

In this report, I try to accomplish a number of tasks. First, I wish to provide an overview of the prevalence and developments of identity theft in three regions, the US, the UK, and the EU. Second, I present an inventory of the different policy initiatives introduced against identity theft in the US, the UK, and the EU. Third, I try, with the help of the inventory of the three cases, to provide an analysis of the different options available to policy makers and their costs, benefits, and potential effectiveness. Ultimately, through these three parts, I aim to identify relevant lessons for Dutch policy makers.

### 1.1 Case Justification

The US, the UK, and the EU provide an intriguing combination of regions to explore with regard to identity theft due to the difference both in prevalence and countermeasures introduced. Furthermore, the inclusion of the EU is significant due to the direct impact of EU initiatives on the Netherlands. The three geographical regions can also be classified along two spectra. First, the prevalence of identity theft in the three regions varies from relatively high, in the US, to relatively low, in the EU. Second, in terms of initiatives the US is arguably the most advanced and has been battling identity theft for an extensive number of years. The EU, on the other hand, is at this point primarily discussing possible initiatives without actually having taken any concrete or specific actions to combat identity theft. The UK fits quite nicely in the middle both in terms of prevalence and countermeasures introduced which

---

<sup>1</sup> United States (US) Department of Treasury 2005, p. 9.

<sup>2</sup> Identity Theft Resource Center 2003, p. 35.

allows for a good mixture of cases. The diversity in prevalence and initiatives provides a wide array of options to consider for the Netherlands.

## 1.2 Report Outline

The first section will provide a brief discussion on the definition of identity theft, which often varies across cultures and has a tendency to create unnecessary confusion. Through a brief discussion, I hope to provide the reader with an understanding of how different stakeholders and authors define the concept. The next section indicates the different types of and ways in which perpetrators commit identity theft. Thereafter, an analysis of the US, the UK, and the EU describes the prevalence and the numerous policy developments and concerns present in each of the regions. In the conclusion, the possible lessons and significant trade-offs are identified with regard to the Netherlands.

## **2. Identity Theft: In Search of a Definition**

As noted in the introduction, differences continue to exist with regard to definitions of identity theft. Part of the problem with establishing a broadly accepted definition is the different ideas individuals have when they speak of identity theft. An important element in defining the crime is, when does an individual or group commit identity theft? When he or she collects personal information? Tries to use the personal information to gain financial benefits? Or when the individual succeeds in gaining the financial benefits through posing as someone else? Graeme R. Newman & Megan M. McNally developed a framework which describes three basic stages of identity theft and breaks the crime down into different phases.

- **Time 1 (T1):** Time of initial offense (acquiring personal information) (...) The acquisition of personal information at T1 is the first step in a sequence leading to the commission of identity theft.
- **Time 2 (T2):** Identity theft. Personal information obtained at T1 may or may not be directly acquired by the offender who uses it at T2 to commit an act of identity theft.
- **Time 3 (T3):** Outcomes of identity theft. This is the time of discovery and potential criminal justice involvement regarding the act of identity theft, as well as the realization of losses by the victim. For offenders, these losses can be understood as gains - both financial and non-financial depending upon the type of identity theft victimization.<sup>3</sup>

These different phases could help to guide research on identity theft and to establish a better definition. They do not, however, provide a workable definition of identity theft. Currently, the most commonly cited definition is provided in the 1998 Federal Identity Theft and Assumption Deterrence Act which considers an individual to commit an act of identity theft when he or she “knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable state or local law.”<sup>4</sup> In the US this definition is by some considered too broad. Primarily private corporations dislike the fact that credit card fraud and account hijacking become part of identity theft under this definition. Julia S. Cheney notes how “the financial

---

<sup>3</sup> Newman & McNally 2005, p. 75.

<sup>4</sup> 18 U.S.C. 1028, Pub. Law 105-318, 112 Stat. 3007.

services industry tends to classify the fraudulent use of stolen card numbers as payment card fraud rather than identity theft.”<sup>5</sup> Differences of what identity theft precisely entails, therefore, exist between the public and the private sector.

Additionally, the prevalence of identity theft and identity fraud in other regions also brings about other definitions. These ‘cultural’ differences both in terms of terminology usage and definitions are crucial with regard to the latter part of this report, because the definitions and terms used by the different regions influence their perception of the problem and their subsequent countermeasures. Currently, the UK Home Office defines identity theft as an act which “occurs when sufficient information about an identity is obtained to facilitate Identity Fraud, irrespective of whether, in the case of an individual, the victim is alive or dead.”<sup>6</sup> Identity Fraud then “occurs when a False Identity or someone else’s identity details are used to support unlawful activity, or when someone avoids obligation/liability by falsely claiming that he/she was the victim of Identity Fraud.”<sup>7</sup> The importance of cultural context is also indicated by Roberto Binder and Martin Gill who note “In Britain both terms – identity theft and identity fraud – are used whereas in the United States identity theft prevails.”<sup>8</sup> Binder & Gill furthermore define identity theft and identity fraud as two distinct concepts. To the authors, identity theft applies to a perpetrator who takes over an existing identity whereas identity fraud is committed when an individual assumes a fictitious identity.



As a result, Binder & Gill identify the two terms as two mutually exclusive concepts. This is not particularly helpful when reading about or writing on identity theft and identity fraud. The UK, for example, as noted above uses the term identity fraud to include both the unlawful use of existing as well as non-existing identities. The same goes for a number of other countries. Consequently, defining identity theft and identity fraud as Binder & Gill do is not a viable option.

Other authors consider a different and more useful framework which, instead of presenting identity theft and identity fraud as two mutually exclusive concepts, presents a hierarchy of definitions and represents a relationship from broad to specific, encompassing additional elements of identity crime. Bert-Jaap Koops & Ronald Leenes propose such a framework in which they provide an umbrella term, identity-related crime, to include both identity fraud and identity theft. Koops & Leenes set forth three definitions:

- “Identity-related crime concerns all punishable activities that have identity as a target or a principal tool.”
- “Identity fraud is fraud committed with identity as a target or principal tool.”

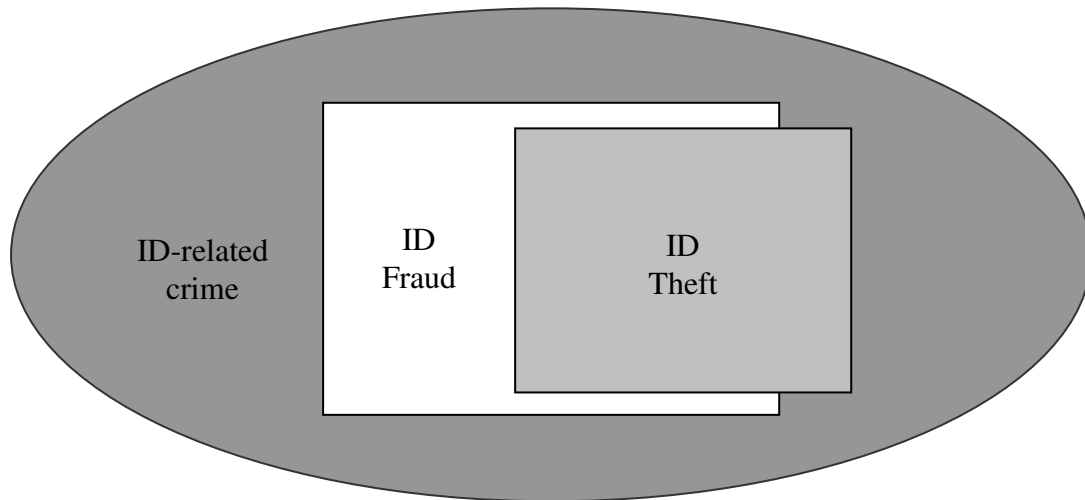
<sup>5</sup> Cheney 2005, p. 2.

<sup>6</sup> United Kingdom (UK) Home Office 2006a.

<sup>7</sup> UK Home Office 2006a.

<sup>8</sup> Binder & Gill 2005, p. 6.

- “Identity theft is fraud or another unlawful activity where the identity of an existing person is used as a target or principal tool without that person’s consent.”<sup>9</sup>



As can be seen from the above figure, identity fraud, according to Koops & Leenes, encompasses both the unlawful use of existing and non-existing persons. An important element of the definitional scheme is the small share of identity theft which does not fit into the category of identity fraud. This outskirts of identity theft is often termed criminal identity theft and will be elaborated upon in the next section. The definitional scheme, however, provides perhaps the most accurate reflection of the connection between identity theft, identity fraud, and the broad concept of identity-related crime due to the logical order of the three proposed definitions in the framework. Furthermore, its contextual range is certainly significant as the definitions are not restricted to any particular context. As John Gerring notes, “A concept that applies broadly is more useful than a concept with only a narrow range of application. A good concept stretches comfortably over many contexts; a poor concept, by contrast, is parochial – limited to a small linguistic turf.”<sup>10</sup> As a result, the definitions proposed by Koops & Leenes will be the definitions used in the subsequent analyses and conclusions of this report. For reasons of recognizability, however, I will use the terminology prevalent in each region at hand. Hence, the section on the US will predominantly refer to identity theft, and the section on the UK will mainly deal with the term identity fraud (which includes incidences of identity theft).

In addition to confusion surrounding the different definitions authors hold, terminology also causes interesting debates. Koops & Leenes recognize the potential problems associated with using the term identity ‘theft.’ The problems with using the concept of theft are significant especially with regard to potential legal ramifications. Under Canadian law, for example, “in order to be considered theft, a person must take an actual ‘thing’ and it must involve a deprivation to the owner. Therefore (...) a person who copies personal information (...) from a computer or official document and retains that information for future criminal use has not committed an offence under the Criminal Code.”<sup>11</sup> Clearly using the term identity theft increases the difficulty with regard to criminal law aspects but, as Elle La Lievre and Rodger Jamieson note, identity theft has more of a personal emotive impact than identity fraud because it presents the idea of identity ownership which is then stolen by another

<sup>9</sup> Koops & Leenes forthcoming 2006.

<sup>10</sup> Gerring 2001, p. 54.

<sup>11</sup> Consumer Measures Committee 2005, p. 5

individual.<sup>12</sup> An alternative is proposed by Gang Wang *et al.* who coin the term identity deception, especially focusing on criminal identity deception. Wang *et al.* note how “Identity deception includes the issue of identity theft or identity fraud (...) Identity deception is a broader concept than identity theft because impersonation is just one of many ways to alter an identity.”<sup>13</sup> Deception is arguably a more accurate reflection of the crime commonly referred to as identity theft since an offender deceives someone into thinking he or she is someone else. The disadvantage of using the term deception, however, is the negligence of the victim’s role, whose personal information is ‘stolen’ or used to commit the crime.

### 3. Identity Theft: One Concept, Many Faces

Identity theft is in a number of ways a catch-all phrase to describe a crime with many different faces. Identity theft is committed in different ways, for different reasons, and by different people. The first distinction which is primarily crucial in the US is the type of identity theft committed. Victims can fall prey to either financial identity theft or criminal identity theft. The former receives the most media attention while the latter is perhaps more damaging to the individual victim. In financial identity theft, the perpetrator uses personal information to gain financial benefits, through, for example, opening a new credit card account. With criminal identity theft, on the other hand, the perpetrator commits a (serious) crime and provides a ‘stolen’ identity to escape prosecution. When individuals become victims of criminal identity theft they may, for example, be initially stopped for a minor traffic violation, but upon checking their records the police officer finds a warrant out of their arrest for a serious crime like murder.<sup>14</sup> The identity theft victim is then wrongfully arrested.

Another important distinction to make is between identity theft which is committed over an existing account or whether the perpetrator opens up a new account. As previously noted, financial institutions dislike the inclusion of existing account fraud into the incidence of identity theft. The greater implications for the distinction are, however, those for the victims. In the US, financial institutions are generally more likely to assume liability for fraud related to existing accounts. Victims of ‘true name fraud’, the term describing identity theft for new (financial) accounts, find themselves in an especially difficult position. As Heather M. Howard notes ‘true name fraud’ “takes a greater toll on its victims than does account theft: their financial losses are more substantial, more difficult to discover, and take considerably longer to resolve.”<sup>15</sup>

Additionally, policy makers distinguish between identity theft which is committed as a direct or an indirect means. The Consumer Measures Committee in Canada for example notes, “It is important to remember identity theft is not always committed for its own sake (...) identity theft is commonly committed to further other criminal activity, such as organized crime and terrorism. Reducing incidences of identity theft may therefore help to reduce broader social harms, such as threats to national security.”<sup>16</sup> Financial identity theft, for example, is a prime instance of identity theft as an end in itself. The perpetrator simply uses the personal information to unlawfully obtain financial benefits. Identity theft becomes an indirect means to an end, however, when individuals illegally obtain personal information as a tool to commit an act of terrorism or engage in organized crime. Identity theft as a means to commit

---

<sup>12</sup> Le Lievre & Jamieson 2005, p. 7.

<sup>13</sup> Wang *et al.* 2004, p. 113.

<sup>14</sup> Binder & Gill 2005, p. 16.

<sup>15</sup> Howard 2005, p. 1266.

<sup>16</sup> The Consumer Measures Committee 2005, p. 6.

another crime, especially transnational organized crime or terrorism, is a major concern for national security and law enforcement agencies across the world. The attacks of September 11, 2001, certainly present an often-cited example of how terrorists can use false or 'stolen' personal information to carry out the rest of their operations.

Within the literature, both academic and non-academic, authors also make important distinctions between the different methods perpetrators of identity theft use. As Larry D. Johnson noted before the Committee on Government Reform, "The methods of identity criminals vary. 'Low tech' identity criminals obtain personal and financial identifiers by going through commercial and residential trash, a practice known as 'dumpster diving.' The theft of wallets, purses and mail is also a widespread practice employed by both individuals and organized groups."<sup>17</sup> These methods, although still available, have appeared to become less prevalent as a result of "the proliferation of computers and increased use of the Internet,"<sup>18</sup> which allowed 'high tech' identity theft to gain significant momentum. As Johnson furthermore notes, 'high tech' identity theft allowed perpetrators "to obtain information from company databases and web sites. In some cases, the information obtained is in the public domain; in others it is proprietary and is obtained by means of computer intrusion."<sup>19</sup> With the use of technology, possibilities for perpetrators have become nearly endless. The crucial note to make about the more recent ways individuals gain personal information is both the relative ease with which they manage to obtain the information and also the fact that they are not location-bound, which makes the ultimate capture nearly impossible. Recently, data security breaches and phishing have received the most media attention and arguably have caused a significant amount of damage. Phishing entails the sending of emails in which the perpetrator claims to be a representative from a financial institution or other kind of affiliation and pretends to need personal information from the recipient. When the recipient follows the link provided in the email, he or she enters a shadow website which directly leads his or her personal information to the perpetrator. Database breaches are also a rather valuable way for perpetrators to gain information because perpetrators receive significant amounts of personal data within a short amount of time. The ultimate challenge for policy makers is therefore to understand the continuous advancements perpetrators make with regard to the methods of obtaining personal information to commit identity theft.

The last distinction I will make here is especially important with regard to victimization. The previously discussed distinctions all concern identity theft where the perpetrator obtains or tries to obtain the personal information of an existing person. Within the broader scope of identity fraud, however, the perpetrator can also decide to simply provide an agency with false personal information. The important distinction between the use of personal information from an existing person versus information from a non-existing person is the ultimate victimization. Through identity theft, the person whose personal information is used to make fraudulent transactions or commit a crime becomes the primary victim. When a perpetrator commits identity fraud, using false personal information, the primary victim becomes, for example, the government, the financial institution, an online store, or a law enforcement agency. As David Lacey and Suresh Cuganesan note, "For the individual consumer to be impacted, the crime must be one of identity theft. However, organizations can be victims of the misuse of both real and fictitious identities. As such, organizations develop their prevention, detection, and recovery responses in relation to identity fraud rather than identity

---

<sup>17</sup> Johnson 2004, p. 52.

<sup>18</sup> Johnson 2004, p. 52.

<sup>19</sup> Johnson 2004, p. 52.

theft specifically.”<sup>20</sup> In an indirect way, however, the general public can also fall victim as a result of identity-related crime when the perpetrator uses false personal information to commit other crimes or acts of terrorism, as became evident in 2001.

#### 4. Identity Theft in Action

In this section, I will provide an overview of initiatives introduced in the US, the UK, and the EU to counter identity theft. As explained in section 2, for reasons of recognizability, I will use the terminology prevalent in the region at hand and the terminology used in the reports, i.e., the section on the US largely utilizes the term identity theft whereas the section on the UK deals primarily with identity fraud; in the EU, both terms are used. The reader should note that these terms are not always well-defined in the reports on which these sections are based, and may overlap. Nevertheless, it should generally be clear to which forms of identity-related crime the text is referring, and it is interesting to note on which types of identity-related crime the debate and policy in the various region centers – the difference in terminology is certainly indicative of a different focus and perspective in the various regions.

##### 4.1 The Fight Against Identity Theft in the US

###### *4.1.1 Prevalence in the US*

When it comes to identity theft, the US continues to dominate media headlines both inside and outside of its borders. The amount of victims and financial costs keeps on rising; yet, the precise damage identity theft causes American society remains relatively unclear. Diverse surveys and studies provide a scattered picture which fails to aid in generating a common understanding of the size and complexity of the problem. Additionally, John E. Matejkovic & Karen Eilers Lahey recognize how “Certain aspects of identity theft have long been criminal activities. Part of the problem with tracking the various incidents is that they usually are part of some other criminal activity.”<sup>21</sup> Among the various studies and surveys, the most cited statistics originate from the Identity Theft Data Clearinghouse, a complaint database maintained by the Federal Trade Commission (FTC) which reportedly received over 685,000 consumer complaints in 2005. In total, 37% of these complaints involved identity theft whereas 63% involved general fraud.<sup>22</sup> The most common form of identity theft reported by victims was credit card fraud (26%), followed by phone or utilities fraud (18%), bank fraud (17%), and employment fraud (12%). Victims also identified other important categories of identity theft which included government documents/benefits fraud (9%) and loan fraud (5%).<sup>23</sup> A comparison of identity theft over the previous three years provides a confusing picture. The percentages are going down whereas the actual number of complaints continues to rise. The explanation for this seemingly contradictory representation is the relatively more significant rise in other types of fraud. The declining percentages of identity theft complaints, from 40% in 2003 to 37% in 2005, leads some to conclude identity theft itself is decreasing, or at least remaining steady, rather than increasing. As Thomas M. Lenard & Paul H. Rubin note, the most comprehensive data on identity theft, which stems from two surveys commissioned by the FTC and conducted by research firms Synovate and Javelin in 2003 and 2004, respectively, demonstrate the same results, which, according to Lenard & Rubin is an indication “that fears of identity theft being a rapidly growing problem are exaggerated.

---

<sup>20</sup> Lacey & Cuganesan 2004, p. 245.

<sup>21</sup> Matejkovic & Lahey 2001, p. 224.

<sup>22</sup> Identity Theft Data Clearinghouse 2006.

<sup>23</sup> Identity Theft Data Clearinghouse 2006.

Indeed the actual incidence of identity theft of all forms decreased from 4.6 percent of the adult population to 4.25 percent (...)”<sup>24</sup> Lenard & Rubin, as a result, conclude identity theft is remaining constant and even hint that the problem is decreasing. This conclusion appears to disregard other factors which could skew statistics and provide a misrepresentation. As noted previously, the percentage of identity theft complaints decreased over the past three years; yet, the number of complaints increased from 215,177 in 2003 to 255,565 in 2005, which is arguably an important indicator demonstrating identity theft is hardly declining. Additionally, when closely analyzing the statistical trends over the past three years readers can hardly ignore the important developments with regard to the types of identity theft the public falls victim to. While credit card fraud is still the largest category of identity theft complaints, it has been steadily declining from 32% in 2003 to 26% in 2005.<sup>25</sup> The other categories largely remained steady except for the ‘Other’ category which demonstrates an increase of 6%, precisely explaining the decrease in credit card fraud. This trend could potentially be explained through the introduction of different methods identity thieves have developed over the past three years. A trend which policy makers and the FTC should try to take a closer look at. An important step with regard to this trend is trying to understand what kind of complaints constitute the ‘Other’ category.

#### *4.1.2 Policy Developments*

The problem of identity theft receives considerable attention from policy makers at state as well as federal levels of government. Furthermore, identity theft is a significant issue within the different branches of government and agencies in the US. As a result, initiatives to counter identity theft are diverse and difficult to divide into particular categories. Within the upcoming sections, I have tried to categorize policy developments according to their overarching similarities. Overall, I have tried to present the initiatives in a chronological order.

##### 4.1.2.1 Criminalization

In 1996, the State of Arizona became the first government to initiate legislative action against identity theft through passing a law which made identity theft a felony and punishable with a prison sentence of up to one and a half year in addition to restitution and a fine of up to \$150,000.<sup>26</sup> After California followed Arizona’s lead, the US government introduced its first initiative. The 1998 Federal Identity Theft and Assumption Deterrence Act identified identity theft as a federal crime, provided a legal definition, and outlined penalties for any violation of the Act. Furthermore, the Identity Theft Data Clearinghouse was created pursuant to the Act and began its operations in November 1999. The Clearinghouse provides valuable information to victims in an attempt to mitigate their losses and it also operates as a database to track identity theft complaints. To many the Act represented an important first step with regard to the fight against identity theft. Matejkovic & Lahey claim the Act accomplished a number of significant tasks. Among them are the classification of individuals as primary

---

<sup>24</sup> Lenard & Rubin 2006, p. 44.

<sup>25</sup> Identity Theft Data Clearinghouse 2006.

<sup>26</sup> The Arizona Revised Statute § 13-2008 considers someone to commit identity theft when “A person commits taking the identity of another person or entity if the person knowingly takes, purchases, manufactures, records, possesses or uses any personal identifying information or entity identifying information of another person or entity, including a real or fictitious person or entity, without the consent of that other person or entity, with the intent to obtain or use the other person’s or entity’s identity for any unlawful purpose or to cause loss to a person or entity whether or not the person or entity actually suffers any economic loss as a result of the offense.”

victims as opposed to financial institutions, and the federalization of the crime, which gives victims the opportunity to request aid from law enforcement officials.<sup>27</sup>

In 2004, the US Congress increased the potential punishments for convicted identity thieves. The Identity Theft Penalty Enhancement Act adds a two year prison sentence to any individual convicted of using a stolen credit card number or other personal information to commit a crime.<sup>28</sup> Furthermore, the Act also directs the US Sentencing Commission to think about enhancing the penalties for employees who illegally obtain personal data from their company's database. When he signed the bill into law, President George W. Bush remarked how the Act would "dramatically strengthen the fight against identity theft and fraud. Prosecutors across the country report that sentences for these crimes do not reflect the damage done to the victim. Too often, those convicted have been sentenced to little or no time in prison. This changes today."<sup>29</sup> Whether enhancing penalties for identity theft violations is a step in the right direction is arguable. According to Betsey Broder, Assistant Director for the Federal Trade Commission's Division of Planning and Information, the Act will make it more likely for an identity thief to be prosecuted because "A prosecutor is less likely to bring a case if they're not going to get any serious jail time when the [sic] get a conviction."<sup>30</sup> The Act, therefore, is not a means to solve the problem but rather to increase the incentive for both prosecutors and law enforcement personnel to take a greater effort to convict and catch identity thieves. Additionally, one of the primary motives behind increasing the penalties is the fight against terrorism. As Dennis M. Lormel, Chief Terrorist Financial Review Group FBI, noted in his Congressional Testimony, "Terrorists and terrorist groups require funding to perpetrate their terrorist agendas (...) There is virtually no financing method that has not at some level been exploited by these groups. Identity theft is a key catalyst fuelling many of these methods."<sup>31</sup> Consequently, the ultimate drive behind the Act may be a good indication for its implementation. Prosecutors may be more inclined to make a greater effort to prosecute identity thieves but only if, or primarily if, they have some sort of terrorist connection. Therefore, if identity theft is committed as a stand alone crime penalties remain the same. An additional drawback is the fact that the Act applies "only to U.S. Postal Service and interstate acts of identity theft. For acts of intrastate identity theft, many states still do not classify this action as a felony and the criminal is given a lenient sentence."<sup>32</sup> The effectiveness of higher sentences, however, primarily relies on the conviction rate which appears to be relatively low. As a result, policy makers perhaps should focus more on prevention of identity theft through increased security instead of deterrence through higher sentencing.

#### 4.1.2.2 Increasing Organizational Responsibility

In the following years after the Identity Theft Assumption and Deterrence Act, Congress shifted its focus and began to draft legislation of a more preventative nature through increasing organizational responsibility. The shift began in 1999 with the introduction of the Gramm-Leach-Bliley Act<sup>33</sup> which became an essential piece of legislation through its provisions on the mandatory protection of consumers' personal financial information by

---

<sup>27</sup> Matejkovic & Lahey 2001.

<sup>28</sup> Identity Theft Penalty Enhancement Act of 2004, Pub. L. No. 108-275, 118 Stat. 831 (2004).

<sup>29</sup> Quoted in Robin K. Olson *et al.* 2005, p. 15.

<sup>30</sup> Qtd. in McGuire 2004.

<sup>31</sup> Lormel 2002, p. 1.

<sup>32</sup> Olson *et al.* 2005, p. 16.

<sup>33</sup> 15 USC, Subchapter I, Sec. 6801-6809 Disclosure of Nonpublic Personal Information.

financial institutions. More recently, California initiated legislation which requires private corporations to notify consumers in case of a data security breach. In 2003, California became the first state to pass two significant data security breach laws. First, the California Security Breach Information Act<sup>34</sup> requires any company which stores customer data electronically to notify its California customers of a security breach to the company's computer system when the company knows or has reason to believe that unencrypted information about customers has been disclosed. The second law, commonly known as the California Financial Information Privacy Act,<sup>35</sup> establishes new limits on the ability of financial institutions to share nonpublic personal information about their customers with affiliates and third parties. The legislation hardly comes as a surprise after hackers gained access to the state government's payroll database, which contained sensitive personal information of over 250,000 state employees, in 2002. The members of the California legislature were among the employees whose personal information was exposed through the data security breach. Benjamin Wright describes the onset for the current laws when he writes, "Many employees, including the legislators, felt the California government was too slow to notify them about the burglary."<sup>36</sup> Data security breach notification legislation is also an important debate at the federal level, especially after some particularly high profile cases involving major data security breaches. In the most highly publicized case, Choicepoint, a company which obtains and sells personal information, including names, Social Security Numbers (SSNs), birth dates, employment information, and credit histories to more than 50,000 businesses, settled a case after the FTC pressed charges as a result of a significant data security breach in 2005. The data security breach caused at least 800 cases of identity theft and personal financial records of approximately 163,000 consumers became available for identity thieves to take advantage of. The FTC pressed charges against Choicepoint claiming it "did not have reasonable procedures to screen prospective subscribers, and turned over consumers' sensitive personal information to subscribers whose applications raised obvious 'red flags.'"<sup>37</sup> Furthermore, the FTC also claimed Choicepoint was in violation of FTC provisions because the company made false and misleading statements about the privacy of consumer information. Choicepoint, ultimately, had to pay a total of \$15 million, of which two thirds for civil penalties and the other third for consumer redress. The settlement became the largest to date.

Additionally, in 2003, Congress passed, and the President signed into law, the Fair and Accurate Credit Transactions Act (FACTA).<sup>38</sup> FACTA is another initiative which increases organizational responsibility. FACTA provides a number of provisions to fight identity theft, among these are "compulsory credit card number truncation on receipts, mandates to card issuers to investigate change of address and new card requests, fraud alert requirements by credit reporting agencies, mandatory blocking of identity theft-related information on credit reports, and free annual credit reports."<sup>39</sup> The Act, therefore, serves a number of purposes. First, the truncation of credit numbers on receipts is an effort to prevent identity theft from occurring. Second, the mandate to investigate requests for new cards and address changes tries to aid in the detection of identity theft attempts. Third, placing a fraud alert on someone's credit card is an instrument to stop repeat identity theft.<sup>40</sup> Fourth, the mandatory

<sup>34</sup> California Civil Code § 1798.82.

<sup>35</sup> California Civil Code § 1798.29.

<sup>36</sup> Wright 2004, p. 171.

<sup>37</sup> Federal Trade Commission 2006, p.1.

<sup>38</sup> Fair and Accurate Credit Transactions Act 2003, Public Law 108-159.

<sup>39</sup> Linnhoff & Langenderfer 2004, p. 205

<sup>40</sup> A fraud or security alert is a process used by consumers to protect their credit. A fraud alert is a statement added to a consumer's credit report which asks credit issuers to check with the consumer before issuing a new

blocking of identity-theft related information is a means for the victim to return to his or her original credit rating and therefore reduce the devastating damage of the crime. The annual credit reports are certainly a valid tool for individuals to discover any irregularity within their credit history as a result of identity theft.<sup>41</sup> Especially, with the relatively short statute of limitations, the annual credit reports can help citizens to actually have a legitimate claim in court in case they fall victim to an identity thief. As to the effectiveness of these measures, some appear skeptic. The ITRC indicates on its website how a fraud alert on a credit report is not necessarily a guarantee a company or financial institution is not going to extend credit to the perpetrator, because they can simply ignore the alert.<sup>42</sup> A more effective means to prevent any further acts of identity theft is the credit freeze which a number of states introduced. The credit freeze allows residents to prevent anyone from viewing their credit reports and opening up a new line of credit. Even individuals who have never been victims of identity theft can request credit agencies to place a credit freeze on their account for a fee. In California, for example, residents pay \$10 to each Credit Reporting Agency (CRAs)<sup>43</sup> (three in total) to freeze their credit. Due to the fact that the credit freeze is an initiative taken at the state level by only a restricted number of states, not everyone in the US can take advantage of this option. The inability of some victims to take advantage of the credit freeze provides a significant strain on their opportunity to prevent identity theft from occurring or reoccurring. These victims find themselves in a rather defenseless position as will become evident later on in subsection 4.1.2.5.

Another significant element of FACTA was the request made by Congress to the Department of Treasury to undertake a study on “the use of biometrics and other similar technologies to reduce the incidence and costs to society of identity theft by providing convincing evidence of who actually performed a given financial transaction.”<sup>44</sup> The Department of Treasury concluded in its study how biometric technology is not a ‘silver bullet’ to reduce identity theft and “Biometrics are not likely in the near term to be very useful to confirm the true identity of an individual at the initial point of opening an account or submitting an application to a financial institution if the person has no prior relationship with the institutions.”<sup>45</sup> Additionally, the Department notes the major obstacles which make biometrics at this point in time a sub-optimal solution. These obstacles include consumer concerns, costs, lack of

---

line of credit. As a result, the fraud alert is meant to strengthen the verification process which should then prevent identity theft from taking place. There are two types of fraud alerts. The first is an initial fraud alert which any consumer can request. The initial alert works for 90 days and gives consumers the right to one free credit report from all three major CRAs. The extended victim alert remains on a consumer’s record for seven years but this option is only available for victims of identity theft who have an identity theft report which they filed with a Federal, State or local law enforcement agency. Another option is only restricted to active duty personnel in branches of the military. They can file an active duty alert which remains on their credit report for one year.

<sup>41</sup> Consumers also use alternative methods to specifically prevent credit card fraud. Instead of signing the back of the credit card, they write in ‘check id’ or ‘see id’ in the hope that when identity thieves steal their credit card they will be unable to use it because they do not have a matching form of identification to go along with the credit card. The effectiveness of this method is highly dependent upon the employees of stores and their commitment to verifying that the person using the credit card actually matches the person standing in front of them. Furthermore with online transactions this consumer action is of course useless.

<sup>42</sup> ITRC 2005. The ITRC specifically notes how “there is no law that requires issuers to honor this request. We find that it works about 50-70% of the time.”

<sup>43</sup> Credit Reporting Agencies are private corporations which collect information about citizens and their credit history from a number of different sources including public records and creditors. CRAs make credit histories of individuals available to, among others, employers and credit issuers.

<sup>44</sup> Qtd. in US Department of Treasury 2005, p. 69.

<sup>45</sup> US Department of Treasury 2005, p. 70.

accuracy and reliability of technology, and the absence of interoperability of biometric systems.

#### 4.1.2.3 Use of Social Security Numbers

Besides criminalization and increasing organizational responsibility, Congress also tries to limit the use of SSNs, which is a particularly vulnerable aspect of the American identification structure. An SSN is the main identifier for both citizens and permanent residents. During phone conversations with financial institutions, an SSN is often an important way to gain information about an account. As Linnhoff and Langenderfer recognize, “Armed with an SSN, a would-be identity thief needs very little additional information to effectively steal an individual’s identity and wreak havoc.”<sup>46</sup> Consequently, legislative proposals try to limit the use and display of SSNs. The most radical, and arguably most effective, proposals urge a return to the original use of SSNs, which is identification for tax and social security reasons only. The possible implementation of a return to the original purpose of SSNs appears to be unlikely due to the severe institutional costs it would incur. When an identity thief obtains an SSN it is not necessarily a direct result from careless use by an individual; rather, SSNs appear on a number of public documents provided by states, local jurisdictions, and judicial courts. In addition to public agencies, private entities also keep documents which display the SSNs of individuals. These private entities include information resellers, CRAs, and health care organizations.<sup>47</sup> The Government Accountability Office (GAO) recently concluded “Although some action has been taken at the federal and state level to protect SSNs, more could be done.”<sup>48</sup> GAO notes how the US lacks a comprehensive law regulating the use and display of SSNs, while certain federal laws do restrict the use and display of SSNs by both public and private sector entities.<sup>49</sup> The importance of a comprehensive law leads GAO to propose and recommend that Congress needs to gather a group containing representatives of local, state, and federal government officials who can develop a unified approach to protect SSNs at all levels of government.<sup>50</sup>

#### 4.1.2.4 Law Enforcement Initiatives

While politicians devote significant attention to establishing means in their fight against identity theft, law enforcement officials also try to compensate for their previous lack of assistance towards identity theft victims. In May 2006, the Office of Community Oriented Policing Services (COPS) developed a national strategy to combat identity theft. COPS provided seven recommendations which could help law enforcement officials at all levels of government to provide more effective assistance to victims and to fight identity theft.<sup>51</sup> The recommendations relate to the seven components COPS considers vital for effective crime prevention and detection. The first is partnership and collaboration, where COPS emphasizes the need for state-level coordination centers to provide crime analysis, victim assistance, statewide investigations, and other necessary services. Furthermore, COPS reemphasizes the need for law enforcement officials to promote collaboration, cooperation, and intelligence fusion among the different agencies involved. Second, with regard to reporting procedures, COPS highlights the need for law enforcement officials to record any report of identity theft

---

<sup>46</sup> Linnhoff & Langenderfer 2004, p. 208.

<sup>47</sup> Government Accountability Office (GAO) 2006, p. 1.

<sup>48</sup> GAO 2006, p. 2.

<sup>49</sup> GAO 2006, p. 9.

<sup>50</sup> GAO 2006, p. 15.

<sup>51</sup> Office of Community Oriented Policing Services (COPS) 2006.

provided in the geographic jurisdiction of the victim, regardless of where the crime actually occurred. In providing this recommendation, COPS tries to prevent a continuance of behavior displayed by especially local law enforcement officials who often claim the crime is someone else's problem because it occurred in a different jurisdiction. Third, COPS recommends improving victim assistance through developing standard operating procedures (SOP) to help victims and identify the available sources of victim assistance. Fourth, increase public awareness through a national campaign, which focuses on prevention and response techniques. Fifth, COPS recommends establishing a database which contains all legislative initiatives at both state and federal level, which can help both in terms of efficiency and in the development of a comprehensive overview for businesses. In the last two recommendations, COPS identifies the need for more adequate training and better information protection to prevent and respond to identity theft.

#### 4.1.2.5 Victims of Identity Theft and the American Judicial System

In addition to legislative initiatives and trying to receive aid from law enforcement agencies, victims of identity theft also try to use the judicial system to their advantage. The recent success of the FTC against Choicepoint, however, should not overshadow the tremendous judicial obstacles individual victims encounter when trying to press charges against private corporations, primarily financial institutions. In 2001, for example, the US Supreme Court ruled against Adelaide Andrews, a victim of identity theft, claiming the statute of limitations had expired. The statute of limitations, which in this case is two years, begins, according to the Court, at the point when the perpetrator begins his or her scheme rather than when the victim finds out. In the case of Adelaide, this left her without any restitution, because she found out about the perpetrator's actions in 1995, only after she inquired about refinancing her mortgage.<sup>52</sup> Adelaide, however, did not file an official complaint against the CRAs involved until October 1996.<sup>53</sup> The perpetrator's actions began in 1993, when a doctor's receptionist, Andrea Andrews, copied all of Adelaide's personal information from a Patient Information form and subsequently relocated to Las Vegas, Nevada where she used Adelaide's information to open a number of accounts and to rent an apartment without ever making any payments. The decision made in Adelaide's case with regard to the statute of limitations provides a particularly negative precedence for future plaintiffs who fall victim to identity theft and only discover this after the statute has expired.

Besides statute of limitations hurdles, victims also encounter other obstacles when they try to prove corporate liability. The first of the four basic elements of a negligence claim requires the defendant to have a duty of care towards the plaintiff. Proving a duty of care has provided a particularly difficult, at times impossible, task for victims. In *Huggins v. Citibank, N.A., et al.*,<sup>54</sup> for example, the plaintiff, a victim of identity theft, pressed charges against three banks, Citibank, Capital One Services, and Premier Bankcard, claiming the banks were liable for "negligent enablement of imposter fraud" because the banks failed to carefully scrutinize the personal information provided on the credit application. The South Carolina Supreme Court dismissed the plaintiff's claim because it did not consider a duty of care to exist from the defendant towards the plaintiff, a non-customer. In order for the duty of care to exist, according to the Court, a legal relationship must exist between the plaintiff and the defendant, which was not the case here. The Court ultimately explained how "We are greatly concerned

---

<sup>52</sup> Discussed in Shoudt 2002.

<sup>53</sup> In her case, Adelaide Andrews alleged the CRAs TRW and Trans Union Corp violated provisions of the Federal Credit Reporting Act (FCRA) the predecessor of FACTA.

<sup>54</sup> *Huggins v. Citibank, N.A.*, 355 S.C. 329 (2003).

about the rampant growth of identity theft and financial fraud in this country. Moreover, we are certain that some identity theft could be prevented if credit card issuers carefully scrutinized credit card applications. Nevertheless, we agree with the New York appellate court decision in *Polzer v. TRW, Inc.*, (...) and decline to recognize a legal duty of care between credit card issuers and those individuals whose identities may be stolen. The relationship, if any, between credit card issuers and potential victims of identity theft is far too attenuated to rise to the level of a duty between them.”<sup>55</sup> Although the recent data security breach legislation in California provides substantial support for victims to prove corporate liability when a company fails to notify them, non-customers continue to be a particularly defenseless population under current law.

#### 4.1.2.6 Most Recent Efforts

In May 2006, the US government installed its most recent effort to fight identity theft. President Bush issued an executive order which launches the Identity Theft Task Force.<sup>56</sup> The task force is assigned to develop a strategic plan to enhance the effectiveness and efficiency of government efforts to deter, prevent, detect, investigate, and prosecute identity theft. Furthermore, during the same time the FTC launched a public awareness campaign. The national education program, titled *AvoID Theft: Deter, Detect, Defend*, aims to educate the public about identity theft while at the same time providing them with valuable tips on how to protect their personal information. The FTC distributed 4,500 education kits to victim advocates across the nation. The national education campaign and the introduction of the Identity Theft Task Force are the most recent efforts in the American battle against identity theft. As a result, commentary on the initiatives is scarce but initial reactions are generally positive and hopeful. Victim advocates warmly welcome the additional effort to increase public awareness, which will certainly be helpful for a part of the identity theft problem. As Johnson notes, however, “It is important to recognize that public education efforts can only go so far with combating the growth of identity crime. Because SSNs, in conjunction with other personal and financial identifiers, are used for such a wide variety of record keeping and credit related applications, even a consumer who takes appropriate precautions to safeguard such information is not immune from becoming a victim.”<sup>57</sup> As a result other initiatives need to provide additional support in the fight against identity theft.

#### 4.1.2.7 Effectiveness

As to the effectiveness of the current enacted and proposed legislation, it is difficult to provide any concrete conclusions. Identity theft continues to rise in the US and there appears to be a lack of empirical studies examining the effectiveness of current regulatory initiatives. The current literature<sup>58</sup> simply reflects on the possible effectiveness of recently proposed or passed legislation. From their overviews, however, it becomes clear that the potentially most effective measures often lead to a conflict of interest between consumer, business, and government entity. Furthermore, more effective measures also appear especially costly. A major example is the problematic nature of SSNs. The most extreme and arguably the most effective measure is to restructure the entire system and therefore eliminate the weakness of SSN usage. Yet, to many these changes are either too costly or too inconvenient. Instead, current legislation proposes the truncation of SSNs on receipts and credit reports; although

<sup>55</sup> *Huggins v. Citibank, N.A.*, 355 S.C. 329 (2003).

<sup>56</sup> Executive Order 13402 - Strengthening Federal Efforts To Protect Against Identity Theft (2006).

<sup>57</sup> Johnson 2004, p. 56.

<sup>58</sup> See for example Linnhoff & Langenderfer 2004; Pastrokos 2004; Holtfreter & Holtfreter 2006.

this may make it more difficult for identity thieves to gather the information the current problems continue due to the fact that many identity thieves already have numerous SSNs to do business with and because they are still such an integral part of the American identification infrastructure.

#### *4.1.3 Policy Conflicts and Concerns*

The first move made by policy makers in the US was to criminalize identity theft. Whether this move is effective is highly disputed by many stakeholders, although the majority recognize that while criminalization serves an important function within the overall fight against identity theft it cannot serve as a final solution to the problem. Arizona, for example, continues to be the identity theft capitol of the US despite being the first state to initiate legislation to criminalize identity theft.<sup>59</sup> The more recent Identity Theft Penalty Enhancement Act is therefore an initiative which appears to receive large support from officials involved in national security; yet, considering the low conviction rate of identity thieves, higher sentences may not be the most effective deterrent to stop or decrease identity theft.

A shift towards an increase of organizational responsibility, on the other hand, also brings along its own conflicts. Organizations wish to solve their problems without governmental interference and critics of governmental policy claim current legislation discourages businesses to be honest about security breaches. Increasing organizational responsibility, despite the conflict of interest, is an important step because as numerous authors notice private corporations are extremely sloppy when it comes to verification processes of applications. Furthermore, policy makers recognize how the majority of corporations do not make security a crucial issue on the agenda. As Bill Conner notes, “There are several reasons for the lack of progress. One, companies don’t know what to do. Many companies don’t understand the scope or threat and how to respond. As a result, they pretend the problem doesn’t exist, and, if it does, it won’t hurt them. Second, it is not a corporate priority. Even if they understand it, many firms refuse to make it an executive priority.”<sup>60</sup>

Policy conflicts also occur as a result of the federal nature of the American political system. Considering both state and federal statutes exist, not each individual or business is protected in the same way. FACTA, for example, “preempts state law and thus limits individual state efforts to impose stronger privacy policies than are set at the federal level...when federal law is inadequate to protect the public, preemption effectively denies relief to citizens of those states inclined to provide it.”<sup>61</sup> Whether federal laws and initiatives are inadequate is clearly open for debate and highly depends on which approach an individual takes. What has, however, become clear over the past few years is that state law has a tendency to be about ten steps ahead of federal law with regard to identity theft legislation. Major examples include Arizona in 1996 with the first identity theft law and California in 2003 as the first state to demand companies to notify consumers when a data security breach occurs. Currently, the federal government is proposing a number of initiatives which would make companies responsible for notifying consumers of a data security breach. From this observation follows a tentative conclusion that federal law can be considered inadequate because it is too reactive and generally too late when it does indeed react. However, what must be taken into

---

<sup>59</sup> Identity Theft Data Clearinghouse 2006.

<sup>60</sup> Conner 2004, p. 97.

<sup>61</sup> Linnhoff & Langenderfer 2004, p. 215.

consideration is that at the federal level there are of course far more competing perspectives and interests than at the state level.

## 4.2 The UK

### *4.2.1 Prevalence*

According to statistics published in February 2006, the UK economy suffers a financial loss of £1.7 billion per year as a result of identity fraud, a significant increase from previous years.<sup>62</sup> In 2002, for example, the Cabinet Office reported a loss of £1.3 billion per year. The Cabinet Office furthermore claimed the presented amount is far below the actual damage caused to the UK economy, because they only rely on available data which represents but a part of the whole figure.<sup>63</sup> On the other hand, however, others disagree and claim identity fraud causes far less financial damage and is exaggerated to assist the Government in gathering support for new legislative initiatives. The rate of victims, however, is clearly increasing. According to data gathered by Credit Industry Fraud Avoidance System (CIFAS), 43,000 reported being a victim of identity theft in 2003, as compared to 32,000 in the previous year.<sup>64</sup> Victims in the UK are in a particularly defenseless position as financial institutions and private corporations are the only victims recognized under the law. As will become clear later on, the UK lacks a law which specifically defines identity theft as a crime.

### *4.2.2 Policy Developments*

Although individual disputes about figures continue to exist, few contest identity fraud is prevalent in the UK and deserves considerable attention. In *Identity Fraud: A Study*, the Cabinet Office clearly emphasizes the crucial link between identity fraud and other forms of crime, including human and drug trafficking, money-laundering, and organized crime. In terms of counter-fraud activity, therefore, the authors recommend and urge for “more effective joint working, more sharing of data and intelligence and more active and effective prosecution policies.”<sup>65</sup>

As a result of the study conducted in 2002, the UK government heightened its initiatives to develop means to prevent and detect identity fraud. The Home Office created the Identity Fraud Steering Committee (IFSC) and the Identity Fraud Forum (IFF) in 2003, which developed a framework to identify effective measures to prevent and react to subsequent occurrences of identity fraud. More specifically, both IFSC and IFF members highlight a number of significant priorities in their work to reduce the occurrence of identity fraud. These include:

- (a) identify new opportunities for data-sharing across the public and private sectors;
- (b) reduce fraud involving the impersonation of deceased persons;
- (c) establish the cost of identity fraud to the UK economy on an ongoing basis;
- (d) researching the impact of identity fraud on victims and statistically tracking those cases;

---

<sup>62</sup> United Kingdom Home Office 2006c.

<sup>63</sup> UK Cabinet Office 2002.

<sup>64</sup> Credit Industry Fraud Avoidance System (CIFAS) 2004.

<sup>65</sup> UK Cabinet Office 2002, p. 27.

(e) improve both the public awareness of identity fraud through joint working with the financial services industry and the training provided to those in the financial sector responsible for checking customers' identity.<sup>66</sup>

As a result of these priorities, the IFSC and the IFF managed to develop a number of regulatory instruments in their battle against identity fraud. Important measures introduced by the Government primarily include aligning penalties, defining a new criminal offense, developing and sharing good practice, and raising public awareness. The Government decided to increase the maximum punishment for fraudulently obtaining a driver's license from a maximum fine of £2,500 to a maximum two year prison sentence, which is the current punishment for fraudulently obtaining a passport.<sup>67</sup> Furthermore, in 2003 the Government decided to introduce a new criminal offense. Under the new criminal offense, any individual who is either in possession or in control of false identity documents, whether genuine documents illegally obtained or derived from another person, is in violation of the law and subject to criminal sanctions. The underlying motive for the introduction of a new criminal offense is the connection between use of false identity documents and organized crime; consequently, the UK government hopes to use the new offense to provide the police with additional means "to disrupt the activities of organised criminals in the early stages of their crimes."<sup>68</sup> The new offense is part of the Identity Cards Act, which will later be elaborated upon.

With regard to the public, the UK launched a number of efforts to increase awareness among its citizens. First, the Home Office IFSC launched a website ([www.identity-theft.org.uk](http://www.identity-theft.org.uk)), which, in addition to raising awareness, provides advice on how to prevent identity theft and also identifies the actions victims of identity theft can take to resolve their issues. Second, Home Office Minister Andy Burnham launched an awareness campaign in 2005 to increase awareness and educate the public on prevention of identity theft while also identifying the available means for identity theft victims. Additionally, as suggested by the Cabinet Office in 2002, a number of government agencies and other associations increased their cooperation to develop and share good practices to combat identity fraud.

Compared to the previously listed initiatives, the hotly debated Identity Cards Act of 2006 is the most radical means to combat identity fraud. The Act is a result of a rather lengthy legislative process, which began a number of years ago but failed to gain significant momentum until after the terrorist attacks of September 11, 2001. Consequently, the Queen officially introduced the Identity Cards Bill in her speech on November 23, 2004. A few days later, on November 29, the bill was officially introduced to the House of Commons, after a two and a half years gestation.<sup>69</sup> On December 20, this legislation was debated (in Second Reading) in the Commons and was considered in Committee during the following month. After the bill passed to the House of Lords, elections were on the horizon and as a result there was insufficient time to debate the matter. Parliament was dissolved on April 11 before general elections took place on May 5, 2005. During its election campaign, the Labour party proclaimed how upon their return to power they would introduce identification cards, including biometric data, and a national register which stores the personal data. Interestingly enough, ten years earlier, Tony Blair had proclaimed, during a Labour Party Conference, "We all suffer crime, the poorest and vulnerable most of all, it is the duty of government to

---

<sup>66</sup> Courtney 2005, p. 1.

<sup>67</sup> UK Home Office 2006b.

<sup>68</sup> UK Home Office 2006b.

<sup>69</sup> London School of Economics and Political Science (LSE) 2005.

protect them. But we can make choices in spending too. And instead of wasting hundreds of millions of pounds on compulsory ID cards as the Tory right demand, let that money provide thousands of extra police officers on the beat in our local communities.”<sup>70</sup> Upon their return to power, however, Labour held true to its latest promise and reintroduced the identity cards bill. The Identity Cards Bill passed in March 2006, but the debate hardly died out and current developments indicate the fragility of the entire scheme. Combating identity fraud and identity theft is one of five main purposes of the Identity Cards Act. The others include combating terrorism, organized crime, immigration and illegal employment, and preventing further benefit fraud.<sup>71</sup> To prevent and combat these ‘evils of society’, the Identity Cards Act introduces the following measures. All individuals who renew their passport in or after 2008 will become part of the future National Identity Register. This database will contain the biometric data of residents along with current and past UK and overseas places of residence. Furthermore, residents and citizens will receive a British National Identity Card, which will include the following biometric data: fingerprint, iris scan, and facial scan. Due to a late amendment, however, citizens are now allowed to decline the Identity Card until 2010; yet, they do have to pay the fee and have their information become part of the register.

#### 4.2.3 Policy Conflicts and Concerns

The Government claims that the identification cards together with the central database will assist them in providing for increased national security; yet, critics raise particular concerns with regard to this claim and potential conflicts of privacy and previous laws, both national and European. In their summary, the authors of the London School of Economics and Political Science (LSE) report entitled *The Identity Project: An Assessment of the UK Identity Cards Bill & Its Implications* write “the proposals currently being considered by Parliament are neither safe nor appropriate. There was an overwhelming view expressed by stakeholders in this Report that the proposals are *too complex, technically unsafe, overly prescriptive and lack a foundation of public trust and confidence.*”<sup>72</sup> In addition to their general conclusions, the authors also specifically indicate how the Identity Cards initiative is perhaps not the best way to fight future occurrences of identity theft. Instead, they suggest the public may better protect itself through “greater control over the disclosure of their own personal information.”<sup>73</sup> Furthermore, the development of a central database with an individual identification number to fight identity theft appears incomprehensible due to significant problems in both the US and Australia as a result of fraudulent use of SSNs and Tax File Numbers, respectively. The primary problem with a central number, both in the US, Australia, and possibly the UK in the future, is the personal information linked to the central number. Basically, if both the public and private sector only require individuals to write down or mention their identification number to gain access to numerous services, then obtaining these numbers becomes an open gateway to identity theft, as it has in other countries. Other important concerns, specifically regarding identity fraud and the Identity Cards initiative, include the “danger that in many day-to-day situations the presentation alone of an identity card will be assumed to prove the identity of the holder without the card itself or the biometrics being checked, thus making possession of a stolen or forged identity card an easier way to carry out identity fraud than is currently the case.”<sup>74</sup> Whether this concern is valid depends on the availability of biometric readers and the presence of biometric spoofing

<sup>70</sup> Qtd. in Grossman 2005, p. 5.

<sup>71</sup> Identity and Passport Service 2006.

<sup>72</sup> LSE 2005, p. 4.

<sup>73</sup> LSE 2005, p. 3.

<sup>74</sup> House of Commons Home Affairs Committee 2004, p. 79.

techniques. Wendy M. Grossman also notes how, “The problem here is that the more valuable an identity document is, the greater the motive to create forgeries. (...) What the card *will* do is ensure that if someone is a victim of identity theft the consequences to that person will be far more severe than they would be now because all their identity will be connected to a single card and number.”<sup>75</sup>

### 4.3 The EU and the Threat of Identity Theft

#### *4.3.1 Prevalence of Identity Theft in the EU*

In 2002, Bernard Clements *et al.* concluded in their report *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview* that identity theft is comparatively less prevalent in the EU, as opposed to countries like Canada and the US. Clements *et al.* identify possible reasons for this, including the existence of “stronger mechanisms in the physical world (in a number of EU countries ID cards are commonly used) and different purchasing patterns, which, in the EU, rely more on face-to-face contact than on distance purchasing.”<sup>76</sup> Furthermore, the authors note “more effective privacy protection in Europe limits the ease of access to personal data needed by would-be identity thieves.”<sup>77</sup> However, Clements *et al.* do recognize the potential threat identity theft poses for the Member States, especially as the information society progresses and e-commerce advances. In February 2004, the European Commission held a Forum on identity theft in which a similar conclusion was drawn about the comparatively low prevalence of identity theft in the EU. The attendees of the Forum noted how “Identity theft is growing fast outside the EU (US, Canada, Australia) and is very relevant in the UK. For now, it does not seem to be equally prominent in the other Member States.”<sup>78</sup> Important to note, however, is Europol’s conclusion in its *2003 European Union Organised Crime report* where it acknowledged that “Identity theft and credit card fraud are increasing”<sup>79</sup> which implies that while comparatively the prevalence of identity theft is relatively low in the EU its increasing rate deserves considerable attention. Consequently, although identity theft in the EU is not as prevalent as it is in the US and the UK, numerous policy makers and scholars identify the crime as a serious threat which will evolve in the future as a result of changes in the information society and an increased use of technology.

#### *4.3.2 Ideas for Prevention and Countermeasures*

According to a questionnaire distributed and analyzed by Fabio Marini, an attendee of the Forum on identity theft, eight Member States have specific legislation on identity theft. Yet, he also notes State legislation demonstrates significant discrepancies across the Member States and during the Forum Marini expressed the need for common guidelines and training programmes to streamline the countermeasures in the EU.<sup>80</sup> Harmonized EU rules with regard to identity theft could, according to the Forum members, simplify the investigation and prosecution of offenders. The important remark to make with regard to the results presented by Marini is the contradiction with other surveys distributed among the Member

---

<sup>75</sup> Grossman 2005, p. 11.

<sup>76</sup> Clements *et al.* 2002, p. 32.

<sup>77</sup> Clements *et al.* 2002, p. 32.

<sup>78</sup> European Commission 2004a, p. 2.

<sup>79</sup> Europol 2003, p. 21.

<sup>80</sup> European Commission 2004a, p. 6.

States, which report that far fewer, if any, Member States have any kind of identity theft legislation. Gill *et al.*, for example, note “In 2004 the FIDIS Consortium in conjunction with Tilburg University surveyed a variety of countries including a number of EU members on identity theft legislation. The survey revealed that there are very few specific provisions in criminal law in the EU member states about identity theft or identity fraud.”<sup>81</sup> Further comparison of these results is unfortunately not possible due to lack of more specific information provided in the minutes of the Forum. The only additional important remark made in the minutes is how “Most countries (11) said they consider ID theft as a part of conspiracy to commit another crime, an aggravating circumstances [sic] in other crimes or it is included in other forms of crime such as fraud, forgery, computer crimes, counterfeiting etc.”<sup>82</sup> As a result, one can safely conclude there is no specific legislation with regard to identity theft as other surveys indicated but that “in most EU Member states, the actions involved in identity theft will generally be sanctioned under other provisions, such those concerning fraud, information fraud, identity usurpation, impersonation, or illegal use or processing of personal data.”<sup>83</sup>

With regard to legislation at the EU level, Neil Mitchinson *et al.* note in their report *Identity Theft – A discussion paper* that “At European Union level specific legislation on identity theft does not exist.”<sup>84</sup> Consequently, Mitchinson *et al.* present a number of key conclusions with regard to potential initiatives to combat identity theft.

First, Mitchinson *et al.* conclude that there appear to be two approaches possible in trying to deal with the problem of identity theft:

1. making it more difficult;
2. making it less profitable.

Mitchinson *et al.*, however, also observe how there may be conflicts between both approaches because measures which try to make identity theft more difficult may also have the effect that such theft is more profitable.

The second conclusion provided in the report is that there is a general lesson to be drawn on the basis of systematic analysis of security vulnerabilities in other areas which demonstrate how single-barrier measures are popular with users, but multi-barrier measures – what the authors call ‘defence in depth’ – will allow for more security, provided that the measures are sufficiently user-friendly that users do not systematically bypass them. Mitchinson *et al.* argue that “although it is possible to imagine multi-barrier approaches in the area of identification, it seems unlikely, given the user convenience of a single-barrier approach, that multi-barrier approaches will gain widespread acceptance without very strong pressure from the public authorities.”<sup>85</sup>

A third observation made in the concluding section of the report is that a systematic analysis should be conducted on the effects of the creation of a centralized database of identifying data. As has been argued in many other publications, a centralized database creates in principle a single point of vulnerability for large-scale identity theft. Hence, it would be recommendable to try and minimize the introduction of such databases. An inventory of policy initiatives in numerous countries that aim at centralized databases in light of efficient

---

<sup>81</sup> Gill *et al.* 2006, p. 8.

<sup>82</sup> European Commission 2004a, p. 6.

<sup>83</sup> Mitchinson *et al.* 2004, p. 24.

<sup>84</sup> Mitchinson *et al.* 2004, p. 23.

<sup>85</sup> Mitchinson *et al.* 2004, p. 29.

crime prevention, national security measures, etc., demonstrate how the introduction of such databases cannot be prevented. Policymakers can, however, be encouraged that such databases only contain the information strictly necessary for the operations the database supports. This could, in citing Mitchinson *et al.*, “be done by the database owner, by encouragement - or if necessary legislation - by the public authorities, or, to some extent at least, by the customer or client restricting the information supplied.”<sup>86</sup> A final conclusion made is that in trying to reduce the vulnerabilities of centralized databases more attention should be given to the development and widespread deployment of identity management systems.

Later on in 2004, the Commission also developed its new Action Plan for 2004-2007 to prevent fraud on non-cash means of payment. In its Action Plan, the Commission recognizes how fraud evolves and how “Criminal actions such as data hacking or identity theft are growing at a worrying pace and new scams are emerging.”<sup>87</sup> As a result, the Commission identifies one of the objectives within the action plan as the need for specific initiatives to prevent identity theft in the EU. The Commission describes how “identity theft is a cross-sector problem affecting governments, businesses and citizens, which is growing rapidly in some sectors or countries and is often linked to organised crime.”<sup>88</sup> To address issues related to identity theft, the Commission outlined a number of action points:

- “The Commission will promote the creation of a database of original and counterfeit identity documents accessible to both the public authorities and the private sector.”
- “The Commission will assess the merits of establishing an EU single contact point for citizens and businesses on identity theft, which could include a register of bodies engaged in the prevention of identity theft.”
- “The Commission will continue to discuss the implementation of a single phone number in the EU for notification of lost or stolen cards.”<sup>89</sup>

Furthermore, the Commission strengthened the role and reorganized the functioning of the EU Fraud Prevention Expert Group (FPEG) as part of its action plan. The FPEG includes all major stakeholders in payment fraud prevention in the EU, which are representatives of national and EU banks, ministries, law enforcement agencies, retailers, consumer groups, and network operators, and the FPEG “provides an added value as a platform where stakeholders could effectively exchange information and best practice to prevent fraud.”<sup>90</sup> As part of the action plan, the Commission identified the need for the FPEG to meet at least twice a year. The members of the FPEG represent seven sub-groups. One sub-group deals specifically with identity theft and phishing. Its primary objective is to provide recommendations and propose countermeasures to effectively prevent, detect, and react to attempts of identity theft and phishing. The group primarily focused its previous work on the prevention and detection of identity theft and a new group is now established to specifically address phishing.<sup>91</sup> The identity theft subgroup is currently working on a comprehensive discussion paper due out in November. During the FPEG’s last meeting on May 16, 2006, Marini introduced the upcoming high level conference titled *Maintaining the integrity of identities and payments. Two challenges to fraud prevention*, which will take place on November 21 and 22, 2006.

---

<sup>86</sup> Mitchinson *et al.* 2004, p. 29.

<sup>87</sup> European Commission 2004b, p. 3.

<sup>88</sup> European Commission 2004b, p. 9.

<sup>89</sup> European Commission 2004b, p. 10.

<sup>90</sup> European Commission 2004b, p. 4.

<sup>91</sup> Fraud Prevention Expert Group (FPEG) 2006, p. 6.

According to the FPEG, “The idea to have a High Level conference on identity theft and payment fraud springs from the importance of a broader involvement of policy makers and high ranking representatives of national administrations in this area. It should be an ideal platform to discuss and launch possible Commission initiatives, including legal proposals.”<sup>92</sup> Furthermore, Marini also identified how the Directorate General (DG) Justice, Freedom, and Security plans to finalize a comparative study on identity theft, which evaluates the need for instruments to combat activities of organized crime related to identity theft within the EU, before the end of the year. A number of research projects from different agencies or groups within the EU are forthcoming and will hopefully identify the most pressing concerns of the Member States and potential initiatives to combat identity theft. One suggestion, noted in the meeting minutes, proposed during the Seminar held earlier this year in March entitled *Payment Fraud and EU Enlargement: Threats and Challenges* is to explore the criminalization of identity theft and phishing as specific criminal offenses, much the same way as the US did previously.

The different published reports and meetings held during the previous years demonstrate how different actors within the EU continuously identify the need to develop measures to prevent and detect identity theft, especially with regard to its connection with organized crime. In the *EU Organised Crime Threat Assessment of 2006*, Europol precisely focuses on how identity theft is just another means to increase the ease of committing other forms of organized crime like money laundering. Measures against identity theft at the EU level can therefore potentially disrupt criminal activity early on, during the stage where criminals gain unlawful access to personal information.<sup>93</sup>

#### 4.3.3 Policy Conflicts and Concerns

In its reports and efforts, the EU emphasizes the need for coordination and cooperation among the different levels of authority and the different agencies. Furthermore, individuals indicate the necessity to harmonize both the definition of identity theft and the initiatives of the Member States. Although the EU often recognizes identity theft as a major security issue, actual implementation appears slow. As Gill *et al.* note, “there is little evidence to suggest much progress has been made.”<sup>94</sup> Whether measures against identity theft at the EU level will actually gain the necessary momentum is questionable. For now, the UK appears to be the primary region where identity theft and, more generally, identity fraud are prominent. From interviews held by Gill *et al.*, officials in other countries, namely France, Germany, and the Netherlands, also appear concerned about identity fraud. Yet, are these concerns combined with the alarming sounds coming from the UK sufficient to generate any initiatives to prevent, detect, and manage the broad issue of identity fraud. Perhaps a discrepancy among priorities between the different Member States is an important factor in the ultimate attention and resources provided to fight identity theft. Furthermore, the general tension within the EU also applies to future identity theft legislation. Certain Member States are simply unwilling to sacrifice any authority to the EU level and wish to solve their problems internally. The problem with disregarding the EU level is the transnational element of identity theft within the EU and its connection with organized crime. On the other hand, an effective balance needs to exist between national and European legislation because the principle of subsidiarity holds true here as well.

---

<sup>92</sup> FPEG 2006, p. 3.

<sup>93</sup> Europol 2006.

<sup>94</sup> Gill *et al.* 2006, p. 12.

## 5. The Forgotten Face

In section 3, I identified the distinction between financial and criminal identity theft. Throughout the remainder of the report, however, there was a clear emphasis on financial identity theft, which hardly comes as a surprise. Criminal identity is a problem,<sup>95</sup> especially because it continues to reside in the shadow of financial identity theft. Regulatory initiatives, in all three regions, focus primarily on financial identity theft. As a number of victim advocates have noted, victims of criminal identity theft suffer greater damage yet have hardly any legal resources to turn to. As Beth Givens, director of the Privacy Rights Clearinghouse, notes “Credit-related identity theft can ruin your life for a couple years. Criminal record identity theft can ruin your life forever. It is virtually impossible to wipe the slate clean.”<sup>96</sup> The inability to provide a clear picture about the prevalence of criminal identity theft is one of the major shortcomings within mainstream identity theft research; yet, if governments are so concerned with the connection between terrorism, organized crime, and identity theft perhaps they ought to start analyzing identity theft from a broader perspective and also investigate the dark number of criminal identity theft cases. The only exception appears to be the research conducted by Wang *et al.* who write about criminal identity deception. Their research, however, focuses on how to provide law enforcement officials with the equipment to detect criminal identity deception, whether it concerns personal information of existing or non-existing individuals. Consequently, their focus does not shed light on how policy makers ought to introduce initiatives which could help prevent criminal identity theft and how to provide additional resources for victims to recover from criminal identity theft. Especially herein rests a major problem, because victims of criminal identity theft often find themselves in an unrecoverable situation. As Givens notes in her conclusion, “Too many people’s lives have been ruined because of this crime. We must find solutions and find them soon. This crime is not going away.”<sup>97</sup>

## 6. The Netherlands

Before moving on to the relevant recommendations and lessons for the Netherlands, I first briefly analyze the current state of affairs in Dutch society with regard to identity fraud. Data on the prevalence of identity fraud in the Netherlands is not readily available. Piet-Hein Donner, Minister of Justice, admitted in 2004 how the government is unaware of the extent of the problem and the exact prevalence of identity fraud.<sup>98</sup> He furthermore claimed the government is highly dependent upon complaints provided by both private corporations and consumers to obtain the necessary data. Donner identified a select number of cases where corporations filed complaints of identity fraud and concluded identity fraud remained primarily a concern for the financial sector of society. Despite the lack of actual figures, Gill *et al.* concluded, based on a number of interviews with experts in the Netherlands, that identity fraud is a serious problem.<sup>99</sup> Part of the reason why the prevalence of identity fraud is so difficult to measure is the fact that there is no specific legislation which criminalizes the act of identity fraud or more specifically identity theft. As a result, individuals may have already filed complaints which can be considered identity fraud yet these complaints fall into different categories of crime which makes gathering data virtually impossible.

---

<sup>95</sup> Data on criminal identity theft is scarce. According to a survey conducted by the Privacy Rights Clearinghouse in 2000, 15% of financial identity theft victims were also victims of criminal identity theft.

<sup>96</sup> Givens 2000, p. 2.

<sup>97</sup> Givens 2000, p. 6.

<sup>98</sup> *Kamerstukken II*, 2003/04, 1783: 3777-3778.

<sup>99</sup> Gill *et al.* 2006.

Furthermore, in 2004 the National Forum on the Payment System, or the *Maatschappelijk Overleg Betalingsverkeer* (MOB), recognized how “In the last few years, there has been an increase in identity fraud committed against consumers, enterprises and banks.”<sup>100</sup> The following year MOB again identified the increase in cases of identity fraud and also recognized how discussions both in the media and in the political arena display the tremendous confusion about the risks, liability, and the role of different stakeholders with regard to identity fraud.<sup>101</sup> In terms of financial damage, the MOB suggests the costs have remained relatively low as a result of effective security of electronic payment traffic, the limited use of credit cards, and other initiatives. These other initiatives include immediately deactivating credit and debit cards, improved methods of mailing credit cards, and more intensive monitoring of credit card payments to detect suspicious transactions.<sup>102</sup> Due to the increasing threat of identity theft, the Dutch Banking Association, or the *Nederlandse Vereniging van Banken* (NVB), began a public awareness campaign which informed consumers of the risks of identity theft and also provided tips on how to protect their personal information.<sup>103</sup> There are a number of additional (limited) public awareness initiatives currently active. These include websites such as [www.surfopsafe.nl](http://www.surfopsafe.nl) and brochures which inform consumers about phishing and how to react when receiving a suspicious email. There is a large need for public awareness as “The perception is growing but mainly [the Dutch] think that only their neighbors can be the victim, well there are already a lot of people who have received some extra letters off [sic] the tax inspectors and that’s hard to prove that you’re not the person that did the work. These kinds of experiences are making the people aware that this is a serious problem.”<sup>104</sup>

## 7. Concluding Remarks and Lessons

### 7.1 Urgency of Identity Theft

The previous sections indicated both the developments and regulatory instruments introduced in the US, the UK, and the EU. The next step is to derive practical implications from experiences in these three cases and the effectiveness of their initiatives to counter identity theft in relation to the Netherlands. Before doing so, however, it is important to reflect back on how urgent identity theft actually is in the different regions. In the US, as previously noted, certain scholars and business professionals question identity theft statistics. Scholars do so primarily because they analyze the declining percentage of identity theft complaints, whereas business professionals disagree with the inclusion of credit card fraud as a form of identity theft. The urgency of the crime as a result is subjective and highly dependent on how policy makers and scholars define the crime. Credit card fraud, while commonly included in identity theft statistics, could also be considered as regular theft or payment fraud. As a result, if the FTC, for example, were to exclude credit card fraud from its identity theft statistics there would be a decrease of 26% and suddenly the problem would appear less urgent. What policy makers and business professionals alike must bear in mind, however, is the steady shift away from credit card fraud towards other forms of identity theft which are yet to be specified by the FTC. These disputes do not only occur in the US. As became evident, certain

---

<sup>100</sup> National Forum on the Payment System 2005, p. 28.

<sup>101</sup> Maatschappelijk Overleg Betalingsverkeer (MOB) 2006, p. 16.

<sup>102</sup> MOB 2006, p. 16.

<sup>103</sup> MOB 2006, p. 17.

<sup>104</sup> Qtd. in Gill *et al.* 2006, p. 27.

scholars also dispute the figures presented in the UK and claim the actual number of identity fraud is much lower. Statistics stemming from the EU generally appear consensual about the relatively low prevalence of identity theft in comparison to other regions. Officials within the EU do however recognize the oncoming threat and as such identity theft is a considerable policy issue.

### 7.2 Cultural Differences

An additional significant remark to make before analyzing the potential lessons the Dutch authorities can derive from the experiences abroad is to recognize the crucial cultural differences in a number of areas including identification, credit card use, political systems, and the legal culture of a region or country. These cultural distinctions are certainly important with regard to, for example, the US where obtaining a credit card occurs with such relative ease in comparison to countries within the EU. As a result the credit card application system is a particularly vulnerable area within the US but perhaps not in EU member states. The importance of recognizing these differences is the fact that analyzing experiences abroad requires great care, especially when using these experiences to develop countermeasures in one's own country.

### 7.3 Policy Options: Criminalization

The next significant remark to make regards the different number of options policy makers can implement to counter identity theft. A comparison between decisions made within the different regions is particularly valuable in terms of analyzing both the benefits and the costs of these initiatives. Criminalization, for example, became an important first step in the US, whereas the UK has so far declined to follow a similar path. The EU as previously noted discussed this option at a conference but is yet to seriously take concrete action on it. The question which arises as a result is whether criminalization brings about any definite advantages. In some respects I have already reflected upon this question in previous sections, but this was usually only with regard to the US. When reflecting back on the effectiveness of criminalization, it becomes clear that actually prosecuting identity thieves is not the most important asset of the legislation. Criminalizing identity theft, however, is an important element in the overall scheme to fight the problem. First, defining identity theft per se as an offense is both helpful for victims and law enforcement officials. Second, to a certain extent it also provides a particular way of raising awareness for the crime among individuals as well as businesses. Third, keeping identity theft merely as an element of other crimes, like passport fraud, neglects the need for specific initiatives to fight the problem. As such the argument that other legislative instruments can help to prosecute identity thieves fails to recognize the other effects of criminalization. When policy makers criminalize identity theft, victims receive a voice and the well needed recognition that they are in fact victims of a crime. Furthermore, it is a crucial move to make especially with regard to the incompetency of law enforcement officials to adequately deal with victims of identity theft. A number of authors, however, claim criminalization fails to address the heart of the problem. Henry Pontell describes how, "Trying to deal with identity fraud through criminalization alone, cannot serve as an effective means of control."<sup>105</sup> Daniel J. Solove notes how "Understanding identity theft in this manner—as a form of criminal activity to be stamped out through criminal law—misconstrues the problem in a profound way. (...) Identity theft is a consequence of an architecture, one that creates a series of vulnerabilities. This architecture is

---

<sup>105</sup> Pontell 2002, p. 14.

not created by identity thieves; rather, it is exploited by them.”<sup>106</sup> Certainly both authors identify crucial arguments and I hardly dispute them, but criminalization is an important part of the *overall* fight against identity theft. Solove raises particularly important concerns when he notes, “The traditional view fails to address this architecture, for it focuses on identity theft as a series of discrete instances of crime rather than as a larger problem about the way our personal information is handled. Even the term of ‘identity theft’ views it as an instance of crime—a ‘theft’ rather than as the product of inadequate security.”<sup>107</sup> As result criminalization is an important initiative, policy makers, however, should not use it as the only means to fight identity theft, because if the ultimate goal is elimination of the crime, the architecture will need to change.

#### 7.4 Raising Public Awareness

Certainly, another important lesson, which both the US and the UK implemented and which would certainly be useful for the Netherlands, is the development of a public awareness campaign. As described above, raising public awareness provides a number of advantages. First, by providing the public with information about identity theft they can better arm themselves to prevent identity theft, which, if effective, helps to prevent the overall occurrence of the crime. Second, if identity theft does indeed take place, the public awareness activities are a tool for victims to ask for timely assistance at the appropriate outlets and in turn they can receive help with their recovery. As became evident above, the Netherlands has already initiated a number of public awareness campaigns and provides information about identity theft through a number of websites. Yet, the outreach of these campaigns deserves critical reflection. Primarily because, as was noted earlier, Dutch citizens have yet to understand the seriousness of the threat and in failing do so they may also be unaware of how to best protect their personal information or what to do when they become a victim of identity theft.

#### 7.5 Identification Numbers and a Central Database

Furthermore, an important factor with regard to identity theft is the presence of an identification number which is used for a number of public and private services. Unfortunately, the Dutch government decided to introduce the *Burgerservicenummer* (BSN).<sup>108</sup> In 2003, the year the proposed bill came into existence, Corien Prins immediately recognized the potential negative effects BSN could have with regard to an increase in identity theft cases and opportunities for perpetrators.<sup>109</sup> Two years later, in 2005, the Dutch Data Protection Authority, or the *College Bescherming Persoonsgegevens* (CBP), made similar remarks in response to the proposed bill. The CBP claimed that identity fraud would increase and that this increase could, without a doubt, be expected based on national and international experiences. Even now, the CBP wrote, perpetrators engage in unlawful activity through the illegal use of existing soft-nummers, which leads into extremely unpleasant consequences for victims as well as for employers, insurance companies, and government agencies. The CBP recognized how identity theft will become more appealing and will increase due to the broader usage of the newly introduced BSN. Furthermore, the CBP claims the consequences will be more severe and far reaching as a result of BSN. All of these

---

<sup>106</sup> Solove 2004, p. 4.

<sup>107</sup> Solove 2004, p. 4.

<sup>108</sup> *Kamerstukken II*, 2005/06, 30 312, nr. 2.

<sup>109</sup> Prins 2003, p. 2-3.

problems are, according to the CBP, ignored in the current bill.<sup>110</sup> Earlier, the Dutch Council of State (Raad van State) expressed similar concerns in its official advice to the Dutch Parliament on the bill.<sup>111</sup> Additionally, the proposed BSN reflects frightening similarities to the American SSN and while it may help to increase bureaucratic efficiency and citizen-friendliness, it will also provide a gateway opportunity for identity thieves. Prins reflects on this point as she notes how it appears as though the Dutch hardly took the effort to analyze the effects of similar projects abroad.<sup>112</sup> A close reflection of experiences abroad would have been highly beneficial as it indicates how the introduction of a central identification number is a process which is significantly difficult to reverse. As the US is currently experiencing, eliminating its SSN or reverting it back to its original purpose, while perhaps one of the more effective means to combat the growing societal evil of identity theft, is highly inefficient and receives fierce criticism. The institutional costs force legislators to introduce less radical changes, where, for example, the SSNs are less publicly displayed through truncation. The concerns raised against the Identity Cards Act of 2006 in the UK deserve considerable attention with regard to the introduction of the BSN. National Identification Numbers and a single database to store them in are certainly beneficial for efficient cross-referencing between different sectors and agencies. The major drawback, however, often voiced by opponents and noted in the discussion paper, provided by Mitchinson *et al.*, is the single point of vulnerability. As soon as an offender either retrieves a person's national identification number or breaks in to a database, he or she can easily commit identity theft. If perpetrators gain access to the database they obtain massive amounts of personal information within a heartbeat. While the introduction of a central identification number is not automatically a problem, however, it should, as it has in the US, not become the single point of reference for individuals. Additionally, the identification numbers should remain as private as possible; yet, for this to happen there is a heavily reliance on citizens, as well as employees, in both private and public sectors.

## 7.6 Biometrics

Additional options considered include the implementation of biometric technology. The US has so far, upon the recommendation of the Department of the Treasury, decided to place a hold on biometrics as a potential solution. The UK, however, will make it an important part of their Identity Cards scheme. Biometrics gained in popularity after the terrorist attacks of September 11, 2001 primarily in areas such as airport security and travel documents. As many authors note and use as an example, the perpetrators of the terrorist attacks used false identities to successfully gain residence documents which indirectly allowed them to complete the terrorist attacks. This example is therefore often used to indicate the link between identity-related crime and terrorism or organized crime. According to some, biometrics provide a number of benefits for both organizations and consumers. As Linnhoff & Langenderfer note, "From an organizational perspective biometric identifiers are attractive because they generally do not vary over the lifetime of the individual, they typically cannot be shared, and they cannot be acquired through computer hacking or surreptitious behavior."<sup>113</sup> From the consumer point of view, the introduction of biometrics also offers a number of benefits. The greatest advantage is the possibility for consumers to be free of any worries about fraudulent use of credit cards, because they will only require their fingerprints to make

---

<sup>110</sup> College Bescherming Persoonsgegevens (CBP) 2005, p. 2. On May 23, 2006 the CBP repeated its concerns in another letter addressed to the Members of Parliament.

<sup>111</sup> *Kamerstukken II*, 2005/06, 30 312, nr. 4.

<sup>112</sup> Prins 2006, p. 13-14.

<sup>113</sup> Linnhoff & Langenderfer 2005, p. 315.

payments.<sup>114</sup> Of course this conclusion provided by Linnhoff & Langenderfer is quite naive and shortsighted because biometrics is hardly without complications.

While for some individuals the introduction of biometrics presents the only viable option to counter identity theft, others recognize the potential negative side effects. The first point of identification is a sensitive area because when the biometric information is entered into the database a perpetrator could pretend to be the victim. If this happens then the victim will encounter an even greater obstacle to prove his or her innocence and personal identity. Furthermore, the accuracy of biometric data is far from optimal and some claim the technology is still in an advanced stage of development. Concerns do not only originate from individuals concerned with regulating identity theft but also from the side of the public. Financial institutions try to avoid implementing biometrics because consumers appear to be rather hesitant to support such measures. They appear concerned with the number and kind of people who can access the data. As Linnhoff & Langenderfer recognize, "Perhaps, chief among privacy concerns for biometric technology is the storage and maintenance of the data files."<sup>115</sup> Furthermore, privacy concerns generally spark debates among a number of individuals. Ann Cavoukian, Information Privacy Commissioner from Ontario, Canada, for example, states "Biometrics need not subvert informational privacy. A pro-privacy position should not be construed as anti-biometric. The technology can actually be privacy enhancing if systems are designed with that objective in mind."<sup>116</sup> Others, however, disagree and identify the ability of organizations to obtain significant power over individuals through their biometric data. As Linnhoff & Langenderfer note in their conclusion, "The rapid growth of biometric authentication technology represents a double-edged sword for consumers. One [sic] the one hand, the increased use of biometrics is likely to reduce the incidence of identity theft, improve consumer convenience by eliminating or reducing password use, and lower prices by reducing fraud costs to retailers. On the other hand, although overall security will likely be enhanced security breaches will be more costly when they do occur and require considerably more effort to correct."<sup>117</sup> Whether biometric technology could actually reduce the incidence of identity theft is a questionable conclusion, because perhaps instead of making changes in the *identification* processes there should be a focus on altering and strengthening the *verification* processes.<sup>118</sup> Jan Grijpink and Corien Prins present the important distinction between these two different concepts. According to these authors, identification occurs when an individual establishes precisely who someone is. Verification, on the other hand, is the process where an individual establishes that a person is the same person as expected or basically that the person is who he or she claims to be.<sup>119</sup> This distinction is crucial with regard to the introduction of biometric technology because without stronger and more unpredictable verification biometrics will not be very effective. As Grijpink and Prins note, "Unfortunately, people are often unaware of the limitations of the customary forms of personal identification, so that verification is often placed on a par with identification. Even if a person can be compared on the spot with a photograph on an identity card, the one-off and isolated verification can never provide certainty that the person in question is actually who he says he is."<sup>120</sup> Grijpink and Prins observe that, with the exception

---

<sup>114</sup> Linnhoff & Langenderfer 2005.

<sup>115</sup> Linnhoff & Langenderfer 2005, p. 324.

<sup>116</sup> Cavoukian 1999, p. 33.

<sup>117</sup> Linnhoff & Langenderfer 2005, p. 334.

<sup>118</sup> Grijpink & Prins 2003.

<sup>119</sup> Grijpink & Prins 2003.

<sup>120</sup> Grijpink & Prins 2003, p. 252.

of criminal law enforcement, a personal identification along the lines of ‘he is the same as...’ is sufficient for the majority of the legal transactions.<sup>121</sup>

### 7.7 Conflicts of Interest: The Challenge of Coordination and Cooperation

In addition to the choices policy makers have to make with regard to fighting identity theft, they also have to consider how to incorporate the different stakeholders. Conflicts of interest often occur between citizens, governments, and businesses, especially since they all have different stakes in the entire battle against identity theft. For the most effective prevention and deterrence, the stakeholders need to both cooperate and coordinate their actions, which has proven particularly challenging in the past. The challenge rests both in the conflict of interest and the different priorities each stakeholder has within the fight against identity theft. As a result, cooperation and coordination often return in policy recommendations from all three regions. As Norm Archer *et al.* note, “The success in combating identity theft relies on joint efforts and coordination among all stakeholders in every relevant activity.”<sup>122</sup> Coordination among different levels of government is key in the US and the EU. As Gill *et al.* note, “there is scope for more co-ordination in responding to identity theft and identity fraud. In the EU for example, there is a hive of activity but it is not clear whether all of the departments and units involved in developing responses are working in a coordinated fashion.”<sup>123</sup> Coordination and cooperation are most crucial in federal and quasi federal political systems; yet both are still significant even in more unitary systems, primarily because identity theft involves, of course, a number of different departments, including law enforcement, treasury, and internal affairs. As previously noted, coordination and cooperation are also essential between the public and private sector. Precisely herein rests some areas of dispute or conflict. The private sector clearly recognizes the problems associated with identity theft, but often wishes to solve the problem without regulatory interference; yet, in the US there is a tendency towards granting private corporations more responsibility, through regulatory initiatives, which generates a less than amicable relationship. Especially stringent state regulations, the credit freeze for example, provide some negative repercussions for private corporations. Cooperation here, therefore, becomes less of a focus. With regard to the Netherlands, effective coordination and cooperation is certainly a significant factor. According to Gill *et al.*, six ministries concern themselves with identity-related crime and clearly all take a distinct approach.<sup>124</sup> The coordination and cooperation problem often originates due to the interdependent relationship of different actors who all maintain different priorities and perceptions with regard to identity theft. As Jody Westby remarks, “Part of the problem is perception. Most people think of information security as a technical issue. It really is a multifaceted issue that requires a multidisciplinary approach. It is multifaceted because it involves privacy and security and cybercrime. It is multidisciplinary because it requires you to dovetail the legal, operational, managerial, and technical considerations of all three of those issues piled in with the business plan that sets the architecture of a company. (...) Security (...) is still perceived as a geek issue. CEO and boards are afraid of becoming geeks.”<sup>125</sup>

### 7.8 Conclusion

---

<sup>121</sup> Grijpink & Prins 2003, p. 252.

<sup>122</sup> Archer *et al.* 2006, p. 31.

<sup>123</sup> Gill *et al.* 2006, p. 29.

<sup>124</sup> Gill *et al.* 2006.

<sup>125</sup> Westby 2004, p. 113.

Overall, identity theft is a considerable problem in different parts of the world. Prevalence is unclear and policy makers along with business officials argue about the available options to counter the problem. As for the Netherlands, it is crucial to be rather careful with the BSN and its use within society. Furthermore, criminalization certainly is a viable option along with a more widespread public awareness campaign. When the government does introduce initiatives to prevent or counter identity theft in the future, an important consideration ought to be the different interests of stakeholders and the goal to maintain coordination as one of the highest priorities.

## Bibliography

- Arizona Criminal Code Revised Statute § 13-2008 (1996).
- Archer, N. *et al.* (2006). 'A Contextual Framework for Combating Identity Theft.' *IEEE Security & Privacy*, Vol. 4 (2): 30-38.
- Binder, R. & Martin Gill (2005). 'Identity Theft and Fraud: Learning From the USA.' *Perpetuity Research & Consultancy International Ltd.*
- California Financial Information Privacy Act (2003). California Civil Code § 1798.29.
- California Security Breach Information Act (2003). California Civil Code § 1798.82.
- Cavoukian, A. (1999). 'Consumer Biometric Applications: A Discussion Paper.' *Information Privacy Commissioner Ontario, Canada.*
- Cheney, J. S. (2005). 'Do Definitions Still Matter?' Discussion Paper Payment Cards Center, *Federal Reserve Bank of Philadelphia.*
- Clements, B. *et al.* (2003). 'Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview.' *Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), IPTS-JRC.*
- College Bescherming Persoonsgegevens (CBP) (2005). Letter to the Members of the Dutch Parliament, October 25, 2005: 2 (z2005/1198).
- Consumer Measures Committee (2005). 'Working Together to Prevent Identity Theft: A Discussion Paper for Public Consultation.'
- Courtney, K. (2005). 'Home Office Identity Fraud Reduction Programme.' Chair's Progress Report, *Identity Fraud Steering Committee.*
- Conner, B. (2004). 'Statement of Bill Conner, Chairman, President and CEO Entrust, Inc.' Hearing on Identity Theft: The Causes, Costs, Consequences and Potential Solutions, Before the *Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census of the Committee on Government Reform.*
- Credit Industry Fraud Avoidance System (CIFAS) (2004). 'How Serious is the Problem?' [http://www.cifas.org.uk/identity\\_fraud\\_is\\_theft\\_serious.asp](http://www.cifas.org.uk/identity_fraud_is_theft_serious.asp)
- Crews, C. W. & Brooke Oberwetter (2006). 'Preventing Identity Theft and Data Security Breaches: The Problem With Regulation.' *Competitive Enterprise Institute (CEI).*
- European Commission (2004a). 'Minutes of the Forum on Identity Theft.'
- European Commission (2004b). 'A New EU Action Plan 2004-2007 to Prevent Fraud on Non-cash Means of Payment.' *COM (2004) 679 final.* Brussels, 20.10.2004.
- Europol (2003). '2003 European Union Organised Crime Report.'
- Europol (2006). 'EU Organised Crime Threat Assessment 2006.'

- Executive Order 13402 - Strengthening Federal Efforts To Protect Against Identity Theft (2006).
- Fair and Accurate Credit Transactions Act (2003). Pub. L. No. 108-159.
- Federal Trade Commission (FTC) (2006). 'ChoicePoint Settles Data Security Breach Charges; to Pay \$10 Million in Civil Penalties, \$5 Million for Consumer Redress.' News Release January 26, 2006. <http://www.ftc.gov/opa/2006/01/choicepoint.htm>
- Fraud Prevention Expert Group (FPEG) (2006). *Draft Minutes of the 10th Meeting of the Fraud Prevention Expert Group*, MFS D (2006). Brussels, 22.05.2006.
- Gerring, J. (2001). *Social Science Methodology. A Critical Framework*, Cambridge: Cambridge University Press.
- Gill, M. *et al.* (2006). 'The Fight Against Identity Fraud: A Brief Study of the EU, the UK, France, Germany, and the Netherlands.' *Perpetuity Research & Consultancy International Ltd.*
- Givens, B. (2000, updated in 2006). 'Identity Theft: The Growing Problem of Wrongful Criminal Records.' *Privacy Rights Clearinghouse.*
- Government Accountability Office (GAO) (2006). 'Social Security Numbers: More Could be Done to Protect SSNs.' Statement of Cynthia M. Fagnoni, Managing Director, Education, Workforce, and Income Security Issues *Before the Subcommittee on Social Security, Committee on Ways and Means, House of Representatives.*
- Gramm-Leach-Bliley Act (1999). 15 USC, Subchapter I, Sec. 6801-6809 Disclosure of Nonpublic Personal Information.
- Grijpink, J.H.A.M. & Corien Prins (2003). 'New Rules for Anonymous Electronic Transactions? An Exploration of the Private Law Implications of Digital Anonymity,' in C. Nicoll, J.E.J. Prins, M.J.M. van Dellen (eds.) *Digital Anonymity and the Law. Tensions and Dimensions*, The Hague TMC Asser Press: 249-269.
- Grossman, W. (2005). 'Identifying Risks: National Identity Cards.' Lecture Delivered at the University of Edinburgh on January 19, 2005. Published in *SCRIPT-ed* Vol. 2 (1): 2-17.
- Holtfreter, R. E. & Kristy Holtfreter (2006). 'Gauging the Effectiveness of U.S. Identity Theft Legislation.' *Journal of Financial Crime*, Vol. 13 (1): 56-64.
- House of Commons Home Affairs Committee (2004). 'Identity Cards: Fourth Report of Session 2003-04.'
- Howard, H. M. (2005). 'The Negligent Enablement of Imposter Fraud: A Common Sense Law Claim.' *Duke Law Journal*, Vol. 54: 1263-1294.
- Huggins v. Citibank, N.A.*, 355 S.C. 329 (2003).

- Identity and Passport Service (2006). 'What Are the Benefits of the National Identity Scheme?' <http://www.identitycards.gov.uk/benefits-glance.asp>
- Identity Theft Data Clearinghouse (2006). 'Identity Theft Victim Complaint Data: Figures and Trends, January 1 – December 31, 2005.' *Federal Trade Commission*, Washington DC.
- Identity Theft and Assumption Deterrence Act of 1998, Pub. L. No. 105-318, 112 Stat. 3007 (1998) (amending 18 U.S.C. § 1028).
- Identity Theft Penalty Enhancement Act of 2004, Pub. L. No. 108-275, 118 Stat. 831 (2004).
- Identity Theft Resource Center (ITRC) (2003). 'Identity Theft: The Aftermath 2003. A Comprehensive Study to Understand the Impact of Identity Theft on Known Victims as Well as Recommendations for Reform.'
- Identity Theft Resource Center (ITRC) (2004). 'Identity Theft: The Aftermath 2004.'
- Identity Theft Resource Center (ITRC) (2005). 'Victim Resources: Victim Guide.'
- Johnson, L. D. (2004). 'Statement of Larry D. Johnson, Special Agent in Charge Criminal Investigative Division United States Secret Service.' Hearing on Identity Theft: The Causes, Costs, Consequences and Potential Solutions, Before *the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census of the Committee on Government Reform*.
- Kamerstukken II*, 2003/04, 1783: 3777-3778.
- Kamerstukken II*, 2005/06, 30 312, nr. 2.
- Kamerstukken II*, 2005/06, 30 312, nr. 4.
- Koops, B.J. & Ronald Leenes (Forthcoming 2006). 'ID Theft, ID Fraud and/or ID-related Crime: Definitions Matter.' *Datenschutz und Datensicherheit*.
- Lacey, D. & Suresh Cuganesan (2004). 'The Role of Organizations in Identity Theft Response: The Organization - Individual Victim Dynamic.' *The Journal of Consumer Affairs*, Vol. 38 (2): 244-261.
- La Lievre, E. & Rodger Jamieson (2005). 'An Investigation of Identity Fraud in Australian Organizations.' *Collaborative Electronic Commerce Technology and Research (COLLECTeR)*.
- Lenard, T. M. & Paul H. Rubin (2006). 'Much Ado About Notification.' *Regulation*, Vol. 29 (1): 44-50.
- Linnhoff, S. & Jeff Langenderfer (2004). 'Identity Theft Legislation: The Fair and Accurate Credit Transactions Act of 2003 and the Road Not Taken.' *Journal of Consumer Affairs*, Vol. 38 (2): 204-216.

- Linnhoff, S. & Jeff Langenderfer (2005). 'The Emergence of Biometrics and Its Effect on Consumers.' *Journal of Consumer Affairs*, Vol. 39 (2): 314-338.
- London School of Economics and Political Science (LSE) (2005). 'The Identity Project: An Assessment of the UK Identity Cards Bill & its Implications.' *Interim Report*, London.
- Lormel, D. M. (2002). 'Congressional Testimony.' Hearing on Senate Bill 2541 "Identity Theft Penalty Enhancement Act." Before *the Senate Judiciary Committee Subcommittee on Technology, Terrorism and Government Information*.
- Maatschappelijk Overleg Betalingsverkeer (MOB) (2006). 'Rapportage Maatschappelijk Overleg Betalingsverkeer 2005.' *Rapportage aan de Minister van Financiën*.
- Matejkovic, J.E. & Karen Eilers Lahey (2001). 'Identity Theft: No Help for Consumers.' *Financial Services Review*, Vol. 10: 221-235.
- McGuire, D. (2004). 'Bush Signs Identity Theft Bill.' *Washington Post Online* Posted on July 15, 2004.
- Mitchison, N. *et al.* (2004). 'Identity Theft: A Discussion Paper.' *European Commission Joint Research Center*.
- National Forum on the Payment System (2005). 'National Forum on the Payment System Report 2004.' *Report to the Minister of Finance*.
- Newman, G. R. & Megan M. McNally (2005). 'Identity Theft Literature Review.' *United States Department of Justice: National Institute of Justice*.
- Office of Community Oriented Policing Services (COPS) (2006). 'A National Strategy to Combat Identity Theft.' *U.S. Department of Justice*.
- Olson, R. K. *et al.* (2005). 'Identity Theft: A Personal Risk Management Approach.' *Chartered Property Casualty Underwriters (CPCU) eJournal*.
- Pastrikos, C. (2004). 'Identity Theft Statutes: Which Will Protect Americans the Most?' *Albany Law Review*, Vol. 67: 1137-1157.
- Pontell, H. (2002). "'Pleased to Meet You... Won't You Guess My Name?'" Reducing Identity Fraud in the Australian Tax System.' Paper presented at *the Centre for Tax Integrity, the Australian National University* on October 29, 2002.
- Prins, J.E.J. (2003). 'Het BurgerServiceNummer en de strijd tegen de Identiteitsfraude.' *Computerrecht*, (1): 2-3.
- Prins, J.E.J. (2006). 'Variaties op een thema: van paspoort- naar identiteitsfraude.' *Nederlands Juristenblad*, Vol. 81: 9-14.

- Shoudt, E. (2002). 'Identity Theft: Victims "Cry Out" For Reform.' *American University Law Review*, Vol. 52: 339-392.
- Solove, D. J. (2004). 'The Legal Construction of Identity Theft.' Presented at the *Symposium: Digital Cops in a Virtual Environment Yale Law School* (March 26-28, 2004).
- United Kingdom Cabinet Office (2002). 'Identity Fraud: A Study.' *United Kingdom: Cabinet Office Publications*.
- United Kingdom Home Office (2006a). 'Identity Crime Definitions.' <http://www.identity-theft.org.uk/definition.html>
- United Kingdom Home Office (2006b). 'What is Being Done About Identity Theft in the UK?' <http://www.identity-theft.org.uk/what-is-being-done.htm>
- United Kingdom Home Office (2006c). 'Updated Estimate of the Cost of Identity Fraud to the UK Economy.' <http://www.identity-theft.org.uk/ID%20fraud%20table.pdf>
- United States Department of Treasury (2005). 'The Use of Technology to Combat Identity Theft.' Report on the Study Conducted Pursuant to Section 157 of the Fair and Accurate Credit Transactions Act of 2003.
- Wang, G. *et al.* (2004). 'Criminal Identity Deception and Deception Detection in Law Enforcement.' *Group Decision and Negotiation*, Vol. 13: 111-127.
- Westby, J. (2004). Hearing on Identity Theft: The Causes, Costs, Consequences and Potential Solutions, Before *the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census of the Committee on Government Reform*.
- Wright, B. (2004). 'Internet Break-ins: New Legal Liability.' *Computer Law & Security Report*, Vol. 20 (3): 171-174.

**About the author**

Nicole van der Meulen completed her Bachelor of Arts degree at the University of Maryland, Baltimore County with a major in Political Science and minors in Sociology and Writing. Within the field of Political Science, she specifically focused on International Relations and Comparative Politics. During her undergraduate career, she interned at the Office of the Public Defender in Baltimore County and worked as a Research Associate for the Institute of Community Health, a local non-profit organization. She recently finished her Master of Science degree in Political Science at the Free University of Amsterdam. Nicole is currently a PhD researcher at the International Victimology Institute Tilburg (INTERVICT) where she conducts research on identity theft.

**About INTERVICT**

INTERVICT is a multidisciplinary institute which conducts research into a variety of aspects within the discipline of victimology. It is based at Tilburg University, with participation of the Faculty of Law and the Faculty of Social and Behavioural Sciences, and supported by various external partners. INTERVICT's mission is to work towards a comprehensive, evidence-based body of knowledge of victim empowerment. It aims to develop and implement a large-scale interdisciplinary research program in order to make significant contributions to the body of international victimological knowledge. The interdisciplinary approach of the research program ensures that proper research is performed into all aspects of victimization, which will ultimately contribute to preventing or reducing instances of criminal victimization across the world and to limiting the effects of such victimization on victims and their families including economic costs, pain and suffering.