Final Report

Study for an Impact Assessment on a Proposal for a New Legal Framework on Identity Theft

11 December 2012

Centre for Strategy & Evaluation Services

P O Box 159
Sevenoaks
Kent TN14 5WT
United Kingdom
www.cses.co.uk
## Contents

<table>
<thead>
<tr>
<th>SECTION</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>i</td>
</tr>
<tr>
<td><strong>1. Introduction</strong></td>
<td>1</td>
</tr>
<tr>
<td>1.1 Resume of Study Objectives</td>
<td>1</td>
</tr>
<tr>
<td>1.2 Methodological Approach and Research Plan</td>
<td>1</td>
</tr>
<tr>
<td>1.3 Structure of the Final Report</td>
<td>5</td>
</tr>
<tr>
<td><strong>2. What is Identity Theft?</strong></td>
<td>7</td>
</tr>
<tr>
<td>2.1 Overview – What is Identity Theft?</td>
<td>7</td>
</tr>
<tr>
<td>2.2 Key Elements in Defining Identity Theft</td>
<td>9</td>
</tr>
<tr>
<td>2.3 Review of Existing Definitions</td>
<td>10</td>
</tr>
<tr>
<td>2.4 Towards a Common Definition</td>
<td>15</td>
</tr>
<tr>
<td>2.5 Identity Theft and Fundamental Rights</td>
<td>19</td>
</tr>
<tr>
<td>2.6 Conclusions – Definition of Identity Theft</td>
<td>19</td>
</tr>
<tr>
<td><strong>3. Problem of Identity Theft</strong></td>
<td>21</td>
</tr>
<tr>
<td>3.1 Identity Theft Problem Tree and Intervention Logic</td>
<td>21</td>
</tr>
<tr>
<td>3.2 Drivers of the Identity Theft Problem</td>
<td>25</td>
</tr>
<tr>
<td>3.3 Identity Theft Methods – Online and Offline</td>
<td>34</td>
</tr>
<tr>
<td>3.4 Types of Identity Theft Information and Victims</td>
<td>47</td>
</tr>
<tr>
<td>3.5 Cross-border Dimension of the Problem</td>
<td>50</td>
</tr>
<tr>
<td>3.6 Conclusions – Problem of Identity Theft</td>
<td>54</td>
</tr>
<tr>
<td><strong>4. Quantification of Identity Theft Problem</strong></td>
<td>55</td>
</tr>
<tr>
<td>4.1 Overview</td>
<td>55</td>
</tr>
<tr>
<td>4.2 Number of Identity Theft Victims</td>
<td>57</td>
</tr>
<tr>
<td>4.3 Costs and Other Effects of Identity Theft</td>
<td>62</td>
</tr>
<tr>
<td>4.4 Impact on the EU Economy and the Wider Society</td>
<td>69</td>
</tr>
<tr>
<td>4.5 Conclusions – Impact of Identity Theft</td>
<td>76</td>
</tr>
<tr>
<td><strong>5. National Perspectives &amp; Existing Measures</strong></td>
<td>79</td>
</tr>
<tr>
<td>5.1 Identity Theft Legislation and Institutional Frameworks</td>
<td>79</td>
</tr>
<tr>
<td>5.2 Identity Verification Systems and Preventative Aspects</td>
<td>90</td>
</tr>
<tr>
<td>5.3 Identity Theft Reporting Systems and Victim Support</td>
<td>100</td>
</tr>
<tr>
<td>5.4 International Cooperation in Investigations</td>
<td>105</td>
</tr>
<tr>
<td>5.5 Conclusions – National Perspectives and Existing Measures</td>
<td>108</td>
</tr>
</tbody>
</table>
## Contents

### 6. EU Policy Objectives & Options  116

- 6.1 Policy Objectives  116
- 6.2 Intervention Logic  117
- 6.3 Overview – Policy Options  118
- 6.4 Policy Option 1: Status Quo  120
- 6.5 Policy Option 2: Non-legislative EU action  122
- 6.6 Policy Option 3: EU Legislative Action  128
- 6.7 Policy Option 4: Combined Action  129

### 7. Impact Assessment  131

- 7.1 Assessment Framework  131
- 7.2 Overview of the Impact of Policy Options  132
- 7.3 Assessment of Policy Option 1 – Status Quo  138
- 7.4 Assessment of Policy Option 2 – Non Legislative EU Action  141
- 7.5 Assessment of Policy Option 3 – EU Legislative Action  156
- 7.6 Assessment of Policy Option 4 – Combined Action  165
- 7.7 Political Feasibility of the Policy Options  167
- 7.8 Monitoring and Evaluation  168
- 7.9 Conclusions – Impact Assessment  170

### 8. Summary & Overall Conclusions  171

- 8.1 Problem of Identity Theft  171
- 8.2 Definitonal Issues and Existing National Legislation  173
- 8.3 Policy Options and Impact Assessment  174
## Contents

<table>
<thead>
<tr>
<th>APPENDICES</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Overview of Legislation in the Member States</td>
<td>178</td>
</tr>
<tr>
<td>B. Feedback on the Problem Tree</td>
<td>194</td>
</tr>
<tr>
<td>C. Examples of Identity Authentication Methods</td>
<td>195</td>
</tr>
<tr>
<td>D. EU and International Policy Measures</td>
<td>196</td>
</tr>
<tr>
<td>E. Case Studies</td>
<td>211</td>
</tr>
<tr>
<td>F. Credit Card Fraud in the Member States</td>
<td>290</td>
</tr>
<tr>
<td>G. Overview of Identification in the Member States</td>
<td>298</td>
</tr>
<tr>
<td>H. Internet and Facebook Users</td>
<td>310</td>
</tr>
<tr>
<td>I. Reporting Mechanisms in the Member States</td>
<td>311</td>
</tr>
<tr>
<td>J. Member States with Legislation under Development or Unclear Coverage</td>
<td>319</td>
</tr>
<tr>
<td>K. 2012 Eurobarometer on Cyber Security</td>
<td>320</td>
</tr>
<tr>
<td>L. Qualitative Assessment of Impacts</td>
<td>326</td>
</tr>
</tbody>
</table>
Executive Summary

Below we provide a summary of the main conclusions of the assignment “Study for an Impact Assessment on a proposal for a new legal framework on identity theft”. The study was undertaken for Directorate-General Home Affairs (DG HOME) by the Centre for Strategy & Evaluation Services (CSES) in cooperation with Deloitte.

The study was launched to inform the Commission’s Impact Assessment on a possible new legislative instrument in the field of identity theft. In line with the Terms of Reference, the preparatory study follows the Commission’s Impact Assessment guidelines.

More specifically, the Impact Assessment Study will inform the Commission’s decision on whether criminal law measures in the field of identity theft are appropriate at the EU level, or whether instead there are other more effective measures that would provide added value in addressing the problem of identity theft. A combination of measures could also be foreseen.

1. Problem of Identity Theft

Stolen data that are used maliciously (either directly by the person who ‘stole’ it or by a third party that acquired it) has impacts on individuals, businesses and/or public sector institutions. A distinction can be made between the costs to the ‘primary victim’, that is, the person whose identity is abused, and the ‘secondary victim’, i.e. the third party who is defrauded or otherwise harmed by the perpetrator impersonating the primary victim.

1.1 Drivers of Identity Theft

The key driver of the problems is the ‘motivation’ or incitement for criminals to obtain identity information because of the benefits (in particular of financial nature) for them. Insufficient or ineffective prevention activities as well as ineffectiveness and inefficiencies in national legal and institutional frameworks, as well as lack of cross-border collaboration, make these types of criminal activities easier. In this sense, they are not drivers per se but rather weaknesses in national responses that make it easier for criminals to commit and get away with this type of crime. Lack of awareness helps explain why victims of identity theft have displayed various forms of risky behaviour.

Online identity theft accounts for the bulk of the known cases. Online ID theft activities include spamming, phishing and the use of spyware. Offline ‘real world’ ID theft activities involve, for example, passport forgery, counterfeit of fingerprint identification, forgery of administrative and official state-issued documents. According to a 2008 study for PayPal, a quarter of the respondents said they were very concerned about identity theft. More recently, a 2011 Eurobarometer survey indicates that more than 40% of European Internet users have been asked to disclose more information than required for accessing or using a service on the Internet. A Generation Y online survey in April 2010 highlighted the fact that it is often young adults often engage in risky online behaviour. Over seven out of ten stated that they were not always as careful as they should be when posting and accessing information online.
Executive Summary

As concerns the types of crime for which identity-related information is used, according to the survey results the key incentives for criminals are financial fraud and money laundering. Human trafficking and the transfer / selling of identity information are suggested to be less frequent motivations. Identity information is, however, also used for further types of crime, including illegal health care access, organised crime, terrorism, drugs trafficking, illegal immigration and bullying and damaging people’s reputation.

1.2 Scale of the Problem

Identity theft and identity-related crime affects a considerable proportion of the population, and the problem is increasing. Our mid-range estimate suggests that as many as 8.2 million individuals are affected by identity theft (2% of the EU’s population) with an average loss of around €2,500 or €20bn at the EU level. There are also indirect financial costs of identity theft arising from damage to an individual’s credit rating, the cost of rectifying the consequences of identity theft (e.g. replacing documents), as well as non-financial impacts of an adverse nature such as stress and reputational damage. Fundamental rights issues are also relevant. Bearing in mind that some identity theft goes undetected or is not made known for statistical purposes, this estimate is likely to be on the low side.

The costs of identity theft to European business are more difficult to estimate because very little research has been undertaken. Our estimate is that business losses could be as high as €500bn or 0.4% of EU GDP. Businesses are affected both as ‘primary’ and ‘secondary’ victims. Of these two categories, the second is easier to estimate and is likely to be similar to the estimate provided above for the number and value of identity theft cases for individuals because these losses are ultimately borne by businesses (insurers, banks, etc.), either directly as a result of settling claims for reimbursement, or because of the need to invest in systems to help minimise the risk of identity theft. (The ultimate net loss, i.e. cases of identity theft-related financial losses where it is not possible to recover the sums involved from the perpetrators is not possible to estimate).

Although the scale of identity theft affecting the private sector directly is more difficult to estimate, there is some useful evidence from Member States. For example, according to data from the UK, the banking industry lost EUR 19.5 million in 2009 as a result of forged cheques (a genuine cheque, stolen and used by a fraudster with a forged signature) and a further loss of EUR 624 million from plastic card, online banking fraud and telephone banking fraud in 2009. The UK telecommunication industry suffered losses in 2009 of around EUR 830 million in the same year as a result of identity theft-related fraud.

Public authorities can also be victims of identity theft when their means of identification are used by someone else. This could be done via illegal access to data bases, the forgery of official documents etc. Similar to businesses, public authorities are also used as a source of information to access personal data of data subjects, including staff and clients. Section 4 elaborates on the scale of the problem.
Executive Summary

According to the survey results for this study, identity theft is increasing and seen as having a pronounced European/cross-border dimension. Indeed, only one of the 89 respondents who answered this question in the online survey launched by CSES indicated that there is no cross-border dimension to the problem, while 68.5% of the respondents considered that there is a ‘quite’ or ‘very’ significant cross-border dimension. Only 6.7% stated that there is hardly any cross-border dimension to the problem. A disproportionate number of perpetrators were, in the survey, indicated to be based in and the proceeds of identity theft go to countries mainly outside of the EU, although a few EU Member States were mentioned by the respondents. These were Romania, Spain, UK, “Eastern Europe”, France, Italy and Poland.

In addition to the loss of money, identity theft can have non-financial consequences for victims. This can include the time and cost associated with cleaning up identity and may have tort implications in some cases. In addition, identity theft may have non-financial effects including psychological and social distress as well as trust implications and limitations of the fundamental rights of data protection and privacy. Furthermore, there are costs to the wider public including enforcement costs and costs associated with crimes that were facilitated by identity-related crimes (e.g. money laundering, illegal immigration etc.). Ultimately, these effects will impact on the extent to which the European area of justice, freedom and security can be realised.

2. Definitional Issues and Existing National Legislation

At present, only some EU Member States have enacted specific ‘identity-related crime’ or ‘identity theft’ legislation. According to a “Comparative study on legislative and non-legislative measures to combat identity theft and identity related crime” (the 2011 RAND report) these are Estonia, France and Slovenia. More recently, according to the present assignment Poland introduced specific provisions in 2011. In the survey we asked for opinions on how effective legislation is in relation to the prosecution of identity theft and identity-related crime (e.g. whether all cases of identity theft and identity-related crime currently covered or there are gaps). A relatively low proportion of the respondents consider existing national legislation to be effective in combating identity theft.

2.1 National Legislation and Measures

In many countries, identity theft is tackled mainly through legislation on fraud, i.e. the secondary crime. Examples of where this is the case include Belgium, Czech Republic, Bulgaria, Germany and the UK. The absence of specific legislation on identity theft does not mean that identity theft is not criminalised in the Member States whose laws do not refer to the identity-related element of the act concerned. Most of the Member States where this is so instead use legal provisions on fraud or forgery and thus do not commonly refer to identity ‘theft’ but rather to ‘fraud’. Furthermore, the mere ‘theft’ of an identity is not always considered a crime but rather it is the use made of the identity acquired illegitimately that takes the conduct into the criminal area. In this way, identity theft is considered as a preparatory act for committing another, independently criminalised offense and not as an act that is criminalised in its own right.

In a written survey with the Member States, to which 18 countries replied, three countries (Czech Republic, Italy and Ireland) confirmed that primary victims are
covered in national legislation before a secondary crime has committed. This said, the legislative situation in other Member States is not clear-cut, and there are opportunities for primary victims to obtain redress in certain cases also in other Member States. In many countries, primary victims are covered once a secondary crime has been committed by means of the stolen identity information.

Currently in the EU there is neither a common terminology used to describe the phenomenon of identity theft (Member States use ‘Identity Theft’, ‘Identity Fraud’ and ‘Identity-related Crime’) nor a common legal definition of it. The extent to which and in what way this general phenomenon is recognised and criminalised in Member States is determined by national laws and the approach taken by the different national legal systems varies considerably.

2.2 Scope for EU Action

The absence of a common definition is a complication in developing a strategy at an EU level to combat identity theft. Most experts consulted as part of the study thought that it would be helpful to have a common definition. However, they suggested that it would be very difficult to agree on the content and scope of the definition and suggested that it should perhaps remain a guideline rather than a legally binding text. Others argued for making a common definition as comprehensive as possible and as ‘operational’ as possible. It was argued that provisions for ‘dishonest intent’ would have to be included in any common definition as a requirement for criminal conduct in this area.

Any EU-wide legal framework on identity theft should achieve not only a harmonised and consistent framework but one that creates scope for practical measures to counter the phenomenon. Two broad approaches are possible to developing a common EU definition – a ‘fully-functional’ common EU definition of identity-related crime or a more flexible definition focusing on key principles.

The advantage of the first ‘fully-functional’ approach is that it would: clarify the exact nature of the conduct that needs to be criminalised; make clear that the crime is one of conduct rather than one defined in terms of the result of the activity, which in a multifaceted and rapidly developing area risks serious limitations and anomalies; and enable more precise gathering of statistical data and improved monitoring of progress in combating identity-related crime.

The factors in favour of a less specific approach include leaving the Member States free to define criminal conduct with respect to identity theft in the way most consistent with, and appropriate to, their own legal systems. A suggested working definition of identity theft is provided in the report.
3. Policy Objectives, Policy Options and Impact Assessment

The rationale for EU intervention is that identity theft and identity-related crime is affecting a significant proportion of the EU’s population, as well as businesses and public institutions, and that action at an EU level is necessary to effectively tackle the problem. As noted earlier, cautious estimates suggest that a range between 2 million and 8 million individuals could be affected per annum and that costs are estimated at 20 bn euros per annum. Secondly, the identity theft has transnational aspects and other features that mean that effective action to tackle the problem requires intervention at an EU level.

3.1 Policy Objectives

EU policy objectives are summarised below:

<table>
<thead>
<tr>
<th>General objectives</th>
<th>Specific objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>To combat identity theft and identity related crime</td>
<td>• To reduce identity theft and related crime.</td>
</tr>
<tr>
<td></td>
<td>• To improve the capacity to prevent and tackle identity theft and related crime both in the public and private sectors, including in relation to cross-border aspects of the problem, at national and EU level.</td>
</tr>
<tr>
<td>More generally, to promote security, combat crime and protect victims’ rights</td>
<td>• To ensure that primary and secondary victims of identity-related crime obtain support and redress.</td>
</tr>
<tr>
<td></td>
<td>• More generally, to safeguard fundamental rights, including in particular:</td>
</tr>
<tr>
<td></td>
<td>- Right to liberty and security (Art. 6);</td>
</tr>
<tr>
<td></td>
<td>- Respect for private and family life (Art. 7) and protection of personal data (Art. 8);</td>
</tr>
<tr>
<td></td>
<td>- Right to property (Art. 17);</td>
</tr>
<tr>
<td></td>
<td>- To protect consumers (Art. 38), whose identity information may be acquired and abused in relation to online shopping, as well as shopping in the offline world and thus have a negative impact on consumer protection. This is also a fundamental right.</td>
</tr>
<tr>
<td></td>
<td>- Right to an effective remedy and to a fair trial (Art. 47)</td>
</tr>
<tr>
<td></td>
<td>• To protect business, in particular SMEs which tend to be more vulnerable to identity theft and its consequences than larger firms.</td>
</tr>
<tr>
<td></td>
<td>• To improve the knowledge base regarding identity theft and related crime.</td>
</tr>
<tr>
<td></td>
<td>• To prevent the risk of forum shopping in relation to identity theft and related crime in the EU.</td>
</tr>
</tbody>
</table>

Work is currently on-going at the EU level both in terms of preventative measures (e.g. concerning the security of online systems) and in terms of aggravated penalties if someone’s identity is used and creates damage to the owner in an online environment. The proposed new Victims Directive is also of key importance, as well as the proposal
Executive Summary

for a European Cybercrime Centre. It is important that any new initiative builds on these and other initiatives.

3.2 Policy Options

There are a number of policy options ranging from maintaining the status quo to legislative intervention to criminalise identity theft across the EU:

Policy Option 1 – Status quo: this option would be relevant if it is determined that the problem is not of such a nature and scale that the EU should intervene. The feedback obtained from the research suggests that most stakeholders are not content with a status quo situation. The CSES survey results show that the majority of the respondents (86.7%) think that there is a need for EU action to improve the current situation. Furthermore, the expert workshops and other consultations suggest that there is a need for EU action.

Policy Option 2 – Non legislative action: could involve the establishment of an online platform for victims and specialists to share experience and knowledge (Sub-option 2.1); the establishment of a network of contact points, which would be responsible for monitoring the situation in the Member States and providing support to victims (Sub-option 2.2); and a Commission Recommendation on a common definition and various other measures to reduce the current fragmentation of approaches (Sub-option 2.3). Feedback from the research suggests that Policy Option 2.2 has widespread support but is not, in itself, a sufficient response to the growing problem of identity theft. Policy Option 2.1 is the least favoured sub-option amongst those we consulted. With regard to sub-option 2.3, the adoption of a common definition of identity theft is seen as essential if Member States are to work more closely together, and with the Commission, to tackle the problem of identity theft.

Policy Option 3 – Legislative intervention: could involve two sub-options. Firstly, adoption of a Directive on identity theft, focusing on primary victims - minimalistic approach (sub-option 3.1); and secondly, adoption of a Directive on identity theft and related crime, i.e. including both primary and secondary victims - maximalist approach (policy option 3.2). The adoption of a common definition of identity theft is seen as essential if Member States are to work more closely together, and with the Commission, to tackle the problem of identity theft.

Combinations of policy options have also been assessed, including two combinations of the non-legislative options, as well one option combining the three non-legislative policy options and the legislative policy option 3.1.

3.3 Assessment of Impacts

As a way of combining different aspects of the assessment, the following table provides a high level summary of the impacts that the research suggests are likely to come about (vertical axis) in relation to different policy options (horizontal axis) using the ‘high level’ criteria set out as part of the intervention logic in Section 3. The status quo is not included as it is rated as neutral.
**Executive Summary**

**Summary of Key Impacts**

<table>
<thead>
<tr>
<th>Impact/Policy Options</th>
<th>2.1</th>
<th>2.2</th>
<th>2.3</th>
<th>2.4</th>
<th>2.5</th>
<th>3.1</th>
<th>3.2</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relevance</td>
<td>●</td>
<td>●●</td>
<td>●●</td>
<td>●●</td>
<td>●●●</td>
<td>●●●</td>
<td>●●●</td>
<td>●●●●●</td>
</tr>
<tr>
<td>Effectiveness</td>
<td>●</td>
<td>●●</td>
<td>●●</td>
<td>●●●</td>
<td>●●●</td>
<td>●●●</td>
<td>●●●</td>
<td>●●●●●</td>
</tr>
<tr>
<td>Efficiency</td>
<td>●</td>
<td>●●</td>
<td>●●</td>
<td>●●●</td>
<td>●●●</td>
<td>●●●</td>
<td>●●●</td>
<td>●●●●●</td>
</tr>
<tr>
<td>Impact and added value</td>
<td>●</td>
<td>●●</td>
<td>●●</td>
<td>●●●</td>
<td>●●●</td>
<td>●●●</td>
<td>●●●</td>
<td>●●●●●</td>
</tr>
<tr>
<td>Feasibility</td>
<td>●●●●●</td>
<td>●●●</td>
<td>●●●</td>
<td>●●●</td>
<td>●●●</td>
<td>●●●</td>
<td>●●●</td>
<td>●●●</td>
</tr>
</tbody>
</table>

Overall, according to our assessment, Policy Option 4 is likely to have the biggest impact on identity theft as it would provide a comprehensive framework, addressing the current legislative gap in relation identity theft for primary victims (Policy Option 3.1), and with the legal means to enforce penalties, as well as introduce non-legislative measures in the form of an online platform and a network of contact points. Whether such a measure would be an effective deterrent to the perpetrators of identity theft beyond the modest impacts we have estimated is impossible to say but it would make it easier to tackle the consequences.

The main disadvantage of Policy Option 4 is that it would be more difficult to implement as it presupposes agreement between EU Member States on the need for action at an EU level, on adopting a common identity theft and the other provisions that a Directive would introduce. Policy Option 2 would be easier to implement but would not have the same impact on the problem. But these options are not mutually-exclusive and a step-by-step approach starting with Policy Option 2 but with the aim of working towards Policy Option 3 might be best.

**Based on our research, a step by step approach is also preferred by many actors.** Non-legislative action in the form that has been described above would be welcome including actions to share information, to help collect information and to oversee the development of an EU strategy to combat identity theft. In addition to these measures, a need for a Directive including a common definition of identity theft as a framework for further initiatives to combat identity theft in the future, including possible criminalisation is seen as useful by many of those consulted in the framework of the present study. Such an approach would demonstrate that the Commission is responding to the need for action to tackle the growing problem of identity theft with measures that are practical and add value to what Member States are already doing.
Executive Summary

4. Methodological Note

This assignment was carried out in three phases:

- **Phase 1: Preparatory Tasks** – including a set-up meeting with DG HOME, preliminary interviews with key stakeholders and initial desk research. The results of Phase 1 were presented in an inception report (19 January 2012).

- **Phase 2: Data Collection and Analysis** – Phase 2 involved different types of activities to collect information for the various aspects of the impact assessment study, such as a widely distributed online survey and interviews with key stakeholders. The outputs of Phase 2 included a baseline assessment of current problems for victims of identity theft and the effective pursuit of offenders, particularly in cases with a cross-border dimension, quantification of the scale and costs of identity theft for individuals and business, as well as draft definitions of the policy objectives and policy options. The results of Phase 2 were presented in the interim report (16 June 2012).

- **Phase 3: Impact Assessment and Final Report** – involved further analysis of the information collected as part of Phase 2, an impact analysis and preparation of a draft final and final report (December 2012).
Introduction

This document contains the final report on the assignment “Study for an Impact Assessment on a proposal for a new legal framework on identity theft”. The study was undertaken for Directorate-General Home Affairs (DG HOME) by the Centre for Strategy & Evaluation Services (CSES) in cooperation with Deloitte.

1.1 Resume – Study Objectives

The study was launched to inform the Commission’s Impact Assessment on a possible new legislative instrument in the field of identity theft. In line with the Terms of Reference, the preparatory study follows the Commission’s Impact Assessment guidelines.

More specifically, the Impact Assessment Study will inform the Commission’s decision on whether criminal law measures in the field of identity theft are appropriate at the EU level, or whether instead there are other more effective measures that would provide added value in addressing the problem of identity theft. A combination of measures could also be foreseen.

1.2 Methodological Approach and Research Plan

This assignment was carried out in three phases:

• Phase 1: Preparatory Tasks – including a set-up meeting with DG HOME, preliminary interviews with key stakeholders and initial desk research. The results of Phase 1 were presented in an inception report (19 January 2012).

• Phase 2: Data Collection and Analysis – Phase 2 involved different types of activities to collect information for the various aspects of the impact assessment study, such as a widely distributed online survey and interviews with key stakeholders. The outputs of Phase 2 included a baseline assessment of current problems for victims of identity theft and the effective pursuit of offenders, particularly in cases with a cross-border dimension, quantification of the scale and costs of identity theft for individuals and business, as well as draft definitions of the policy objectives and policy options. The results of Phase 2 were presented in the interim report (16 June 2012).

• Phase 3: Impact Assessment and Final Report – involved further analysis of the information collected as part of Phase 2, an impact analysis and preparation of a draft final and final report (December 2012).

The following diagram, taken from our tender, provides an overview of the research plan for the assignment and an indication of the timing of the different phases. It should be noted that the timing of the interim report was adjusted to allow a workshop to take place before the document was submitted and of the draft final report in order to allow for further research on countries that have adopted specific legislation on identity theft. The work that was carried out as part of each of the Phases is described in further detail below.
Introduction

Figure 1.1: Overview of Work Plan

Phase 1 – Preparatory tasks

At the outset of the assignment, we undertook a number of preparatory tasks, including a set-up meeting with DG HOME (15 December 2011) and preliminary discussions with Commission officials and other key stakeholders that were identified together with the Commission. During this phase, desk research was begun to identify examine readily available information and information gaps. We also finalised the methodological approach for the study and the arrangements for Phase 2. These and other activities led to preparation of an inception report, which was submitted on 19 January 2012 and a review meeting.

Phase 2 – Data Collection and Analysis

During the course of Phase 2 a number of research activities have been undertaken. This includes continuing desk research, a survey, an interview programme, research for eight country case studies and two workshops.

The Phase 2 survey was conducted online and aimed at obtaining feedback on a range of questions from key stakeholders. In total, there were 127 responses to the survey at the time when the final report was prepared. As can be seen from the following chart (based on 121 answers where the type of organisation represented was mentioned), law enforcement agencies made up the largest single group of survey respondents followed by private sector organisations (financial institutions, credit rating agencies, etc.) and national authorities. Insofar as the sample provides a good spread of responses across different identity theft stakeholder groups, it can be considered to be representative.
Introduction

There is no obvious way, however, of determining whether the number of survey responses obtained from each category is representative because the totals are not known (except with national authorities).

**Figure 1.2: Survey responses by type of organisation**

![Survey responses by type of organisation](chart)

The survey was re-launched several times to help boost the response rate. It should be noted that although there were 127 survey respondents in total, the number who completed all sections of the questionnaire was 89 with much lower numbers of responses to some of the questions (e.g. costs of identity theft).

Responses were obtained from all EU27 Member States except Slovenia. The sample is broadly representative of the EU Member States although some countries were slightly over-represented (most obviously BE, CY, LT) while others (DE, FR, IT) were by comparison under-represented. The following graph is based on 117 answers.
Introduction

Figure 1.3: Survey Responses by EU Member State

The Phase 2 interview programme focused on key stakeholders (national authorities, data protection and consumer organisations, legal experts, private sector bodies, etc.) in a sample of Member States (Estonia, France, Germany, Netherlands, Poland, Portugal, Romania, Sweden and UK). Furthermore, interviews were carried out with EU level stakeholders such as Europol and Eurojust, as well as the UN. The following table provides a breakdown of the interviews. A list of types of organisations interviewed is provided in Appendix A.

Table 1.1: Phase 2 Interview Programme (* information received in writing)

<table>
<thead>
<tr>
<th>Countries</th>
<th>No. of interviews</th>
</tr>
</thead>
<tbody>
<tr>
<td>France</td>
<td>4</td>
</tr>
<tr>
<td>Germany</td>
<td>2*</td>
</tr>
<tr>
<td>Netherlands</td>
<td>5</td>
</tr>
<tr>
<td>Poland</td>
<td>4</td>
</tr>
<tr>
<td>Portugal</td>
<td>7</td>
</tr>
<tr>
<td>Romania</td>
<td>6</td>
</tr>
<tr>
<td>Sweden</td>
<td>5</td>
</tr>
<tr>
<td>UK</td>
<td>4</td>
</tr>
<tr>
<td>Other interviews</td>
<td>8</td>
</tr>
<tr>
<td>Total</td>
<td>45</td>
</tr>
</tbody>
</table>
Introduction

In eight of the selected Member States (DE, FR, NL, PL, PT, RO, SE, UK) feedback from the interviews was used to produce case studies setting out an assessment of the nature and extent of the identity theft problem in the country concerned, the legislation in place to combat the problem and other issues. The feedback was complemented by desk research on the situation in each country. The case studies provide a more detailed insight to the nature and scale of the identity theft problem, existing national legislation and other measures to combat the problem, and how actions at an EU level could add value. The case studies are provided in Appendix E. It should be noted that the Phase 2 interview programme was not limited to the case study research and was broader in terms of country and thematic coverage.

Two workshops took place during Phase 2. The first of these (2 February) involved a one-day session with a small group of experts, Commission officials and a representative from Europol. The second workshop (18 April) had a larger number of participants with representatives from national authorities and law enforcement organisations from most EU Member States being present. Both workshops covered the definition of identity theft, current problems and ways to address these, including EU action. At both workshops, the participants provided very useful feedback on key issues as well as experiences and information from their Member States.

Phase 3 – Impact Assessment and Final Report

In the final phase of the study we completed the outstanding research and prepared a draft final report setting out an analysis of the research and containing the impact assessment. The draft final report was reviewed with the Commission and presented at an inter-service meeting in September 2012.

1.3 Structure of the Final Report

The final report is structured as follows:

- **Section 2: Definition of identity theft** - examines the definition of identity theft and issues involved in developing a common definition;
- **Section 3: Problem of identity theft** - outlines the problem in terms of the methods used, targets and national responses;
- **Section 4: Quantification of identity theft impacts** – the scale of identity theft, number of victims and financial and other costs, impacts of identity theft and related crime on primary and secondary victims;
- **Section 5: National Perspectives** – legislation in place in Member States to combat identity theft, the national institutional frameworks and measures to prevent and combat the problem.
- **Section 6: Policy objectives and options** - outlines the policy objectives and the policy options that might be adopted to promote them and address the problems outlined earlier;
Introduction

• **Section 7: Impact Assessment** - provides an assessment of the impacts of the policy options against a number of key criteria.

• **Section 8: Overall conclusions** – summarises the key findings and overall conclusions from the research.

The report is supported by a number of appendices including an overview of legislation relating to identity theft in the EU Member States (Appendix A), a summary of EU and international policy measures (Appendix C) and a set of case studies examining the problem of identity theft and responses to it in a number of Member States (Appendix E). Other technical appendices are also provided.
What is Identity Theft?

In this section, we examine the definition of identity theft and some of the key issues involved in developing a common definition at the EU level. A common definition is the key to many of the possible actions that could be taken at the EU level to combat the problem.

2.1 Overview - What is Identity Theft?

The situation most generally understood to constitute identity theft involves both primary and secondary victims. To illustrate this, an example can be taken of a situation where person A obtains evidence of person B's identity so as to impersonate B (the primary victim) with the aim of procuring cash, goods or services from person or entity C (the secondary victim). Within this general formulation there are numerous permutations.

At the most basic level, evidence of B's identity may take the form of traditional identity documentation, such as a passport or driving licence or, in the Internet medium, a username and password. However, more sophisticated evidence of identity may include either B's biometric details, such as fingerprints or DNA, or biographical information such as past addresses, employment or the unmarried name of a parent or grandparent. Furthermore, A's objective in impersonating B may take other forms than obtaining a financial benefit such as cash, goods or services. These aims may include, for example:

- Human trafficking (often via large, transnational criminal networks) and illegal immigration. False ID documents e.g. allow illegal immigrants to pass through border controls;
- Avoiding a criminal prosecution or a fine;
- Enabling A to obtain a new identity when his/her credit record is bad or to evade payment of debts;
- Money laundering;
- Terrorism;
- Drugs trafficking;
- Inflicting harm on B in the form of damage to his reputation, Internet bullying or stalking;
- To enable A to avoid being recognised by his/her true identity, for example if s/he is a disqualified driver or a paedophile wishing to obtain permission to work with children;
- Inflicting B's right to privacy and family life.

Another permutation of identity theft occurs where A does not acquire and use another person's identity, but instead invents an identity. While invented identities or aliases may have innocent and socially acceptable purposes, it is widely acknowledged that they can also be used for the purpose of fraud and in this event should be considered to fall within the phenomenon of identity theft, even though they do not involve the theft of another “actual” individual's identity and therefore do not give rise to a primary victim as in the classic scenario referred to above.
What is Identity Theft?

As far as the boundaries of identity theft are concerned, it is not self-evident that the mere acquisition of identity information should in itself be considered to fall within the definition of identity theft, even if the gathering of such information was not authorised by the persons whose identity was involved. Such activity may involve infringements of data protection regulations but, that aside, various sorts of identity information are widely available in the public domain and may be legitimately used by, for example, market researchers or advertisers. Any initiative to address primary victims needs to take this into account.

Another issue is whether it should be essential for identity theft to be linked to a secondary act beyond the first "effect" of the risk to someone's identity that is already created through the theft of his/her information, and if so, what the nature of that link should be (actual commission, intent, etc.). In many cases there could well be difficulties in proving a secondary outcome and, at the same time, there are policy arguments, particularly in relation to conduct such as 'phishing', in favour of enabling the law to intervene at an earlier stage where intent can be shown, even before the damage has arisen. National legal systems have given attention to such issues. In the UK, for example, the Fraud Act 2006 now focuses on the intent lying behind the conduct rather than on its result, whereas previously if the law was to intervene before the conduct achieved its objective it could only do so by way of charging A with an attempt to commit a crime, which carried its own problems.

There are various forms of behaviour involving the unauthorised acquisition of identity information that do not constitute identity theft in this sense of being accompanied by a provable intent on the part of A to obtain a benefit or inflict financial damage on B. Examples include:

- Person A acquiring B's identity information in order to read personal communications but with no further use of the information (although this could of course cause offence to the person concerned).
- Employer A acquiring employee B's identity information for the purpose of surveillance or with a view to some other action that falls within the legitimate concern of the employer.
- Person A collecting identity information of numerous individuals without authority where the intent behind this widespread acquisition of information is impossible to establish but nevertheless gives rise to a risk of damage to B or C (some forms of mass marketing could fall into this category).
What is Identity Theft?

2.2 Key Elements in Defining Identity Theft

Currently in the EU there is neither a common terminology used to describe the phenomenon of identity theft (Member States use “Identity Theft”, “Identity Fraud” and “Identity-related Crime”) nor a common legal definition of it. The extent to which and in what way this general phenomenon is recognised and criminalised in Member States is determined by national law and the approach taken by the different national legal systems varies considerably.

However, notwithstanding the absence of a common definition, identity theft generally involves a number of key elements, as outlined in the following figure:

Figure 2.1: Key elements in defining identity theft for the purpose of a legal provision

To elaborate on the diagram:

- **Objective**: at the most basic level, all types of identity theft involve the use of personal information in a pernicious and illegitimate manner and/or for dishonest objectives. Immediately, therefore, consideration has to be given both to the type of information involved and the use to which it is put by the wrongdoer.

- **Type of identity information** – while the kinds of personal information that may be involved are many and various, it is their relevance to identifying a particular individual that is the common feature (e.g., identity documents, logins, 

---

1 In this section where we use the term ‘identity theft’ we intend this, save where the context indicates otherwise, to include identity fraud and identity-related crime generally.
What is Identity Theft?

passwords, bank account details, credit card numbers) as well as false identifying documents enabling the creation of a 'synthetic identity'. Rather than list or categorise the types of identity information that are targeted in identity theft it is preferable merely to note (in the same way as in the OECD definition – see below) that the identifying information is “personal” and to leave its exact nature undefined.

- **Primary crime/secondary crime**: the types of acts covered include, firstly, ones that cause harm to the individual whose identity information is wrongfully used (the primary victim). These acts involve the wrongdoer pretending to have the identity of the victim, having acquired the information in various possible ways, for example, by stealing identity documents or from tricking the individual into giving away online identifying information such as passwords or acquiring such information from a third party. A second basic category of acts are ones where the motivation for this misuse of identity information involves defrauding or damaging another party such as a bank or retailer (the secondary victim).

Other elements include the qualifier and the issue of dishonest intent. The significance of these elements lies principally in the need to ensure that uses of identity information that are socially acceptable do not find themselves characterised as identity theft. Thus where authorisation has been given – and perhaps even where this can be implied – the acquisition, use, transfer etc of personal information is in principle seen as permissible.

Similarly, unless the intent lying behind the action is generally regarded as being to some degree reprehensible there is a clear risk that actions will be drawn into the net that ought not to be regarded as forms of identity theft. This is because, at a very general level, criminal law reflects society’s most fundamental attitudes to its members’ conduct. If the law does not criminalise certain conduct or otherwise prohibit it, it is permitted. On the other hand, if it is defined as criminal, carrying a range of punishments, society’s law makers have carefully assessed the respects in which that conduct is to be prohibited and have calibrated the degrees of seriousness of any breaches of the law with a range of punishments. Whenever new types of socially-disapproved conduct emerge, which fall outside the current criminal law, law makers are eventually compelled to consider bringing them within its ambit. This, in broad terms, is what is happening now with regard to the conduct we have characterised as ‘the general phenomenon’ of identity theft.

### 2.3 Review of Existing Definitions

As noted earlier, there is no universally-accepted definition of the term ‘identity theft’. Below, we review a number of definitions that have been used by the Commission, OECD and several other organisations.

The Commission’s terms of reference for the study begins with the proposition: ‘...Identity theft involves the impersonation of someone else in order to obtain an advantage or to avoid detection...’ However, as we have seen above, even a seemingly broad statement such as this fails to include all the kinds of conduct involving identity information that are
commonly understood to be socially pernicious and meriting prohibition and sanction and which the present study is required to address. This example does not, for instance, deal with malicious damage to reputation through identity theft. Nor does it cover the transfer of identities without intended or actual advantage (e.g. free of charge), which may be required to be considered.

As already argued, the term 'identity theft' may not be the best description of what is intended to be covered, for 'theft' can be regarded as an over-limiting term in the context of the many and varied kinds of action that are popularly grouped together under 'identity-related crime'. If 'theft' is an over-limiting element and 'identity-related crime' is a more comprehensive starting point, what then is to be understood come within the scope of this term? While still using (as we will do by way of shorthand) the description 'identity theft', the OECD has proposed the following:

“Identity theft occurs when a party acquires, transfers, possesses or uses personal information of a natural or legal person in an unauthorised manner with the intent to commit, or in connection with fraud or other crimes.”

Whilst at first sight broad, this approach to defining what should be included does not deal with behaviour where the ingredient of intent to commit fraud or other crimes is missing, such as the mere acquisition of personal data, even though, as mentioned, this area undoubtedly involves difficult policy issues. Nor, clearly, does it attempt to describe in any detail the relationship with the 'secondary' crime. It does not describe how, or whether, the unauthorised acquisition or use is to be viewed as deceptive, or the range of results of such conduct that are to be integral to its criminality.

2.3.1 Primary and secondary victims

The degree to which definitions of identity theft limit their attention to the primary victim whose identity has been acquired or go further to incorporate the link to a secondary victim is one way of categorising the various alternative approaches. This distinction is particularly important to the current study as it influences the scope for EU intervention. Examples of definitions that focus on the primary victim are:

- “Identity theft [...] occurs when one person [...] obtains data or documents belonging to another – the victim – and the passes himself off as the victim”. This definition contains two key elements – the object (data or documents belonging to another) and two acts that are both required in order to lead to a criminalisation. The first is the obtaining of data. In addition, the offender needs to pass him- or herself off as the victim. It should be noted,
What is Identity Theft?

however, that if this constitutes a single offence, neither the act of obtaining the information nor the act of obtaining the information in order to sell it, or the act of transferring, is by itself covered by the definition.

• “Identity-related crime concerns all punishable activities that have identity as a target or principal tool”. 5 Again, this approach neither specifies the object covered nor does it set out the criminalised acts. Instead it is based in part on whether conduct is already criminalised as opposed to whether it is harmful and should be criminalised. It therefore does not advance an understanding of the elements significantly and does not assist in arriving at a common understanding on which to begin building up a working definition. 6

• “Identity theft” may be used to describe the theft or assumption of a pre-existing identity (or significant part of it) with or without consent, and regardless of whether the person is dead or alive. 7 This brings together two elements: the object (identity) and the related acts (theft or assumption) and compared to other definitions, this provides a more detailed description of the object. However, the definition of the act focuses on obtaining the identity and its limitation, therefore, is that the transfer of identity-related information or the use of such information is not covered. In addition, once again this does not cover fictitious identities.

• “ID fraud arises when someone takes over a totally fictitious name or adopts the name of another person with or without their consent.” 8 This can be broken down into two elements: the object (fictitious or real identity) and the related act (takes over), but neither the object, nor the acts are further defined. The provision concentrates on the act of obtaining the identity and – depending on the interpretation of “takes over” – the use of the identity. Therefore it is unlikely that transferring or selling the identity-related information would be understood as covered.

One unique aspect is the fact that the definition does cover the act of taking over a fictitious name. This therefore reflects the current research 9 highlighting the fact that the majority of identity theft offences are related to fictitious identities.

---

5 See Koops/Lenes, Identity Theft, Identity Fraud and/or Identity-related Crime, Datenschutz und Datensicherheit, 2006, page 556.
6 Koops/Lenes, Identity Theft, Identity Fraud and/or Identity-related Crime, Datenschutz und Datensicherheit, 2006, page 556.
What is Identity Theft?

(synthetic) identities. However, one concern about this approach is that where existing identities are involved, the criminalisation is limited to names. Other types of identity-related information are not included. Another concern is that – depending on the interpretation of “take over” – this may also cover acts that are widely accepted as legitimate (such as the use of a fictitious name by an actor in a play or providing a fictitious name when asked by a stranger).

Examples of definitions that move beyond the act affecting the primary victim per se, and develop the link with fraud or with a secondary victim, include the following:

• “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”. Here the term identity theft contains two key elements: the object (identity) and the related act (using identity as a target or tool fraudulently or unlawfully). However, neither the object, nor the acts are further described. Furthermore the definition refers to “an existing person” and thereby does not cover fictitious identities which were highlighted as important during the first meeting of experts in Brussels on 2 February 2012.

• US Federal Law (18 USC s.1028(a)(7)) prescribes an offence where a person “Knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.” Three main elements can be noted here – the object (means of identification), the act (transfers, possesses, or uses) and the intention that links the act to further criminal activities (intent to commit, or to aid or abet, or in connection with, any unlawful activity). In the case of both the acts and the intended offences, the provision follows a broad approach. It is noteworthy that the act does not need to be related to fraud.

• Another US legal definition states: “Identity theft - the term “identity theft” means a fraud committed using the identifying information of another person, subject to such further definition as the Commission may prescribe, by regulation.” This brief description of the term “identity theft” is contained in 15 U.S.C. 1681a (q)(3). The main difference to the description provided by 18 U.S.C. § 1028(a)(7) is the fact that 15 U.S.C. 1681a(q)(3) links the term identity theft to fraud. This limits the application of the provision in other cases where the offender is using the identity-related information for other offences. In addition, despite the fact that the provision defines an act that contains the word “theft”, it only criminalises the use of the information but not the act of obtaining it.

11 Koops/Lanis, Identity Theft, Identity Fraud and/or Identity-related Crime, Datenschutz und Datensicherheit, 2006, page 556.
What is Identity Theft?

- A further definition from the US Federal Trade Commission in 15 U.S.C. 1681a(q)(3) is that: "The term 'identity theft' means a fraud committed or attempted using the identifying information of another person without lawful authority." The term 'identifying information' means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including: (a) name, social security number, date of birth, official state- or government-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number; (b) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation; (c) unique electronic identification number, address, or routing code; and (d) telecommunication identifying information or access device. Like 15 U.S.C. 1681a(q)(3), this description links the term identity theft to fraud and only covers the act of using the identity-related information.

2.3.2 Specific legislation on identity theft and identity-related crime

Only some EU Member States have enacted specific 'identity-related crime' or 'identity theft' legislation. According to a "Comparative study on legislative and non-legislative measures to combat identity theft and identity related crime" (the "RAND report") from 2011, these are Estonia, France and Slovenia. Furthermore, in the research for the present assignment it was established that Poland introduced specific provisions in 2011.

Estonia is an interesting case. In 2009 Estonia introduced a new Article into its Criminal Code, which targeted identity theft as it affects the primary victim whose identity information is misused, without touching upon secondary crimes such as identity fraud, which are covered elsewhere in the Criminal Code. The translation provided to us of the 2009 Article (Article 157) defines the new crime as follows:

"Illegal use of another person's identity - transmission of personal data that establish or may enable to establish the identity of another person, grant of access to the data or use thereof, without the consent of that person, with the aim to knowingly cause a misconception of that person by means of assuming that person's identity, if damage is caused thereby to the rights or interests of another person that are protected by law, or to conceal a criminal offence, is punishable by a pecuniary punishment or up to 3 years' imprisonment."

Section 3 and Appendix A contain a detailed assessment of the definition of identity theft in Member States. Given the differences in national laws relating to fraud and varying ways in which identity fraud is covered as a crime in the Member States, a definition which is concentrated upon damage to the rights and interests of the primary victim merits further consideration in the EU context. This is a point we develop later in this report.

12 Related Identity Theft Definitions, Duration of Active Duty Alerts, and Appropriate Proof of Identity Under the Fair Credit Reporting Act, Federal Register 69, no. 82.
What is Identity Theft?

2.4 Towards a Common Definition

Going beyond the requirement of a common understanding of the problem being addressed, since the present study involves assessing the need for a new EU instrument to define and criminalise identity theft, it is important to have a working definition to show what behaviour might be considered to come within its ambit. Putting together an illustrative example the various elements that would be needed in any comprehensive and common legal definition is an important starting point for any type of EU action. However, it should be emphasised that the purpose of a working definition in the present context is to help crystallise the analysis of the problem and possible ways of achieving policy objectives rather than attempting to arrive at any definitive legal draft, which is outside the scope of this study.

The views on what elements to be covered or not in the definition of identity theft as indicated in the online survey responses are presented in the chart below. The chart summarises the proportion of survey responses in the 'very' and 'quite' important categories. Most of the other responses were 'don't knows'. As can be seen, the elements of 'acquisition', 'transfer' and 'possession' are seen as the three most important elements in any definition. It can be noted that 'use' is only rated as fourth of the various elements included in the list.

Figure 2.1: Online survey respondents’ views on the importance of covering various elements in a common definition of identity theft

---

13 This was the conclusion reached at the Expert Workshop meeting on 2 February 2012 which called for a working definition of a crime of Identity Theft for the purposes of the study. In particular it was suggested by the experts that a working definition was required which would deal, firstly, with the issue of the relationship between any initial theft or misuse of identity information and a secondary required element, such as fraud and, further, would do so taking a broad perspective.
What is Identity Theft?

Our consultations, and the experts' workshops, confirm the importance of a common definition of 'identity theft' or 'identity-related crime' as a starting point for actions at the EU level to help combat the phenomenon. The view was expressed that a definition is essential to give focus to the problem and to promote information gathering about its extent. Moreover, there appears to be support for considering how to enact a criminal offence of 'identity-related crime' at an EU level. Whilst it is beyond the scope of this study to devise a common definition, some key considerations are highlighted below.

Building up the elements of a comprehensive definition requires going further than most existing definitions which, as we have noted, generally hitch the misuse of identity information to an existing crime, without any attempt to define the inter-action of these two separate aspects. Furthermore, various experts have stressed that as the field of cybercrime is constantly developing it is essential that any definition goes well beyond the traditional preoccupation with identity documents and their misuse and includes all the manifestations of online conduct that need to be classed as criminal. At the same time, it is key to keep the definition "technologically neutral", in order for it to not become obsolete or not cover new and emerging methods and activities.

As noted earlier, the question of the link to a 'secondary' crime is also central to defining where to draw the line between legitimate access and use of identity information and illegitimate access and use. For example, a person might establish a table of identity information on the basis of Facebook accounts and even make it available for sale – should that be considered a criminal offence? There was doubt expressed at the expert workshop about this. It also needs to be considered whether financial damage should be required or whether non-financial harm to the victim (such as could be caused e.g. through misuse of a Facebook account to post slanderous comments) should be covered as well; or, indeed, whether prejudice to a person's human rights should be covered. The consensus of experts consulted appears to favour this quite strongly.

Taking the various considerations discussed in the previous section into account and applying them to the illustrative OECD-type definition highlighted earlier, the 'minimum scope' elements are shown as being the object ("personal information of a natural or legal person") and the action ("...a party acquires, transfers, possesses or uses"). At the same time it can be noted that 'synthetic identifying information' is not included and that 'enabling impersonation of that person' is a missing minimum ingredient which only enters the picture when linked to the intent or connection with the committing of a crime.

A commented definition, which shows the effect in practical terms of each part of the wording, is outlined below. This illustrates how the various components of a definition might fit when applied to a comprehensive definition of identity theft or identity-related crime and how different kinds of conduct could be criminalised. Because this model definition is intended to be all-encompassing it includes identity theft affecting both primary and secondary victims.
What is Identity Theft?

Working Definition of Identity Theft

Identity theft occurs when any person [either one offender or a group of offenders]:

- (a) Acquires [for example by breaking into a computer system or collecting documents from the trash], or
- (b) Transfers [for example by granting someone (paid) access to a database of illegally obtained identity information], or
- (c) Possesses [for example by maintaining a copy of credit card records], or
- (d) Uses [for example by pretending to be the rightful owner of the identity]

Personal information of a natural or legal person [such as name, passport number, biometric identification data, credit card information, usernames and passwords, social security numbers] in an unauthorized manner [when for example a hotelier at a hotel reception produces a copy of a credit card that was handed over to him to settle a bill] with the intent to make a false representation as to his identity to:

- (a) Make a gain [for example by purchasing goods using somebody's credit card], or
- (b) Acquire a benefit for himself or another [for example by obtaining access to an expensive online database or other resource], or
- (b) Cause direct or indirect loss to another [for example by deducting money from her/his account, damaging her/his credit record or putting the victim in a position where she/he needs to in new effort to restore the situation prior to the time the crime was committed], or
- (c) Expose another to a risk of loss [for example by posting another person's credit card data, enabling others to abuse it], or
- (d) Damage the reputation of another [for example by posting slanderous messages], or
- (e) Expose another to a risk of damage to the reputation [see above], or
- (f) Mislead investigation related to any crime [for example by using somebody's identity while committing a crime and making the police believe it was committed by her/him].

Rather than starting from scratch, several existing definitions of identity theft could be used as a framework for developing a common definition. This includes elements of the OECD definition:

"Identity theft occurs when a party acquires, transfers, possesses or uses personal information of a natural or legal person in an unauthorized manner with the intent to make a false representation as to his identity in order to make a gain or acquire a benefit for himself or another or to cause loss to another or expose another to a risk of loss."

We have further elaborated the notion of "making a false representation" of identity as occurring when a person without lawful authority creates, appropriates or transfers proof or purported proof of: (i) either biometric identity; (ii) or documents recording identity; (iii) or identifying information used for obtaining access to information or property by means of a computer or automated system which relates or belongs to another person; or with the effect of creating a false impression in the mind of a recipient or facilitating unauthorised entry to a computer or automated system. With regard to

---

14 By "making a false representation" we mean making an untrue statement or otherwise creating a false or misleading impression.
causing a loss to another or exposing another to a risk of loss, we have taken this to include reputational loss and/or knowingly or recklessly prejudicing another's human rights. It can be noted that fictitious identities are not covered in the above definition. 15

This definition was tested in the online survey carried out as part of this study where the respondents were asked to indicate if they agree or disagree with the definition, and to make any suggestions for amendments. Although only a small number of survey respondents could answer the question on defining identity theft, most (68.6%) of those that did agree with this definition; only 7 out of 89 did not agree with the definition, while 54 agreed and 28 indicated that they 'don't know'. The table below shows the results of the online survey with regard to the need to establish a common definition and identity theft as a criminal offence in the EU.

Table 2.3: Online survey respondents’ views on the importance of establishing a common definition of identity theft at the EU level and establishment of identity theft as a criminal offence

<table>
<thead>
<tr>
<th>Options</th>
<th>1-Not important at all</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6-Very important</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establishment of a common definition of identity theft and identity-related crime</td>
<td>6.2</td>
<td>0.0</td>
<td>4.6</td>
<td>9.2</td>
<td>16.9</td>
<td>63.1</td>
<td>65</td>
</tr>
<tr>
<td>Establishment of identity theft as a criminal offence in the EU</td>
<td>6.3</td>
<td>4.7</td>
<td>6.2</td>
<td>12.5</td>
<td>15.6</td>
<td>54.7</td>
<td>64</td>
</tr>
</tbody>
</table>

Overall, it is clear that any legal definition at an EU level of a crime based on the misuse of identity information would diverge in various respects from national legislation as currently there is, to quote the RAND study, ‘no homogeneous approach to the topic of identity theft as such among EU Member States’. The more extensive and precise the definition, the more likely this is. Potential conflicts with existing legislation in the Member States would be a negative consequence of any EU-wide legal framework that included a newly-defined crime.

On the other hand, a definition of an identity-related crime that allows doubt to remain over the boundary between legitimate and illegitimate access and use of identity information might be considered even less desirable – the possibility of conflicts with national legislation would remain and at the same time little progress would have been made in achieving a homogeneous approach to the problem across the EU as a whole. A possible compromise approach would be to concentrate efforts on defining the types of misuse of identity-related information to be covered and to leave a required link to a secondary crime, such as fraud or even non-financial loss, as defined in national legislation, in the same way as in the OECD or the US Federal law definitions.

15 In order to cover fictitious identities consideration should be given to adding the words ‘or uses a fictitious identity’ to the proposed definition as follows: ‘Identity theft occurs when a party acquires, transfers, possesses or uses personal information of a natural or legal person in an unauthorized manner, or uses a fictitious identity, with the intent…’
What is Identity Theft?

2.5 Identity Theft and Fundamental Rights

Although influenced by the precise definition used, identity theft has a number of implications for fundamental rights, as established in the Charter of Fundamental Rights of the European Union\(^6\). The rights set out in the following Articles are, in addition to the Articles in the Chapter 3 on Equality, particularly affected:

- **Right to liberty and security** (Art. 6): Identity theft and related crime have a negative impact on the security of EU citizens.

- **Respect for private and family life (Art. 7) and protection of personal data (Art. 8)**: Identity theft and related crime implies the abuse of personal identity data and a lack of respect for private life. Thus, in order to safeguard these rights, it is imperative to combat identity theft as well as related crime.

- **Right to property** (Art. 17): This right is directly affected where property is the target of the related (secondary) crime. In relation to primary victims, this Article can also be interpreted to cover identity documentation and other (physical) sources containing identity information.

- **Consumer protection** (Art. 38): Identity information may be acquired and abused in relation to online shopping, as well as shopping in the offline world and thus have a negative impact on consumer protection.

- **Right to an effective remedy and to a fair trial** (Art. 47): This right is closely related to the protection of victims, who according to this Article have a right to an effective remedy.

In Section 6 of this report, we provide an assessment of how the various policy options affect fundamental rights.

2.6 Conclusions – Definition of Identity Theft

It is clear from this review of the meaning of ‘identity theft’ and various of the legal definitions of the term that are currently in use, as well as those that might be proposed, that the absence of a common definition of identity theft is an impediment to developing a strategy at an EU level to combat this problem.

At present, there is a lack of clarity as to what is understood to be within the scope of the phenomenon. However, there is a consensus amongst those we consulted that a common legal definition would be advantageous and is a necessary starting point for any interventions at the EU level. A further consideration is that a common definition would help in obtaining a more accurate EU-wide picture of the situation by assisting in common reporting and gathering of data and statistics.

\(^6\) http://www.europarl.europa.eu/charter/default_en.htm
What is Identity Theft?

The pros and cons concerning the form of any new EU-wide legal framework on identity theft essentially revolve around the possibility of achieving not only a harmonised and consistent framework, but one that creates scope for practical measures to counter the phenomenon. Factors in favour of a wider, more ‘fully-functional’ common EU definition of identity-related crime, including within its scope the effect on both primary and secondary victims, are:

- Giving clarity to the exact nature of the conduct that needs to be criminalised and defining clearly what areas of conduct should not be regarded as criminal;
- Where national laws on fraud (the ‘secondary’ element of the comprehensive definition) diverge, insofar as they are applicable to all aspects of identity theft, making clear that the crime is one of conduct rather than one defined in terms of the result of the activity, which in a multifaceted and rapidly developing area risks serious limitations and anomalies;
- Facilitating more effective cross-border cooperation between law enforcement authorities;
- Limiting the possible ability of Internet fraudsters to exploit differences between national legal systems in criminalising their activities;
- Enabling more precise gathering of statistical data and improved monitoring of progress in combating identity-related crime.

On the other hand, factors in favour of a less specific OECD-type of definition include leaving the Member States free to define criminal conduct with respect to identity theft in the way most consistent with, and appropriate to, their own legal systems. There is also a reduced possibility of unintended loopholes being introduced into different legal systems that may not at present be experiencing any significant difficulties in their existing legal response to identity-related crime. In particular, the OECD approach could be adapted so as to leave each Member State to deal with the impact of identity theft on secondary victims under their existing national laws – principally those relating to fraud. The example of Estonia’s recent Article 157 of its Criminal Code shows how a Member State has chosen to legislate on identity theft with a view to protecting exclusively the primary victim from types of damage that are mainly non-financial such as damage to reputation.

In the following sections of the report, for the purpose of examining the current problems, identity theft and related crime is considered in the wide sense. A narrower definition is then considered in the context of possible EU action to help tackle the problem. Any common definition of the crime that might eventually be drawn up would have implications for Member States’ existing legislation currently in use in combating ‘identity theft’, but the precise extent of this depends on the definition used (this is sue is considered later in the report).
In this section we analyse the problem of identity theft, including the causes ("drivers") of this problem as well as its effects. The links between these various elements that all form part of the problem definition are illustrated by means of a "problem tree". Estimates of the scale of the problem as well as how the problem is likely to develop are provided in Section 4. National responses are examined in Section 5.

3.1 Identity Theft Problem Tree and Intervention Logic

This section first provides a high level overview of the problems, drivers and effects, illustrated by means of the "problem tree" and supporting intervention logic. The purpose of the problem tree is provide a framework for analysing the causal links between the identified problems, their drivers and effects and to structure the research, a (hypothetical) "problem tree" was developed at the start of the assignment. The intervention logic sets the problem in the wider context of possible interventions to tackle the problem.

3.1.1 Identity Theft Problem Tree

The following chart sets out the problem tree. The focus is on identifying problems for individuals, businesses and public authorities. We have also considered the effect on primary and secondary victims of identity theft.

Figure 3.1: Outline of the problems, drivers and effects ("Problem Tree")
Problem of Identity Theft

The problem tree was tested in two expert workshops when the participants were asked to comment on the elements that were included in the diagram and the links between the different elements. While there was a general agreement that the problem tree provides a good picture of the current situation with regard to the problems, drivers and effects, some suggestions for refinements were made. How these have been taken into account is described in Appendix B.

The problem tree is based on a “matrix” of drivers. More specifically, amongst the drivers or causes of the current problems, there is a distinction to be made between the incitement / motivation of criminals, on the one hand, and inadequate national responses, on the other:

- The incitement / motivation of criminals is closely linked to the effects, in terms of e.g. economic gain for the perpetrators and or causing other types of harm to the victim, for example, in terms of harassment of individuals and damage to the reputation of business. Furthermore, research points to that there is a low risk of detection, which is an additional incitement for criminals.

- Inadequate national responses can further be divided into two different “pillars”, namely those relating to prevention and those relating to criminalisation and redress:
  - Prevention refers to the (risk) behaviour of legal and natural persons (such as individuals, business or public sector institutions) as well as the properties of systems underly the exchange and processing of identity information, presented on the left hand side in the figure.
  - Criminalisation and redress measures comprise the legal and institutional frameworks, presented on the right-hand side of the diagram. It also includes support to victims, provided by public and private organisations or NGOs.

When looking at the resulting problems, inadequacies in preventative measures impact on the scale of the problem of identity theft and related crime, and opportunities for perpetrators to acquire, store, transfer/sell on and use identity information. Inadequacies in criminalisation and redress measures complicate law enforcement, leads to difficulties in (international) police cooperation and to a lower risk of detection of identity-related crimes. This limits the deterrent effect resulting from law enforcement activities. Thus the main focus of the elements on the right hand side is on criminalisation and redress once a problem has occurred, and less weight is placed on reducing the scale of the problem, although this may be a “sub-aim”.

17 A first, small workshop was held on 2 February 2012. A larger workshop involving experts from the Member States was held on 18 April 2012. See also the introduction.
http://www.swindles.org/imp/risk/.
Problem of Identity Theft

Turning to the effects, stolen data that are used maliciously (either directly by the person who ‘stole’ it or by a third party that acquired it) will have a number of impacts on individuals, businesses or public sector institutions. A distinction can be made between:

- The costs to the ‘primary victim’, that is, the person whose identity is abused, and the ‘secondary victim’, i.e. the third party who is defrauded or otherwise harmed by the perpetrator impersonating the primary victim.

- There are also non-financial costs including psychological and social distress as well as trust implications and impacts on the fundamental rights of e.g. data protection and privacy as well as security. These effects may result both for those directly affected, as well as for others that hear about cases e.g. in the media.

- There can also be legitimate beneficiaries. Insurance companies may benefit from the problem. In the research, it has been identified that a number of insurance companies provide insurances against identity theft. While these companies will also need to bear some of the costs for the problem, it can be assumed that if this market would not be profitable on balance, such insurances would not be offered.

- Costs to society as a whole, including enforcement costs and costs associated with crimes that were facilitated by identity-related crimes (e.g. money laundering, illegal immigration etc.).

Ultimately, these effects of identity theft will impact on the extent to which the European area of justice, freedom and security can be realised. For this reason, and because identity theft has pronounced cross-border features and requires concerted action to be effectively addressed, there is prima facie a case for EU intervention. As concerns the broad competence of the Commission to act (without making an assessment of whether this can be justified or not), it can be noted that both DG CONNECT and DG HOME have competencies in the field. More specifically, many of the measures that may be counted as preventative action are covered by DG CONNECT (e.g. identity management etc.), while action by DG HOME tends to focus on criminalisation and redress measures, i.e. the drivers mentioned on the right hand side of the problem tree. In addition, it is DG HOME that could take action to support victims of identity theft.¹⁹

The problem assessment is provided in sections 3 to 5 of this report. In the present and the following two sections of the report, we have largely structured our analysis around

¹⁹ In line with the Terms of Reference, while being carried out on behalf of DG HOME, the present assignment is not limited to those areas in which DG HOME may take action, but a broad assessment of the current problems is to be carried out. Therefore, we have structured our analysis around the elements of the comprehensive problem tree rather than around the type of action that is in the remit of DG HOME.
Problem of Identity Theft

the elements of the problem tree. More specifically, in this section we start by examining the underlying driver of the problem, namely the motivation/incitement of criminals to acquire and use identity information. In the present section, we also discuss the problem in terms of the different methods used, types of identity information that are “stolen”, victims and the cross-border dimension of the problems. The impact of identity theft is examined in more detail in Section 4. Finally, in section 5 we outline national responses to the problem. While this is not strictly in line with the problem tree approach, the logic in terms of first examining the underlying driver, the problem and its effects and as a final step any inadequacies in national responses has been followed.

While the impacts of the problem are examined in detail in section 4, to provide the context for the next sections in summary, in terms of the primary victims, it is clear that identity theft and identity-related crime is affecting a considerable proportion of the population, and that the problem is increasing. Our mid-range estimate (see Section 4) suggests that around 8 million individuals are affected by identity theft (2% of the EU’s population) with an average loss of around €2,500 or €20bn at the EU level. Some of these costs are borne by insurance companies and banks. There are also indirect financial costs of identity theft arising from damage to an individual’s credit rating, the cost of rectifying the consequences of identity theft (e.g. replacing documents), as well as non-financial impacts of an adverse nature such as stress and reputational damage. It is relevant to differentiate between primary victims (those whose identity is “stolen”) and secondary victims (those who are affected by the crime that is committed on the basis of the stolen data). Fundamental rights issues are also relevant.

The costs of identity theft to European business are more difficult to estimate because very little research has been undertaken. Our best estimate is that business losses are around €300bn or 0.25% of EU GDP and perhaps as high as €500bn (0.4% of EU GDP). Businesses are affected both as ‘primary’ and ‘secondary’ victims. Of these two categories, the second is easiest to estimate and is likely to equate to a figure that is similar to the estimate provided above for the number and value of identity theft cases for individuals because these losses are ultimately borne by businesses (insurers, banks, etc.), either directly as a result of settling claims for reimbursement, or because of the need to invest in systems to help minimise the risk of identity theft. (The ultimate net loss, i.e. cases of identity theft-related financial losses where it is not possible to recover the sums involved from the perpetrators is not possible to estimate).

Public authorities can also be secondary victims of identity theft when their means of identification are used by someone else. This could be done via illegal access to data bases, the forgery of official documents, etc. Similar to businesses, public authorities are also used as a source of personal data of data, for example, on staff and clients. They can also be victims in the sense of incurring enforcement costs and the like. As a consequence of identity theft and related crime, public authorities face enforcement costs and there are also costs for the wider society and economy, including impacts on e-Commerce. Thus the role of public authorities in relation to identity theft takes multiple forms, including the role of secondary victim, source of data and the carrier (or victim).
Problem of Identity Theft

of enforcement costs and other related costs, including costs for e.g. prevention. Examples of public authorities being primary victims have not been identified.

3.2 Drivers of the Identity Theft Problem

As pointed out at the start of this chapter, the key driver of the problem of identity theft is the “motivation” or incitement for criminals to obtain identity information because of the benefits (in particular of financial nature) for them. These benefits are so to say the “other side of the coin” when looking at the costs for victims and are analysed above in the section on the costs of identity-related crimes.

As noted above, research points to that there is a low risk of detection, which is an additional incitement for criminals \(^\text{20}\). Indeed, insufficient or ineffective prevention activities and national responses, as well as cross-border collaboration, make these types of criminal activities easier. In this sense, they are not drivers \(\text{per se}\), but rather weaknesses that make it easier for criminals to commit and get away with this type of crime.

Below the incitement of criminals is considered. National responses are examined in Section 5.

Types of crime for which identity information is used

Identity information is used for a variety of crimes. A non-exhaustive list is as follows:

- Transferring / selling identity information for use for or funding of other criminal activities (e.g. organised crime, terrorism);
- Various frauds (financial fraud, money laundering, social services fraud etc.);
- Human trafficking, smuggling of people, illegal migration;
- Stalking, bullying / harassment / damage reputation;
- Funding of and use for the purpose of other types of criminal activities (e.g. drugs trafficking, terrorism, organised crime)

No readily available data concerning the extent to which identity-related information is used for various types of criminal activities have been identified to date. Some information is, however, available for France, which has introduced identity theft as a specific offence. In 2010, out of 3,572 convictions, 389 were made for ID theft as a single crime, while in 89% of cases identity theft was associated with other crimes. In about half of cases (55.2%) identity theft was associated with

\(^{20}\) http://www.stopidfrauds.com/index.php/home/trends-costs
http://www.swindlecorp.com/risk/
Problem of Identity Theft

traffic-related crimes\textsuperscript{21}, in 9.5% of cases with theft and in 3.2% of cases with infringements to the immigration law.

Below we examine in somewhat further detail in what way identity information is used for various types of crime.

3.2.1 Transferring / selling identity information for use for or funding of other criminal activities (e.g. organised crime, terrorism)

Identity theft is a crime that can be committed by a single person or by a group. When being transferred and sold, identity information is used as a commodity. Often, single offenders with access to the technology can acquire (for an overview of methods used, see Section 3.3) and use the information on their own, or sell it on to others who are able to better exploit the data. The seller and the buyer of identity-related information are involved in the offence, but they do not form a “group” as such. Since offenders may act as a single person and the crime may be committed from anywhere around the world, it is very difficult to classify identity thieves. According to research, many of the currently active groups are operating from Eastern Europe. However, there are no statistics available to underline this fact.\textsuperscript{22}

Once (large) datasets of information have been extracted, identity information can be – and is – sold to those in a position to exploit it, including organised criminal groups, who are specialised in “cashing out”, and/or other types of crime such as money laundering (see below). For many individual criminals, this is the end of the process. One explanation for this provided in the interviews that have been carried out as part of this study is that the degree of sophistication that is needed in order to commit crimes by means of identity information often goes beyond the means of individual offenders. An example of a case where identity information was sold on to crime groups is provided below.

Card fraud mastermind sentenced to three years (October 2011)

- A German electronics engineer who helped criminal gangs to clone credit and debit cards and steal thousands of pounds from members of the public has been sentenced to three years in prison.

- The German electronics engineer was “employed” by organised criminal networks to compromise PIN Entry Devices so that once placed back on a shop counter they recorded all card details and PINs. Organised criminal networks then downloaded this information and used the data to create cloned cards which were then used in several countries where no chip and PIN system is available (e.g. USA).\textsuperscript{23}

In the following paragraphs we look at some of the types of crime for which identity information is used.

\textsuperscript{21}The specific types of traffic-related crimes were not specified.
\textsuperscript{22}http://www.unodc.org/documents/data-and-analysis/tocta/10_Cybercrime.pdf
\textsuperscript{23}http://www.financialfraudaction.org.uk/cms/assets/1/depot%20pcd%20criminal%20criminal%2014%2010%2011.pdf
Problem of Identity Theft

3.2.2 Types of fraud (financial fraud, money laundering, social services fraud etc.)

The importance of the use of identity information for the purpose of fraud is, for example, noticeable through the fact that some countries, such as the UK, refer to the entire phenomenon as “identity fraud” (see also Section 2).

Information obtained via identity theft is, for example, used for the following types of fraud (the list is not exhaustive):

- **Financial fraud** relates to the use of deception to appropriate someone else’s property. Financial fraud may refer to e.g. check fraud, chronic unlawful issuance of bank checks, embezzlement, credit/debit card fraud, forgery, counterfeit instruments such as checks or documents, organised counterfeit check rings, and organised identification theft rings, i.e. also include additional aspects of financial fraud.  

- **Car registration fraud** relates to the falsification of vehicle registrations or other documents in order to receive a driver license, registration document or title certificate through the use of a falsified or stolen ID in a different person’s name.

- **Money laundering** – money laundering refers to a criminal offense including the procedure to conceal the acquisition of illegally obtained money by introducing it into the financial system through commingling with legitimate money and thereby converting the “dirty” money to “clean” money, i.e. making it appear as if the funds were derived from legitimate activities.

While it is clear from the research carried out that identity theft is frequently associated with financial fraud, identity theft is also often related to money laundering as it is commonly used in the process of converting “dirty” money into “clean” money. Money launderers have the incentive to attain the identity of a different person in order to open bank accounts, get credit cards and write cheques in other people’s names, which constitutes a way for criminals to complicate to trace the money trail back to them. Stakeholders consulted as part of the present assignment have confirmed that there is a strong relationship between money laundering and identity theft. More specifically, false identity information is generated or otherwise obtained to facilitate remote transfer to conceal assets. Money laundering crimes also

---

25 http://www.dmv.ny.gov/fraud.htm
26 https://legislation-essentials.lexisnexis.com/webcd/app?action=DocumentDisplay&crystal=1&doctype=cm&docid=1-13-3+Repeal+of+Investment+Companies+13+sm&src=sm&srcid=2A13&key=8735ebe9c6e051 63763489403294c8
27 http://www.aboutidentitytheft.co.uk/identity-theft-money-laundering.html
Problem of Identity Theft

depend on abuses of identity information to avoid or obfuscate measures to counter the activity. 

A study carried out by the UN underlined the relationship between identity-related crimes and money laundering. The study further highlighted that identity or identification elements are important to counter money laundering. Some States indicated that money laundering methods used information, communication and commercial technologies, which provided an instrument for generating false identification documents. This enabled, for example, remote transfers through the use of false identification. These technologies have resulted in a significant expansion of international transfers and offshore banking. However, new technologies have made progresses in crime prevention as well as security.

There is a distinction to be made between the type of ordinary fraud outlined above affecting the private sector and fraud vis-à-vis the public sector, for example, social benefit fraud, which relates to the unjustified claim for social benefits with the purpose of gaining an illegitimate financial benefit from public institutions or authorities. Social benefit fraud is conducted by using falsified identity or supporting documents in order to unlawfully apply for these social benefits.

3.2.3 Illegal migration, smuggling of people and human trafficking

Another area where ID theft crime is often detected is that of crimes linked to illegal immigration (often via large, transnational criminal networks) and smuggling of people. In these cases, false identity documents allow foreign people or illegal immigrants to pass the immigration controls and, lately, to have access to economic resources (such as access to employment by provid ing false documents, and/or to social security benefits).

However, illegal immigration may take place through different forms of identity theft and related crimes. An illegal immigrant may, for example, buy a genuine birth certificate relating to a deceased person of roughly the same age that has previously been stolen by the perpetrator. The illegal immigrant then assumes the new identity and may this way not only enter a country, but also obtain supporting documents such as a driver's license etc. Also, cases have been reported where a child born overseas has been "adopted", while the baby in fact had been stolen and sold and the breeder documents were falsified.

Another way of entering a country illegally is by means of so-called "look-a-like-fraud" (one uses a legitimate passport which is not his/her own, but the picture on it looks similar). In, for example, the Netherlands, it appears to be harder to be allowed to enter the country based on falsified passports, since the detection of

---


29 http://escholarship.org.uk/doc/UNDOC/GEN/W07/805/01/PDF/W0780501.pdf?OpenElement

Falsification is improving. Therefore, the Dutch alien police have noticed an increase of look-a-like-fraud.

Identity theft and the production of false documents are also one of the main crimes related to human trafficking. In this case, identity theft may be used for committing a number of different crimes, including for the purpose of crossing borders (i.e., identity theft is used to get the trafficked persons into a certain country), opening bank accounts and gain access to credits etc. (the latter types of crime are made with the help of identity documentation acquired from trafficked persons). Victims of human trafficking are mainly people in a needy, poor or weak position; especially women and children whose IDs or other identification documents have been taken away by their exploiters. An example from the UK can illustrate this.

**UK – Effects of Identity Theft**

- UK reported the trend of criminals who facilitated the trafficking of individuals from Eastern Europe, confiscated identity documents from these individuals when they arrived in the country and opened bank accounts to gain access to credit through overdrafts, loans and credit/debit cards.

- Furthermore, the accounts were used to obtain tax credits and crisis loans, illegally obtained by the criminals. As a result, debt accumulated on the accounts and was not paid back to the lender. When the lender tried to contact the account holder to demand payment, the organised criminals sent the trafficked individual back to their home country and the lenders lost their money.

In addition, the crime of human trafficking is related to other criminal offenses such as smuggling, corruption, visa fraud and money laundering.

### 3.2.4 Stalking Bullying / Harassment / Damage reputation

The definitions of stalking, bullying, harassment and damage reputation are not exactly mutually exclusive, but overlap to some extent. Whereas there is no internationally valid definition of bullying, the term generally can be defined as the repeated, unreasonable behavior directed towards an individual, or group of individuals, that creates a risk to health and safety. The term bullying may encompass both physical...
Problem of Identity Theft

and psychological violence, i.e. comprises both verbal and physical attacks, as well as more subtle acts like devaluation of a colleague’s work or social isolation.\

With the increasing importance of communication channels and social media (especially social networks) on the Internet, there is a growing prevalence and importance of cyber/digital bullying. Identity theft in the context of bullying and harassment primarily relates to Internet-based activities, as the anonymity on the Internet allows people to bully/harass others without immediately and obviously revealing their identity and therefore might intensify the willingness to engage in bullying/harassing activities. Identity theft is used in the context of stalking in order to cover up the stalkers’ real identity. In particular, this holds true for Internet-based stalking activities.

3.2.5 Identity theft and other types of criminal activities

As pointed out above, identity information may be used for a number of other criminal activities, some of which are outlined below.

There is, for example, a clear link between the transfer / selling of identity information and organised crime. As concerns obtaining and the use of identity information for the purpose of organised crime, the 2010 Report on Organised Crime of Canadian authorities states that:

"Organized crime groups are known to produce, supply or use false identities. The increased availability and ease of access to personal information and business records online makes it easier for criminals to steal information and use it fraudulently. Organized crime uses three main methods of some aspect of their own identity creation of a wholly fictitious identity; or theft of someone else’s identity, either living or dead. These false identities assist organized criminals to avoid detection by law enforcement, particularly when travelling and to protect their assets from confiscation. Individuals also use false identification to carry out or enable criminal activity where evidence of an identity is a key requirement, such as fraud, financial crimes, or people smuggling. Other forms of misrepresentation may also be used, such as false information on company or vehicle identity, consignment, business accounts and transactions."

35 An organised crime group is defined under Art. 2 of the United Nations Palermo Convention against Transnational Organised Crime of 2000 as: "a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit". By 'structured group', it is intended a group that is not randomly formed for the immediate commission of an offence and that does not need to have formally defined roles for its members, continuity of membership, or a developed structure. In turn, 'serious crime' is defined as a conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty. This definition is also applicable in the Member States, since they have signed up to the Convention United Nations Convention against Transnational Organized Crime and the Protocols Thereto (2010), p. 5, available at: http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCbook.pdf
Problem of Identity Theft

While ID theft has a well-recognised offline dimension, linked to the loss or theft of individuals' documents (including ID documents, bank accounts, etc.), according to a report by the United Nations Office on Drugs and Crime the online dimension appears to be more linked to its exploitation by organised crime. The dimension of ID theft related to organised crime was stated to be likely to grow in the future. The apparent correlation between online ID theft and organised crime has led to the classification of this type of crime as a case of cybercrime. The link between online ID theft and organised crime is close for different reasons:

- **The first reason is the increased accessibility of technology for cybercrime (including ID theft), in terms of both price and skills required.** More specifically, software tools can be now easily be purchased online (e.g. software that helps users to locate open ports or overcome password protection). These tools allow a large number of people to become offenders, as sophisticated IT skills are not necessary anymore – at least not to obtain the data (the situation is different when it comes to abusing the identity information). While skilled cyber thieves may not see any advantage in working for organised crime or may not need to do so as they can abuse the data themselves, these tools could allow organised groups to employ large numbers of relatively unskilled individuals to work on their behalf.

- **The second reason is the changing profile of Internet users.** In 2005, the number of Internet users in developing countries surpassed the number in industrialised countries. This implies that, while the number of possible victims will remain substantially unchanged (as they are mostly located in industrialised countries), the number of possible ID thieves will substantially grow. The Internet has made high value victims as accessible as local ones for perpetrators in developing countries.

- **Finally, the higher automation capacity of the new tools allows offenders to easily reach very large numbers of potential victims.** This creates viable criminal strategies that were not profitable only a few years ago due to high failure rates. For instance, despite widespread knowledge of advanced fee fraud and phishing schemes, these are still profitable because the perpetrators only need to have a few marks out of millions tries. In addition, the automation capacity allows cyber-thieves to go undetected, as they can take only a small amount of money from a large number of victims, lowering the chances of detection.

Problem of Identity Theft

Ad-hoc studies⁴⁰ have found out that different types of organised crime groups are involved in identify theft-related crimes in different ways. Traditional organised criminal groups (such as the Japanese Yakuza, Asian triads, Eastern European gangs) use ID crimes to generate funds, via software piracy, plastic card fraud and card skimming. Other organised crime small groups (i.e. Shadowcrew, Theft Services, Mpack) gather with the common objectives to commit ID crime, via underground malware markets, for instance.

On a more general level, as concerns the relationship between organised crime and identity-related crime, the UN study⁴¹ suggested that often situations of organised economic fraud, money laundering and human trafficking occur. These types of crimes are often carried out by organised criminal groups. Furthermore, according to the study, these criminal groups are involved in fabricating highly sophisticated identity documents or deceiving or corrupting authorities to obtain necessary documents, which then could be sold to others for the use in terrorism as well as in other crimes.

Indeed, there is also a ID-related crime can also be linked to terrorism and more in general to ideologically/politically motivated groups that commit identity theft in order to raise funds and launder money to commit other crimes (as in the case of Tariq Al-Daour, a UK Al Qaeda cell)⁴². There is serious concern among law enforcement authorities on the perpetration of ID-related crimes by terrorist groups. Similar to organised crime groups, terrorist groups can also buy stolen or false IDs fabricated by cybercriminals and/or other criminal groups in order to conceal themselves from authorities during travels and during or after the criminal acts.

For example, according to one of the interviewees, terrorists make use of fabricated sophisticated identity documents, exploiting weaknesses in existing structures to obtain documents. These may also be sold on for the purpose of smuggling of migrants. In this regard, it can be pointed out that it is difficult to distinguish between identity-related crime connected to terrorism and identity-related crime associated with organised crime. In case terrorist groups lack expertise as regards the fabrication of false identity documents, they might simply buy these documents from organised criminal groups.⁴³

Furthermore, there is a link between identity theft and corruption. According to the UN Study quoted above⁴⁴, this is primarily a result of the increased sophistication of the identity documentation that is issued, making it more difficult to falsify identity cards, passports etc. As a result, criminals are exploiting various ways of obtaining authentic identity documentation, which includes bribing public officials to either obtain authentic documentation or to falsify information in

Problem of Identity Theft

systems used for the purpose of identification. The latter is assessed by experts to be trend in the future. False or stolen identities may also be used to complicate investigations by criminals that are trying to avoid tracing.

Based on the above analysis, it is clear that identity theft and related crime are a multilevel and multistate phenomenon. Also, identity-related information is used as an enabler for other criminal purposes. It cuts across all forms of crime, but is particularly relevant to public and private sector fraud.

When looking at the importance of identity theft for the purpose of crime, according to the CSFS survey results, the key motivations for criminals are financial fraud and money laundering. Human trafficking and the transfer/selling of identity information are suggested to be slightly less frequent motivations.

Table 3.1: Frequency of use of identity-related information for the purpose of various types of crime

<table>
<thead>
<tr>
<th>Options</th>
<th>Rarely</th>
<th>Very Little</th>
<th>Not very often</th>
<th>Sometimes</th>
<th>Quite often</th>
<th>Very often</th>
<th>Don’t know/no</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transferring(selling)</td>
<td>0</td>
<td>0.0%</td>
<td>3</td>
<td>3.4%</td>
<td>7</td>
<td>7.9%</td>
<td>21</td>
<td>23.6%</td>
</tr>
<tr>
<td>Identity information</td>
<td>4</td>
<td>4.5%</td>
<td>7</td>
<td>7.9%</td>
<td>11</td>
<td>12.4%</td>
<td>9</td>
<td>10.1%</td>
</tr>
<tr>
<td>Human trafficking</td>
<td>3</td>
<td>3.4%</td>
<td>5</td>
<td>5.6%</td>
<td>5</td>
<td>5.6%</td>
<td>16</td>
<td>18.0%</td>
</tr>
<tr>
<td>Money laundering</td>
<td>1</td>
<td>1.1%</td>
<td>2</td>
<td>2.2%</td>
<td>2</td>
<td>2.2%</td>
<td>10</td>
<td>11.2%</td>
</tr>
</tbody>
</table>

Some respondents took the opportunity to also identify further types of crime, including some of those mentioned above, such as terrorism, illegal immigration, “hiding from monitoring while travelling”, as well as bullying and damaging people’s reputation. Drugs trafficking and illegal health care access were also referred to. These types of crimes were all mentioned a number of times.

The findings from the survey are supported by data from France, where identity theft is a specific offence. According to French stakeholders, the majority of ID thefts occur in cases of economic and financial crimes and fraud (e.g. opening bank account and obtaining payment cards using a fake identity, fraud to social security, telecom operators and car rentals). Another area where ID theft crime has been detected is that of crimes linked to illegal immigration (often via large, transnational criminal networks). In these cases, false ID documents allow foreign people or illegal immigrants to pass the immigration controls and, lately, to have access to economic resources (such as access to employment by providing false documents, and/or to social security benefits).

Few cases have been detected of ID theft linked to terrorism. It has to be noted, however, that identity theft is not necessarily a crime that needs to be committed with the help of others. Even when groups exist, they tend to be smaller and less structured than those involved in other forms of organised crime. It is possible that ID-related information acquired from cybercriminals is used by organised criminal groups while
committing other crimes, such as people smuggling. However, there are no reliable statistics on this type of crimes (in relation to ID theft)\(^45\).

**3.3 Identity Theft Methods – Online and Offline**

In this sub-section we examine how and what type of information is obtained through identity theft.

As noted earlier, identity theft can be committed by exploiting weaknesses in identity verification mechanisms or the absence of care with personal details. While there is a lack of clarity concerning the definition of identity theft, it is generally agreed that identity theft can take a number of different forms. In pre-digital times the 'theft' of personal identity could take place by such means as impersonation or the forgery of a signature. However, in the digital age, breaching security measures designed to verify identity by, for example, misappropriating codes, such as PIN numbers, or by acquiring personal information to enable (un)authorised acts serves the same deceitful purpose.

**Methods of obtaining identity information**

A key distinction is usually made between ‘online’ and ‘offline’ identity theft activities:

- **Online ID theft activities** include, for example, botnets, skimming, hacking, phishing and the use of spyware. Information may also be collected from social networking sites. These methods may also be used in a blended fashion.

- **Offline ‘real world’ ID theft activities** involve, for example, theft of identity documentation such as passports\(^46\) or driver’s licenses, collection of identity-related information from ‘dumpster diving’, gathering of information from public records about individuals, by using stolen bank cards or impersonating trusted organisations in emails and/or phone calls etc.

A further distinction can be made between various methods that are being used to obtain identity information, in particular theft of a physical document containing identity information and the acquisition of identity information, either from a physical document or an online source (without necessarily obtaining any physical document). As concerns the first aspect, attempts to obtain identity documentation can, in addition to theft of the document from a victim, take place at different stages of the identity management process\(^47\).

---


\(^{46}\) Passport fraud is when someone fraudulently applies for, uses, or possesses a passport of any nation. This includes using false documentation to gain a new passport, or altering an existing passport to appear as if it had been issued to the person possessing the document.

\(^{47}\) Based on stakeholder interviews carried out as part of the present assignment.
Problem of Identity Theft

Misuse of personal data can occur, for example, when a person claims that his/her passport was stolen and then uses personal information about another person (e.g. collected from social networking sites or through theft of a birth certificate) to illegally obtain an official identity card in that other person’s name. Furthermore, often actors other than governments or government agencies can issue some form of identity document without a legal foundation as far as the proof of identity is concerned. Examples include credit cards with photographs. This facilitates misuse.

In the following sub-sections we first provide descriptions of online and offline methods used to obtain identity information. This is followed by an examination of the prevalence of and trends with regard to the use of the different methods.

3.3.1 Online methods of identity theft

The widespread access to the Internet is one of the main reasons for the rapid evolution of identity theft techniques, which affect individuals as well as businesses and public institutions. In this regard it can be noted that the level of Internet access increased in all Member States between 2006 and 2011, however, the differences remain significant. In 2011, shares of Internet access of 90% and over were recorded in the Netherlands (94%), Luxembourg and Sweden (both 91%) and Denmark (90%), while shares of 50% and below were registered in Bulgaria (45%), Romania (47%) and Greece (50%).

Looking at the EU as a whole, in 2011 76% of the EU population had used the Internet at least once. This was 2%-points higher than in 2010. The percentage of people in the EU who have never used the Internet decreased continuously in recent years; a figure of 24% was recorded in 2011 compared to just below 45% in 2005.

Figure 3.3: Proportion of individuals who have never used the Internet

---

Problem of Identity Theft

A regular use of the Internet by individuals (i.e. use of the Internet every day or almost every day) increased to a proportion of 56.1% of the population in 2011, as illustrated in the following figure.

Figure 3.4: Internet use as a proportion of the population by usage frequency

The more households and companies have access to the Internet and the more online activities are used, the greater the potential risk of becoming a victim of identity-related crime. This is the case, because people provide ever more identity data online for personal reasons (e.g. on social networking sites), to conduct business or deal with public authorities and the recipients store large amounts of identity data. For example, online banking, e-Commerce and e-Government services (e.g. tax declarations) require a person to provide certain types of personal data — such as card number, the card’s security number, address and in the case of e-Government tax forms — the breakdown of persons or a household income. This data is very useful to fraudsters, and such websites are therefore frequently targeted and sensitive data is obtained by phishing.

Indeed, according to CIFAS (UK) one reason for the increase of identity theft is the availability to fraudsters of large quantities of personal details. Some of this data will have entered the criminal domain through staff fraud. However, the majority are likely to be as a result of the compromise of personal data over the Internet. CIFAS has also pointed out that the greater risk of identity fraud appears in those UK locations where the fraudsters are e-enabled and there is a wide access to the Internet. Another factor is that in many cases businesses and public authorities share (some of) the data they have collected, which may increase vulnerability to data theft during the transfer process, and because the same information exists in more than one location simultaneously.

Problem of Identity Theft

In terms of the types of online / digital methods that are used to obtain personal identity information, examples are provided below:

Examples of Online Methods used to obtain Personal Identity Information

- **Skimming** refers to the process where an identity thief copies the details from the victim's credit or debit card by using the front of a bank machine. In the front of the bank machine the perpetrator may e.g. place a false panel with a small webcam or digital camera and a magnetic card reader (the so-called skimmer). Thus the identity thief scans the details from the magnetic strip of the card as well as the Personal Identification Number (PIN).

- **Hacking** is a method where unauthorised individuals gain access to a computer located somewhere else using the Internet as a means of access. To do so they introduce lines of code by email or use specific programs, so-called spyware (see next explanation). The purpose of hacking is to cause damage or mischief or to steal information, such as identity data and banking details.

- **Phishing** describes the practice of sending emails on behalf of existing institutions and companies and request details relating to the victim's identity, bank accounts as well as details of credit and debit cards and other financial contracts. There are three different methods of phishing which are pharming, smishing and vishing. Phishing refers to the act of redirecting a user from an authentic webpage to a fraudulent site that replicate the original. Smishing occurs when cell phone users receive a confirmation message for signing up for e.g one of its dating services. The users are told to be charged a certain amount unless they decide to cancel the order. It happens that the operators of the website compromise and steal personal information. The last method is vishing which refers to act of receiving a spoofed email from a legitimate looking institution. The phisher invites the customer to call a telephone number. In the course of the call, the customer is requested to reveal personal data (e.g. account number) for "security verification reasons". In this way, the phisher can obtain personal information for identity theft purposes.

- **Spyware** stands for small programmes or viruses that can pass information out over the Internet without detection (these programmes are also known as "Trojans"). With *Trojans* - many people who have been the victim of computer hackers have only discovered the problem afterwards. Thus spyware is an instrument for identity theft. It can be downloaded without the victim's knowledge and can be stored on the computer's hardware drive for collecting all kinds of data. Furthermore, they permit to open up channels ("ports") to send and receive also specific (identity) information.

- A computer *virus* is a type of malware that propagates by inserting a copy of itself into and becoming part of another programme. Viruses are spread from one computer to another when the software or document they are attached to is transferred from one computer to another using a network, a disk, file sharing or infected e-mail attachments, leaving infections as they "travel". Viruses can range in severity from causing mildly annoying effects to damaging data or software and causing denial-of-service conditions. Almost all viruses are attached to an executable file. This means that the virus may exist on a system without being active or able to spread until a user runs or opens the malicious host file or programme. Once the host code has been executed, the viral code is executed as well. Normally, the host programme keeps functioning after it is infected by the virus. However, some viruses overwrite other
Problem of Identity Theft

A computer **worm** is a “program that propagates itself over a network, reproducing itself as it goes”. Worms are distinct to viruses, which refer to a programme fragment that inserts itself into other programmes. Because of the recursive structure of this propagation, worms spread extremely fast and pose a big threat to the Internet infrastructure as a whole; modern worms are capable of gaining control over a substantial portion of the Internet hosts within several minutes. Worms are also e.g. capable of stealing sensitive information from servers or directly from desktops.

It can be noted that viruses, Trojans, worms and bots are all part of a class of software called **malware**. Malware is code or software that is designed to damage, disrupt, steal, or in general inflict some other “bad” or illegitimate action on data, hosts, or networks. There are a variety of classes of malware that have different ways of infecting systems and propagating themselves, e.g. by being bundled with other programmes or attached as macros to files.

Other types of malware are installed by exploiting a known vulnerability in an operating system (OS), network device or other software, e.g. a hole in a browser that requires users to visit a website to infect their computers. The vast majority, however, are installed by some action by a user, e.g. by clicking on an e-mail attachment or downloading a file from the Internet. Damage by malware varies from “minor irritation” (e.g. browser popup ads), to stealing confidential information or money, destroying data, and compromising and/or entirely disabling systems and networks. While malware cannot damage the physical hardware of systems and network equipment, it can damage the data and software residing on the equipment.

A quite recent method to obtain data is the use of wireless data transmission (Bluetooth, WLAN, RFID), which can lead to so called ‘wireless identity theft’. This involves a rather new technique of gathering an individual's personal information from RF-enabled cards carried on a person in their access control (e.g. credit, debit, or ID cards). Each of these cards carries a radio frequency identification chip, which

---


54 Internet bots are software applications that are used on the Internet for both legitimate as well as malicious purposes. Bots can e.g. be used as agents for mass identity theft (through phishing or pretending to be a legitimate company in order to convince the user to submit personal information and passwords). A variety of bots are used for malicious purposes. **Spam Bots** spider the Internet with the purpose of collecting data from forms that have been filled out online, spreading advertisements and pop-ups throughout the Internet, and collecting email addresses for the purpose of spamming. **Hacker Bots** are used by hackers to find vulnerabilities in websites and online applications. They can be exploited for malicious purposes. **Botnets** are networks that hackers set up online by using “zombie” computers, i.e. computers that have been taken over by the hacker without the knowledge of the owner, to perform malicious acts, e.g. denial of service attacks. **Download Bots** are bots that are used to forcibly download a webpage that the hacker wants the surfer to see instead of the page that was requested by the surfer. Sources: [http://www.spambusiness.com/how-internet-bots-are-used.html](http://www.spambusiness.com/how-internet-bots-are-used.html) and [http://www.tech-faq.com/botnet.html](http://www.tech-faq.com/botnet.html)

55 Malware or malicious code (malcode) is short for malicious software.

Problem of Identity Theft

responds to certain radio frequencies. When these responses come into contact with radio waves, they respond with a slightly altered signal. The response can contain encoded personal identifying information, including the card holder’s personal data (name, address, insurance number etc.). Upon capturing this data, the thief is then able to programme their own cards to respond in an identical way.58

Individuals may also access other persons’ identity in an online environment without obtaining access to login details, for example, to post information in the name of others on social networking sites. Such access may be possible where individuals have forgotten to log out of their account, either on a personal or public computer, making it possible for others to access their account. Some information on the situation concerning the use of other persons’ identity online is available from Sweden. While information is not available concerning the way in which the other persons’ account has been accessed (i.e. via access to login details or not), it is likely that many of the cases are caused by individuals forgetting or neglecting to log out.

Sweden – Online Identity Theft via Social Networking

- In a Swedish Report from 2011, published by the Data Inspection Board59, in which the results of a regular survey concerning young people’s views on data protection and privacy in general and online, it was first of all noted that compared to the previous three similar surveys that have been carried out (2009, 2008 and 2007), more and more young people have access to their own computer.
- This results in that parents have less control over what information their children share with others, and increases the responsibility of the young people themselves. As much as 92% of the 522 young people aged 15 to 18 are members of Facebook and of these, half indicated that they have been subject to “Facerape”, which means that someone accesses your Facebook account and writes posts on Facebook in your name.

No similar figures for other EU Member States were identified by the research.

Also different features and applications might allow strangers to access information. On certain sites, such as Facebook, users are encouraged to provide their profiles with free online games that can be played with other members. However, what most general users do not realise is that adding an application is like adding a friend, and the creator of that application gains full access to the entire information a person reveals about him/herself in the profile. Furthermore, the uses that social networking sites make of personal data (addresses, telephone numbers and other information concerning their everyday life), even if seeming harmless, could nevertheless be used for the purposes of identity theft.60

58 http://w2.eff.org/Privacy/RFID/rfid_position_statement.php
60 http://www.identitytheft.com/article/social_networking
Problem of Identity Theft

The risk behaviour of individuals is further explored in Section 3.5. To illustrate current problems, two cases of identity theft where phishing was used are provided below. Further examples of cases where other methods are used are provided in the appendices.

<table>
<thead>
<tr>
<th>Case 1: Phishing scam targeting customers</th>
</tr>
</thead>
<tbody>
<tr>
<td>• In 2004, eBay investigated a series of phishing scams originating in Europe in collaboration with the US Secret Service. More than 100 people were arrested in the course of the investigation by national authorities. One individual was convicted for stealing nearly $500,000 through phishing. This particular individual had circulated e-mail messages that appeared to come from eBay to people who were unsuccessful auction bidders, advising them of similar merchandise for sale at even better prices. To purchase the goods, the message recipients were told to supply personal information such as bank account numbers, credit card numbers and passwords and then to transfer money to an escrow site.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Case 2: Phishing scam targeting businesses</th>
</tr>
</thead>
<tbody>
<tr>
<td>• The phishing in question targeted businesses and scam started with an email from the businesses' respective banks. One victim said that it “looked absolutely genuine. It came from my bank and said that there had been some unfamiliar activity on my account. I had been using my card quite a bit and so it seemed reasonable to me that they were checking up.” The business in question assumed that the email was legitimate. “It had my bank's logo and looked completely genuine.” The email requested recipients to click on a link and to enter their personal details. Furthermore, the email stated that the bank card in question may be suspended if account activity was not confirmed. “They put in a note of fear so that you feel that it's urgent for you to act. To be honest I just wanted to get my account sorted out so I didn’t really stop and think.”</td>
</tr>
</tbody>
</table>

• The link lead to a legitimate-looking website where the information requested in the email could be entered. This provided fraudsters with sufficient information to access businesses’ bank accounts. In the case described above the fraudsters withdrew over £1,000 from the bank account. Once the business in question noticed the transaction, it contacted its bank and reported the scam. The bank refunded the money and advised the business to change its password as well as to report the scam to one of the main credit agencies in order to secure his credit rating. Reporting the security breach to a credit agency the business discovered that the scammers had already applied for a new credit card under his identity. There is now a note against its name saying that he is prone to identity theft.

---

62 [http://www.aboutidentitytheft.co.uk/ikell-for-phising-scam.html](http://www.aboutidentitytheft.co.uk/ikell-for-phising-scam.html)
Problem of Identity Theft

3.3.2 Offline Theft of Information

Turning to identity theft in an offline environment, only scarce information has been identified by the research.

With regard to the theft of identification documents, around 300,000 identity-related documents are estimated to be lost yearly in the Netherlands and only around 10% of the documents are retrieved. It is not clear from the available figures whether the “loss” is a result of theft or simply misplacing the identity document, however, it is likely that some of these identity documents are stolen. A related problem is the falsification of identity documents. According to data provided in the ‘Coopération Policière’ report, since 2006, there have been about 14,000 cases of false administrative documents registered in France, mainly concerning false identity documents.

Other cases are reported by the Police aux Frontières. According to these data, 2,774 cases of use of false national ID documents were detected in 2011, and 3,278 of use of false passports; a trend increasing with respect to the previous years. Furthermore, the Préfecture reported 2,290 attempts of obtaining false national IDs and 914 of false passports. More generally, according to data gathered by the Police aux Frontières, the number of reports of people using at least two identities at the same time has grown of about 109.9% from 2005 to 2010, i.e. 52,761 more cases in five years. The gendarmes detected 19,568 false identities or aliases thanks to the digital fingerprint repository (Fichier Automatisé des empreintes digitales – FAED) in 2011 and 31,668 in 2011. Using the same tool, the police detected 81,189 cases in 2010 and 89,906 in 2011. Similar types of data have been identified for Germany, however, the figures are much lower.

Table 3.3: Germany – Abuse of identity documentation

<table>
<thead>
<tr>
<th>Offense</th>
<th>2011</th>
<th>2010</th>
<th>Growth rate (absolute)</th>
<th>Growth rate (in %)</th>
<th>Detection rate (in % 2011)</th>
<th>Detection rate (in % 2010)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Altering official identification</td>
<td>553</td>
<td>593</td>
<td>50</td>
<td>9.9</td>
<td>95.4</td>
<td>97.0</td>
</tr>
<tr>
<td>Preparation of altering official identification</td>
<td>31</td>
<td>32</td>
<td>-1</td>
<td>-1.7</td>
<td>92.1</td>
<td>96.6</td>
</tr>
<tr>
<td>Procurement of false official identification</td>
<td>1,513</td>
<td>1,596</td>
<td>80</td>
<td>5.1</td>
<td>95.6</td>
<td>95.6</td>
</tr>
<tr>
<td>Abuse of official identification</td>
<td>5,923</td>
<td>5,313</td>
<td>80</td>
<td>11.5</td>
<td>94.8</td>
<td>94.5</td>
</tr>
</tbody>
</table>

63 Scale of Identity Fraud and social damage in the Netherlands, PWG, July 2011.
64 Further information on what the documents were used for is not available. Information is also not available as to whether the fake documents relied on other “real life” persons’ identities or if they were fictitious identities.
65 Source: Polizeiliche Kriminalstatistik 2011, p. 52.
http://www.bmi.bund.de/SharedDocs/Downloads/DE/Pressemitteilungen/2012/_PK52011.pdf?__blob=publicationFile
Problem of Identity Theft

Similar data is, however, not available in all countries.

For example, there is no consolidated data concerning the number of identity documents stolen each year in Italy. Based on a media review, our research however suggests that thefts in Italy mainly concern blank documents, i.e. originals in blank stolen from municipalities and other authorities’ offices, which eventually are filled in and sold. These documents can be sold at more than 1,000 euros each. Furthermore, from newspapers, it emerges that organised crime is behind this type of crime (at least in the majority of cases, and especially in large scale thefts). In terms of figures, estimates emerging from aggregating the information found on newspapers are of at least a few thousands (15-20,000) per type (ID card, passport, driving licence). However, caution needs to be exercised with regard to these estimates. It can be noted that it is not clear from the sources whether the identity documents were completed with fictitious or existing identities and as a consequence it is also uncertain whether there are any primary victims in these cases.

Figures on the theft of post have been identified for Northern Ireland and Germany and are shown below:

Table 3.4: Northern Ireland - Theft of mail (recorded theft by offence)\(^66\)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Cases</td>
<td>21</td>
<td>22</td>
<td>22</td>
<td>96</td>
<td>96</td>
<td>84</td>
<td>61</td>
</tr>
</tbody>
</table>

In Germany, there were 1,702 and 1,949 recorded violations of the privacy of correspondence, postal and telecommunications in 2010 and 2009 respectively\(^67\). Thus, there seems to be a downward trend in both Germany and Northern Ireland, However, not enough data is available to draw any clear conclusions.

Examples of methods used to acquire identity information in the “offline world” are provided below. The list is not exhaustive.

Problem of Identity Theft

Examples of Methods used to obtain Identity Information in an Offline Environment

- **Theft of physical documents**, which refers to the act of fraudulently obtaining various types of documents that contain identity information about a specific person or institutions (e.g. theft of passports and other identity documentation as well as breeder documents, post theft, theft of business records and records of public institutions etc.). For example, business record theft implies that someone steals data from a business or bribes insiders to obtain specific information from the business concerned. Naturally, this type of theft can also affect public institutions.

- **Dumpster diving** also belongs to the offline methods that are used by offenders to obtain information for identity theft purposes. It refers to the act where fraudsters go through bins/garbage in order to find copies of individual’s cheques, credit card or bank statements or other documents containing personal information.

- **Shoulder surfing** describes the action of looking over someone’s shoulder or from a location nearby while a person e.g. enters a PIN at an ATM.

- Another method to obtain information for identity theft purposes is to **compromise PIN Entry Devices** in order to record all card details and PINs once they are placed back on a shop counter. The relevant information is then downloaded and the data used to create cloned cards.

- **Pretexting** refers to acts in which fraudsters impersonating a legitimate customer and contact a financial institution or telephone company in order to request account details of a customer. Pretexting can also refer to actions carried out by insider of financial institutions.

In addition to the methods identified above, identity documentation is also forged by criminals. However, the research suggests that given the increased security features of identity cards and passports, criminal activities have been switching from forging the identity documents to forging the administrative documents or breeder documents that have to be submitted to obtain identity cards and/or passports. Breeder documents are an important part of the identity chain. Due to the fact that most breeder documents are less secure, it is easy for criminals to exploit the loopholes in the present identity process.

---

68 Ibid.
69 Rand Report 2011
70 Ibid.
71 Ibid.
72 A breeder document is defined as an ID document issued to support one’s identity and used to obtain another document or privilege. One of the most important breeder documents is a birth certificate. But also driver’s licenses may function as a breeder document to obtain certain privileges, such as legitimately acquiring alcohol, while in fact the individuals are underage. Breeder Documents, the key to identity, J. Mercer,Keeping Journal of Documents & Identity, issue 29, 2009.
3.3.3 Prevalence of online and offline identity theft and trends

According to the responses to the CSES survey, malware is the most common method used offenders use to obtain information for identity theft purposes (62.9% of survey respondents said that this was either very common or quite common). This is followed by phishing (59.6%), the abuse of information freely available online (53.9%) and other methods such as hacking into a database (47.2%). Reflecting overall patterns, offline methods of obtaining information are far less common.

The following chart provides an indication of trends with the most common methods of obtaining information for identity theft purposes also being the ones that are experiencing the most pronounced upward trends. The chart shows the percentage of survey respondents saying that different methods are increasing as opposed to remaining the same or decreasing in frequency of use.

Figure 3.5: What are the trends in relation to the methods used by offenders to obtain information for identity theft purposes?

<table>
<thead>
<tr>
<th>Method</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware/virus/other snooping software</td>
<td>62.9</td>
</tr>
<tr>
<td>Phishing</td>
<td>59.6</td>
</tr>
<tr>
<td>Abuse of information freely available online</td>
<td>53.9</td>
</tr>
<tr>
<td>Hacking into a database, etc.</td>
<td>47.2</td>
</tr>
<tr>
<td>Interception of email</td>
<td>41.6</td>
</tr>
<tr>
<td>Skimming</td>
<td>33.7</td>
</tr>
<tr>
<td>Abuse of legitimate access to data</td>
<td>19.1</td>
</tr>
<tr>
<td>Theft of post</td>
<td>9.0</td>
</tr>
<tr>
<td>Going through bins / rubbish</td>
<td>4.5</td>
</tr>
</tbody>
</table>

It can be seen that while the first methods are used in an online environment, especially the two last methods to acquire data are offline methods. While these two last types of methods are more likely to be used in a national context, there is a strong transnational element to the first methods, which may be used independently of the location of the perpetrator.

Available information on the number of cases of identity theft supports the results of the online survey. More specifically, while research from previous years point out phishing to be the most frequently used method for identity theft, the cases where phishing is used is thought to have decreased in 2011 (no figures are, however,
### Problem of Identity Theft

available). Instead, there is an increase in the use of viruses, such as Trojan horses, and other malware. As concerns the trends with regard to malware, a UK source reported the following:

- During the first half of 2011, 1,245,403 new computer malware programmes were identified, which was 15.7% more than in the previous six months. The average number of new malware programmes per day was 6,881.
- Among the different malware categories, Trojan horses and adware recorded an above average increase. The number of backdoors and downloaders declined slightly.
- In the first half of 2011 there were a total of 2,670 active malware families.
- The share of Windows malware increased to 99.6%. Classic Windows programme files decreased by 0.3%, but an increase in .NET programmes compensated for this loss.
- Malware programmes active on websites and malware for mobile devices showed an upward trend.

While it is not clear from the source to what extent these attacks relate to identity theft, the increasing trend in malware can be assumed to also result in an increasing trend in identity theft carried out by such means.

The downward trend of phishing is confirmed in other sources that consider the problem of phishing worldwide. For example, in the second half of 2011 there were at least 83,083 unique phishing attacks worldwide in 200 top-level domains. This is less than the 112,472 attacks that were observed in the first half of 2011. The decrease was explained as being due in part to a decrease in phishing attacks that leveraged shared virtual servers to compromise multiple domains at once. Another US source estimated that in 2011, the number of phishing attacks decreased by 2%.

Some data on the use of phishing and other methods are available from national sources. For example, of the 6,800 cases of digital (online) identity fraud recorded by the German Criminal Police Office in 2009, most cases occurred when using accounts

---

73 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht_2011.pdf?_blob=publicationFile
75 Adware are programmes that hijack computers for profit, normally hidden inside so-called "free" downloads and pop-up ads that forcibly install software on systems with improper security configurations. http://antivirus.about.com/od/spywareandadware/a/adware.htm
76 A backdoor is a secret or undocumented means of accessing a computer system. Many programmes have backdoors that have been placed by the programmer in order to allow them to gain access to troubleshoot or change the programme. Some backdoors are, however, placed by hackers once they gain access to get easier access next time or in case their original entrance is discovered. http://netsecurity.about.com/cs/generalsecurity/g/def_backdoor.htm
Problem of Identity Theft

of telecommunication services abusively (over 3,000 cases), followed by phishing in the context of online banking (over 2,920 cases). In the case of phishing, it can be noted that the number of cases (still) increased by 64% compared to 2008. An overview is provided in the following table.

Table 3.5: Extract - cases of cybercrime in Germany (2009 and 2010)

<table>
<thead>
<tr>
<th>Type of offence</th>
<th>2009</th>
<th>2010</th>
<th>Change (in %)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online fraud</td>
<td>22,963</td>
<td>27,292</td>
<td>+18.9%</td>
</tr>
<tr>
<td>Phishing</td>
<td>11,491</td>
<td>15,190</td>
<td>+32.2%</td>
</tr>
<tr>
<td>Phishing in the context of online banking</td>
<td>2,923</td>
<td>5,331</td>
<td>+82.4%</td>
</tr>
<tr>
<td>Cybercrime</td>
<td>50,254</td>
<td>59,839</td>
<td>+19.1%</td>
</tr>
</tbody>
</table>

According to the Federal Criminal Police Office these figures should, however, be viewed with caution as there is a significant under-reporting since many victims do not realise or at least do not report that identity theft has taken place. In 2010, the Police Office estimated it was aware of only 40% of all cases.

Hacking and interception also seem to be on the rise. According to CIFAS, this is part of an overall trend of an increased number of cases where the fraudster gains access (e.g. through computer hacking, interception of post details, social engineering through popular websites etc.) to another person’s account details and takes over the account. This type of fraud increased by 18% during 2011, which means that the two data driven frauds (identity fraud and account takeover combined) now account for over 58% of all fraud identified (online and offline). Furthermore, the number of victims of both types of fraud has – when combined – risen by 10% from the levels in 2010; underlining the very real cost of these crimes.

Skimming, on the other hand, seems to be decreasing. According to European ATM Statistics, in 2011 the incidences of card skimming fell by 26% to the lowest level since 2008. Overall, losses due to ATM related fraud attacks were estimated to have fallen by 13% from 268 million euro to 234 million euro. This fall was stated to be driven by a continued reduction in losses due to card skimming attacks, which fell 13% from 267 million euro to 232 million euro. The majority (79%) of the ATM related card skimming losses were further indicated to continue to be international (losses outside national borders by criminals using stolen card details) with most cases occurring in countries outside of Europe. The top three locations for such losses were indicated to be the USA, the Dominican Republic and Colombia. In the interviews carried out by us, it was explained that this reduction is in part due to the increased use of chips on credit card transactions.
cards as well as the use of mobile card readers, implying that the card is read at the table in restaurants rather than being taken away from the sight of the customer.

In terms of insider abuse of Internet access or e-mail, this threat includes two separate “threat vectors”: (i) threats posed by malicious employees; and (ii) threats due to employees who have made some kind of unintentional blunder. Figures have only been identified for the US, which suggest a ratio of 60:40.

As concerns the abuse of freely available information, the issues of malpractices and abuse of Internet have been rather constantly increasing the last decades. The rapid increase in particular in the last years is e.g. due to the increasing use of social networking sites such as Facebook, where users post information about themselves online.

An Italian study confirms that different types of identity theft are developing differently. The study found evidence of an overall slight decrease of identity theft incidences: from 26% in 2008 to 22% of the sample interviewed in 2009. Identity theft as a consequence of lost or theft of identification documents and/or credit cards remained the most common case. Lost or stolen documents and credit cards are eventually used to purchase goods, subscribe contracts, etc. (a decrease from 53.5% in 2008 to 40.2% in 2009 was registered). On the contrary, a slight increase was reported for cases of credit cards cloning (25.7% in 2009). Some decrease was also reported for cases of trashing and phishing cases.

3.4 Types of Identity Theft Information and Victims

In this section we examine further aspects of the problem, namely the types of information and victims targeted for the purpose of identity theft and identity theft related crime.

3.4.1 Types of information targeted for identity theft

Turning to the types of information that are targeted most for identify theft, the following chart suggests that the name of the victim, bank details and security details for operating online services (login name, password, etc.) are most frequently targeted. It should be noted that the chart shows the proportion of respondents indicating that the various types of data are targeted ‘quite’ or ‘very’ often.

---

85 http://www.ipedr.com/vol33/010-3CLMC2012-100023.pdf
86 It has been estimated that there were around 170 million Facebook users in the EU in 2012. An overview table of users by Member State is provided in Appendix 1. http://www.internetworldstats.com/stats5.htm
Problem of Identity Theft

Figure 3.6: In your experience, what types of data are targeted most often for the purpose of identity-related crime?

Furthermore, some respondents (7 of 89) mentioned other additional types of data, which were not at choice, such as the following:

- Online identity in online games;
- Driving licences;
- Function / professional status;
- Potential secret questions for logins;
- Document’s validity;
- Medical records.

According to the respondents to the CSES survey, the types of data that can lead to the worst consequences for the victims are bank details/financial information, name and login details (i.e. login name and password). This is followed by passport numbers, PIN numbers, birth details and aliases.

Based on the survey results, there seems to be a clear overlap between the types of data that are most frequently targeted and that those that are identified as leading to the worst consequences for victims. In this regard, it may, however, be pointed out that some types of data may not be particularly targeted or risky on their own, but a name in combination with e.g. a PIN number or password may lead to very negative
Problem of Identity Theft

Consequences if they end up with criminals. The use of these various types of data for the purpose of different crimes is further explored in Section 3.5.

3.4.2 Types of victim groups affected (targets)

As noted earlier, identity theft causes harm to the individual whose identity information is wrongfully used (the primary victim) and can also involve the misuse of identity information by defrauding or damaging another party such as a bank or retailer (the secondary victim). Identity theft affects different types of victims within overall target primary victim group. According to the survey:

<table>
<thead>
<tr>
<th>Characteristics of Identity Theft Victims</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Gender</strong> - the majority of the survey respondents say that men and women are equally targeted (44%), while 9% indicated that men are more targeted than women, and 7% stated that women are more targeted than men. Around 40% of the respondents stated that they don’t know.</td>
</tr>
<tr>
<td><strong>Age groups</strong> - opinions are more divided with roughly similar proportions of respondents saying that younger people are targeted most (19%) rather than the reverse (20%) and 33% saying the age groups are equally affected.</td>
</tr>
<tr>
<td><strong>Affluence</strong> – close to a third of survey respondents (29%) argue that the wealthy and less wealthy are targeted to the same extent. Sixteen percent stated that wealthy are more targeted than less wealthy and 8% indicated the reverse. A high proportion (40%) said that they do not know.</td>
</tr>
<tr>
<td><strong>Business</strong> – there is a similar pattern with business – 32% of survey respondents say that large and small firms are affected equally by identity theft, 13% that large businesses are targeted more than small ones and 10% that small businesses are the main target. Close to half of the respondents (45%) indicated that they don’t know.</td>
</tr>
<tr>
<td><strong>Countries</strong> – approaching a quarter of survey respondents (24%) said that people or businesses in particular countries are targeted more than in other countries while 15% said this was not the case and the rest did not know.</td>
</tr>
</tbody>
</table>

Overall, it can be concluded that identity theft is mainly associated with online types of information rather than theft of physical documents or information from physical documents “offline”. In terms of the methods used, malware seems to be particularly important and on the rise. Phishing is also one of the mostly used methods, although recent trends have been decreasing. The types of information most frequently targeted are the name of the victim, bank details and security details for operating online services (login name, password, etc.). Younger people seem to be targeted slightly more than older people (possibly because of more frequent use of the Internet).
3.5 **Cross-border Dimension of the Problem**

The cross-border dimension of identity theft involves the following types of cases:

- **Situations where the perpetrator is “based” in one country and the victim in another.** As concerns the place where the perpetrator is based, in the online context situations may also occur where the perpetrator him/herself is based in one country and the server is located in another country;

- **A criminal acquires information and then transfers it on/sells it to a second criminal.** One or both of these criminals may be “based” (see comment above) in another country than the victim;

- **A criminal acquires information in one country and uses it in a second country,** e.g. by stealing identification papers in Portugal and using them in France.

These are of course only examples - the cross-border dimension can take on many other forms. The United Nations Office on Drugs and Crime (UNODC) carried out a threat assessment of transnational organised crime in 2010, which also included identity theft. According to this analysis, which considers identity theft as a type of cybercrime, the dimension of the phenomenon is not negligible, even though accurate estimates are not possible, and there is a clear cross-border dimension to the problem. The following figure provides an illustration of the results of the UNODC’s threat assessment of ID theft.

The figure shows the flows of crimes related to ID theft and involving organised crime. As is shown in the figure, flows from developing and emerging countries (South America, Africa, and South-East Asia) primarily target Western countries (US and Europe). It is not clear from the source whether the flows refer to the acquisition of identity data and / or the secondary crime.
Problem of Identity Theft

Figure 3.7: UNODC threat assessment of ID theft


Also according to the survey results, identity theft is seen as having a strong European/cross-border dimension. Indeed, only one of the 89 respondents who answered this question indicated that there is no cross-border dimension to the problem, while as much as 68.5% of the respondents considered that there is a quite significant or very significant cross-border dimension. Out of 89 respondents in total, close to a quarter did not give an answer.
Table 3.6: Do you consider that identity theft has a significant European / cross-border dimension

<table>
<thead>
<tr>
<th>Options</th>
<th>Nº</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>No cross-border dimension</td>
<td>1</td>
<td>1.1</td>
</tr>
<tr>
<td>Very little cross-border dimension</td>
<td>6</td>
<td>6.7</td>
</tr>
<tr>
<td>Quite significant cross-border dimension</td>
<td>23</td>
<td>25.8</td>
</tr>
<tr>
<td>Very significant cross-border dimension</td>
<td>38</td>
<td>42.7</td>
</tr>
<tr>
<td>Don’t know/ no opinion</td>
<td>21</td>
<td>23.6</td>
</tr>
<tr>
<td>Total</td>
<td>89</td>
<td>100.0</td>
</tr>
</tbody>
</table>

To substantiate these results, according to the survey one third of the cases can be estimated to involve either two or three EU27 Member States with a significantly higher proportion – just over half of cases – involving countries outside Europe. Some examples of cross-border cases are provided below.

Examples of Cross-border Cases

- The people behind the online enterprise Confidential Access (CA) sold fake IDs, documents and tips on how to commit fraud to their clients. CA’s leaders ran it from Alicante, Spain, while UK employees monitored the website and produced false documents. Many of CA’s documents looked very authentic. They were bundled together and sold as full credit profiles, including wage slips, credit history print-outs and a postal address. This enabled CA to defraud companies of thousands of pounds. According to the police, the persons involved in carrying out the crimes were already brought or will be brought to court/justice.

- A 21-year-old Dutch citizen has been charged with allegedly selling credit card numbers collected from Boeing’s employee credit union and “… stealing card numbers from other illegal online data markets”. The citizen, who went by the online nickname “Fortezza”, was extradited from Romania to the United States in March, according to the U.S. Department of Justice. Prosecutors allege that the citizen trafficked upwards of 44,000 credit card numbers, which caused millions of dollars in damages.

Another example provided by French stakeholders refer to cases when the identity theft is done via ID cards/passports. Cases occur, where one person applies for documents in a French consular office abroad, while another person has already obtained by a prefecture a document using the same identity. In this regard, it can be noted that a disproportionate number of perpetrators were, in the survey, indicated to be “based in” and the proceeds of identity theft go to countries mainly outside of the EU.

88 http://www.bbc.co.uk/news/uk-england-18377246
89 It is not specified in the article where the Boeing’s employee unit is located
91 It can be noted that it is not clear from the survey responses whether perpetrators being “based” in a certain country is interpreted as meaning that the perpetrators are physically based in a certain country or
Problem of Identity Theft

although a few EU Member States were mentioned by the respondents. These were Romania, Spain, UK, France, Italy and Poland. In addition, some respondents simply referred to 'the region of Eastern Europe'.

The following figures provide an overview of countries and regions where survey respondents indicated that perpetrators are most frequently based. It can be noted that some countries within the wider regions / continents (e.g. in Eastern Europe and Africa) have been pointed out specifically by some respondents, while other respondents did not refer to specific countries but only the wider regions / continents. The first figure shows the spread across regions / continents, while the following figure includes the exact references as they were made by the respondents, and thus refer to both countries and regions.

**Figure 3.8: Regions / Continents where perpetrators are based**

![Regions / Continents where perpetrators are based](image)

**Figure 3.9: Countries and regions where perpetrators are based**

![Countries and regions where perpetrators are based](image)

if certain countries were pointed out because servers are located here. The answers may therefore refer to both situations.
Problem of Identity Theft

To conclude, based on the analysis in this and the previous section, it can be said that there is a clear transnational dimension to the crimes that have been examined. Several of the crimes, such as smuggling of people and illegal migration, are inherently transnational. There is also a strong transnational component in money laundering. On the other hand, stalking, bullying and harassment are either carried out within individual countries, although this may not always be the case. Damage reputation may be a direct aim, but also a result of the acquisition of identity information e.g. from companies. Fraud may or may not have international elements. In many cases, as can be seen from the above figures, the problem is not restricted to the EU, but non-EU countries are also involved.

3.6 Conclusions – Problem of Identity Theft

As this section has shown, identity theft has multiple causes and manifestations with effects on both primary and secondary victims. While it can be concluded that the problem per se has trans-national aspects which cannot be dealt with satisfactorily through action by the Member States (see Section 5) and that the scale of the problem is significant (see Section 4), based on the problems identified in this section, common action seems important to:

• Reduce identity theft and related crime;
• Improve the capacity to prevent and tackle identity theft and related crime both in the public and private sectors, including in relation to cross-border aspects of the problem, at national and EU level.
• Ensure that primary and secondary victims of identity-related crime obtain support and redress.
• More generally, to safeguard fundamental rights, including in particular: the right to liberty and security (Art. 6); respect for private and family life (Art. 7) and protection of personal data (Art. 8); right to property (Art. 17); and to protect consumers (Art. 38), whose identity information may be acquired and abused in relation to online shopping, as well as shopping in the offline world and thus have a negative impact on consumer protection. This is also a fundamental right; and the right to an effective remedy and to a fair trial (Art. 47)
• To protect business, in particular SMEs, who may be affected both in the offline and online environments, and which tend to be more vulnerable to identity theft and its consequences than larger firms.
• To improve the knowledge base regarding identity theft and related crime.
• To prevent the risk of forum shopping in relation to identity theft and related crime in the EU.

The case for intervention at the EU level to help tackle the problem of identity theft depends on Member States accepting that the nature and scale of the problem is such that national measures alone are no longer sufficient to contain and preferably reduce its occurrence. In the next section we seek to identify the scale of identity theft while Section 5 then examines existing national measures.
Quantification of Identity Theft

In this section, we quantify identity theft impacts, starting with the number of victims and related issues such as whether certain countries seem to be particularly targeted. In Section 4.3, we then estimate the cost of identity theft. Finally, we consider how the problem is likely to develop.

4.1 Overview

A number of considerations need to be taken into account in quantifying the impact of identity theft:

- As noted in Section 2, those adversely affected by identity theft include primary and secondary victims (individuals, businesses and public institutions) but also wider society (e.g. the increased costs for enforcement that are covered by taxpayers).

- Apart from the perpetrators of identity theft and identity-related criminal activities, there are ‘legitimate’ beneficiaries (e.g. insurance companies, software producers) whose products and services are designed to help individuals, businesses and public authorities to protect themselves against the risk of identity theft.

- Different types of impacts - identity theft and identity related crime leads to both financial and non-financial costs.

In theory, quantifying the scale of the identity problem can be done in terms of the number of individuals, businesses and other organisations that are affected by it, either as primary or secondary victims, and the financial losses involved. The impact of policy options should clearly be possible to quantify in these terms as well, i.e. the extent to which the number of victims and costs to them are reduced by interventions.

Problem of Lack of Data Availability

The magnitude of identity theft and identity-related crime in the EU is difficult to quantify. As noted in Section 2, there is no common definition, and the use of other offences such as fraud to cover identity-related crime makes it difficult to compile reliable and comparable data on the extent of the problem. Additionally, identity theft seems to be a crime that frequently is only reported to financial institutions but not to the police. This may be either because the victims are unaware that they have been the target of identity theft and/or because they are reluctant to admit that this has been the case.

The problem of poor data to quantify problems and the impact of possible EU measures to tackle them is not unique to identity theft. Taking several examples
Quantification of Identity Theft

from other fields, in its IA for a Directive on combatting cybercrime\textsuperscript{92}, the then DG CONNECT commented that: “There is also the issue of openness of data: in the European Union, firms are less willing to share data on cybercrime they experienced, for reasons of loss of reputation and potentially business opportunities. Most attacks are not reported or do not become public, because the private sector, particularly small-size enterprises, either does not record such data, or is reluctant to release such data not to draw attention to its system vulnerabilities.”\textsuperscript{93}

The same report quoted the UK’s Federation of Small Businesses finding that a third of SMEs do not report fraud or online crime to the police or to their banks because of a lack of faith in the system. It estimated that SMEs lose up to GBP 800 a year on average to cybercrime. Likewise, a similar point was made in a DG HOME IA on Critical Information Infrastructure Protection: “No-one wants to share information about embarrassing security incidents. Moreover, those who invest in data collection initiatives want a return on their investment. Collecting, aggregating and sharing data needs a sustainable business model.”\textsuperscript{94}

Although not specifically focused on identity theft, a report on the situation in the UK suggests that only 16\% of victims report cybercrime to the police\textsuperscript{95}. Another source of information concerning the scale of the problem is surveys of individuals concerning whether or not they have been affected by identity theft, often covering a certain time period such as the last ten years. Since this source is not based on victims reporting their case, it must be noted that while these data are helpful, one weakness is that not all cases that are thought to be identity theft by individuals may in reality be categorised as such.

In the US, in 2005 more than 255,000 individuals reported identity theft complaints to the US Federal Trade Commission. According to a survey by this Commission, the number of victims of identity theft accounted for approximately 8.3 million people in 2005. Therefore, only about 3\% of all victims reported their theft to the Federal Trade Commission\textsuperscript{96} (OECD, “Scooping Paper on Online Identity Theft”, DSTI/CP(2007)3/FINAL, 2008).

From a slightly different perspective, it is argued that information on identity theft is also influenced by the relatively low risk of detection and an even lower risk of prosecution although there is no real evidence to support this assertion as the source would the perpetrators of identity theft\textsuperscript{97}. The number of individuals, businesses and public institutions affected by identity theft can therefore not be

\textsuperscript{92}http://eur-lex.europa.eu/ Ryan/EN/99/2008/ DRC/009/EN
\textsuperscript{93}http://eur-lex.europa.eu/ Ryan/EN/99/2008/ DRC/009/EN
\textsuperscript{94}See European Commission, Roadmap of Legislative proposal on criminalization of identity theft (included in the European strategy on identity management), No. 2.
Quantification of Identity Theft

estimated by using data concerning the number of complaints and prosecutions - although this type of data is helpful for other reasons. To the extent that data on complaints and prosecutions is used, it needs to be taken into account that these underestimate the number of victims significantly because victims do not always report their cases.

4.2 Number of Primary Identity Theft Victims

Some recent surveys suggest that around 5% of individuals are affected by identity theft of one type of another with higher estimates in several cases. Survey data is available for a number of countries:

- In France, 4.2% of over 15 years confirmed having suffered from ID theft in the previous 10 years in total in a survey carried out in 2007 by Consumer Department of Cadoc.\(^7\)

- According to a study conducted by PwC\(^8\), 5.6% of the population in the Netherlands has been a victim of identity theft over time.

- Almost 7% of the respondents to a survey in Poland\(^9\) by declared to be victims of identity theft in Poland, which contrasts with the situation before 2004 (before Poland joined EU), when identity theft was hardly known.

- Significantly higher figures are estimated for the UK. According to an online survey in 2009, representative of the British population, 25% of the respondents indicated that they had been a victim of identity fraud.\(^10\) The higher incidence of cases in the UK is generally explained by the fact that there are no official identification numbers in the UK and that a variety of documents are used to prove a person's identity.

A similar survey with an EU-wide scope\(^11\) has been carried out within the framework of the Eurobarometer. However, while covering the entire EU, the survey does not only cover situations where individuals have experienced identity theft themselves, but it also covers situations when the respondents have “heard” about data losses. More specifically, the following question was posed: “In the last 12 months, have you yourself been directly affected by identity theft?”

---

\(^7\) Cadoc (Study Centre for study and observation of living conditions), 2009


\(^9\) TNS OPH, 2008.

\(^10\) Which, “Beat the ID fraudsters”, 2009. It is not clear if the survey results are based on all types of identity fraud or only “banking and credit card fraud.”

Quantification of Identity Theft

Table 4.1: Proportion of the population who indicate that they are affected by identity theft

<table>
<thead>
<tr>
<th>%</th>
<th>Countries</th>
</tr>
</thead>
<tbody>
<tr>
<td>1%</td>
<td>Austria, Bulgaria, Czech Republic, Finland, Greece, Hungary, Italy, Poland, Portugal, Romania, Slovakia, Slovenia, Spain</td>
</tr>
<tr>
<td>2%</td>
<td>Cyprus, Estonia, Germany, Latvia, Lithuania, Malta</td>
</tr>
<tr>
<td>3%</td>
<td>Belgium, Denmark, France, Ireland, Netherlands</td>
</tr>
<tr>
<td>4%</td>
<td>Luxembourg</td>
</tr>
<tr>
<td>5%</td>
<td>United Kingdom, Sweden</td>
</tr>
</tbody>
</table>

It can be noted that all of the eight countries in which 3% or more of the respondents have indicated that they have been affected by identity theft are "older" EU15 Member States.

Information is also available from a 2012 Eurobarometer. This Eurobarometer is focused on Internet users who have been subject to identity theft. On average 8% of the Internet users in the EU27 countries who participated in the survey indicated that they have experienced or been a victim of identity theft.

Looking at the individual EU Member states the numbers differ. Romania recorded the highest level with 16% of internet users who said that they have experienced identity theft, including 5% who indicated it has happened to them often. Respondents in Hungary (12%), UK (12%) and Austria (11%) are also more likely to have experienced identity theft compared to the average of 8%. The lowest levels were recorded in Slovenia (2%), Lithuania (2%), Greece (3%) and Denmark (3%). In Germany, 6% of the Internet users said that have experienced or been a victim of identity theft.

On average 61% of Internet users across the EU indicated that they are very or fairly concerned about identity theft. The level of concern was highest in Czech Republic, where 76% were concerned (with 45% very concerned), Cyprus (76%), Spain (75%), Bulgaria (72%), Lithuania (72%), France (71%) and Luxembourg (71%). The lowest levels of concern were recorded in Sweden (38%), Denmark (40%) and the Netherlands (42%). In Germany, the level of concern was 52% from which 16% indicated very concerned. The following figure gives an overview of the level of concern regarding identity theft in the different EU Member States.

Furthermore, an average of 12% of the responding Internet users in the EU27 indicated in the survey that they have experienced online fraud. The highest proportion was indicated by Polish respondents (18%) as well as Hungary (17%), Malta (16%) and UK (16%). The lowest levels could be found in Greece (3%), Slovenia (6%).

---

102 An overview of the results by Member State is provided in Annex K.
103 Eurobarometer 390, 2012, p. 48
104 Eurobarometer 390, 2012, pp. 48-49
and Spain (7%). In Germany, 13% of the internet user said that they have experienced online fraud. As regards the level of concern, on average 49% of the EU27 Internet users indicated that they are very or fairly concerned about online fraud. Respondents in Cyprus (70%) and Czech Republic (68%) recorded the highest levels while respondents in Sweden (23%), the Netherlands (17%) and Denmark (21%) said that they are not concerned at all about online fraud.\footnote{Eurobarometer 390, 2012, pp. 52-53}

**Although the availability of data is generally poor, there are more detailed statistics on identity theft available for several EU Member States – Germany, France, Portugal and the UK.** These cases involve individuals as well as businesses and public institutions as victims. Hence, it is not possible to convert the estimates into proportions of the population. In Germany, no figures on the total number of cases are available, but the Criminal Police Office registered 6,800 cases of digital (online) identity fraud in 2009.\footnote{Federal Criminal Police Office, “RK-Kriminalität: Bundeslagebild 2009”, 2010} It was, however, pointed out that there is significant underreporting; many victims do not realise or at least do not report that identity theft has taken place. Some relevant data have also been identified in the official statistics on fraud from Germany, as outlined in the table below:\footnote{Federal Ministry of Interior, „Polizeiliche Kriminalstatistik 2010“, 2010}:

<table>
<thead>
<tr>
<th>Fraud with illegally acquired:</th>
<th>Cases in 2009</th>
<th>Cases in 2010</th>
<th>Change (in %)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Debit cards</td>
<td>18,759</td>
<td>13,785</td>
<td>-36%</td>
</tr>
<tr>
<td>Credit cards</td>
<td>8,971</td>
<td>8,974</td>
<td>0%</td>
</tr>
<tr>
<td>Data of payment cards</td>
<td>17,072</td>
<td>19,100</td>
<td>+11%</td>
</tr>
</tbody>
</table>

Some statistics on convictions are available for France but figures could only be retrieved for the period 2007-10. In 2007, there were 3,664 cases of ID theft leading to convictions (crime foreseen by Article 434-23, Paragraph 1 of the French penal code, the only case for which some data are available). This increased to 3,709 in 2008 but fell to 3,484 cases in 2009. In 2010, 3,572 cases were reported. In about half of cases (55.2%) ID theft was associated with traffic-related crimes, in 9.5% of cases with theft and in 3.2% of cases with infringements to the immigration law.

In Portugal, one of the respondents to the online survey indicated that: “In the last three years Portugal had more than 18,000 cases and the investigations have been costly”. This estimate was supported by other respondents to the CSES online survey; in total three respondents estimated that from 2009 until 2011 there were about 4,000-6,000 investigations of identity theft and identity-related crime in Portugal on an annual basis. It can be noted that two of the respondents indicated an increasing trend (from 3,600 in 2009 and 3,900 in 2010 to 4,500 in 2011), while the third respondent estimated that there are around 6,000 cases per year in Portugal.

The most detailed figures are available for the UK, where figures are available from the UK’s Fraud Prevention Service, CIFAS. In 2011, CIFAS identified over 113,250 cases of identity fraud.
Quantification of Identity Theft

The number of cases of identity fraud increased on average by 14.8% p.a. between the years 1991 and 2011. In total, the cases have multiplied fifteen fold since 1991.

**Figure 4.1: Cases of identity fraud reported to CIFAS (UK, 1991 to 2011)**

The online survey provided several interesting explanations as to why certain countries have higher incidences of ID theft than others. One respondent commented that “Some countries are more targeted than others, like France, England and Sweden, for example, because of the social protection systems”. Another respondent suggested that “The EU as a whole is considered as an interesting target. Depending on the origin of the attack, some countries might be targeted first (based on the language)”. It is interesting to note that all those countries for which figures are available, except Germany, have been highlighted both in the survey and wider research summarised above as being particularly targeted by identity theft and identity related crime.

**Extrapolation to the EU Level**

Below, we provide estimate at the EU level of the number of identity theft cases based on three scenarios relating to the Eurobarometer data and the estimates for the incidence of identity theft cities for particular countries cited earlier suggesting that around 5% of individuals have been affected (Section 4.2). The scenarios are defined as follows:

- **Scenario 1: Lower estimate (1%)** - according to the Eurobarometer question “In the last 12 months, have you heard about or experienced issues in relation to data losses and identity theft?”, in no country the proportion of respondents that replied “Yes, it affected me directly” was below 1%. For a cautious estimate, the

---

\[108\] See CIFAS, http://www.cifas.org.uk/is_identity_fraud_serious. We assume that the organisation uses identity fraud and identity theft for the same circumstances.

\[109\] Note that the figure shows the number of identity frauds and a moving average trendline over two periods.
Quantification of Identity Theft

minimum has been set at 1% for the average population of the EU27 in view of the potential “over-reporting”.

- **Scenario 2: Higher estimate (5.0%)** - according to the results of the Eurobarometer survey, the highest proportion that reported being aware of problems were 5% of the population.

- **Scenario 3: Mid-range estimate (2%)** - according to the Eurobarometer results, the arithmetic mean is 2.0%. It should be noted that this average scenario does not consider the size of the countries.

As is shown in the table below, the mid-range estimate for the number of people affected by identity theft is just over 8 million but the figure could be as high as 20 million. These scenarios could be refined. Thus, it would be possible to weight the average by country size. For instance, the country replies of the some larger economies (e.g. NL, SE and UK) are far above the average of 2%. The scenarios could be further adjusted to take into account demographic factors and the likelihood that identity theft is correlated with the different age groups’ use of the internet and perhaps their awareness of identity theft risks/precautionary measures. However, such refinements are probably not justified given the rather indicative nature of the underlying data.

In the following table, we convert the estimates into population numbers. The estimate is based on the EU’s population of over 15 years as it is assumed that individuals who are younger than this will be less likely to be affected by identity theft (e.g. because they do not have their own bank accounts or credit cards).

**Table 4.3: Estimated number of identity theft victims**

<table>
<thead>
<tr>
<th>Scenarios</th>
<th>No. Victims</th>
</tr>
</thead>
<tbody>
<tr>
<td>EU population over 15 years</td>
<td>411,468,085</td>
</tr>
<tr>
<td>Scenario 1 – Lower estimate (1% of population)</td>
<td>4,114,680</td>
</tr>
<tr>
<td>Scenario 2 – Higher estimate (5%)</td>
<td>20,573,404</td>
</tr>
<tr>
<td>Scenario 3 – Mid Range average (2%)</td>
<td>8,229,360</td>
</tr>
</tbody>
</table>
Quantification of Identity Theft

4.3 Costs and Other Effects of Identity Theft

The following figure provides a typology of costs for victims resulting from identity theft.

**Figure 4.2: Typology of costs**

<table>
<thead>
<tr>
<th>Identity theft</th>
<th>Direct costs</th>
<th>Indirect economic costs</th>
<th>Indirect non-economic costs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Victim</td>
<td>Expenses to “clean up”: wage loss, suite and attorney costs</td>
<td>Financial disadvantages due to (false) negative information</td>
<td>Reputational damage</td>
</tr>
<tr>
<td>Victim</td>
<td>Expenses for prevention and investigation: e.g. IT systems</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Victim</td>
<td>Time spent to “clean up”</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Victim</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*depending on liability agreement

In the diagram above, the primary victim is defined as being the person or entity that is in the first instance affected by an act of identity theft. Businesses (banks, retailers, etc) and public institutions can also be secondary victims because there may be recourse to them to compensate the primary victim for negative effects arising from identity theft (e.g. financial loss). In both cases there can be direct and indirect consequences.

The types of effects arising from identity theft and the extent to which primary and secondary victims are affected is summarised in the table below:

**Table 4.4: Types of effects on victims**

<table>
<thead>
<tr>
<th>Effects</th>
<th>Primary victim</th>
<th>Secondary victim</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of money</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Time and cost of cleaning up one’s identity</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Tort implications</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Impact on credit (availability and costs)</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Impact on reputation</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Costs of enforcing one’s interests</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Cost of insurance</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Psychological and social distress</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
Quantification of Identity Theft

4.3.1 Cost of Identity Theft

Below we examine the research feedback on the costs of identity theft to the primary and secondary victims.

Primary Victims

There are a number of sources of information that can be used to estimate the cost of identity theft to primary victims – our survey, other research undertaken in several EU Member States.

The survey results suggest that the financial loss to the primary victims of identity theft is less than EUR 5,000 on average. The following table provides the results of the survey of the costs of identity theft to individuals. As can be seen, in the case of individuals, to the extent that the costs can be estimated, these are generally below EUR 5,000 per case. We received 89 responses to this question, of which 46 (51.7%) were unable to provide an estimate. The distribution of the answers of those who did reply to the question was as follows:

<table>
<thead>
<tr>
<th>Options</th>
<th>Nº</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 1,000 euro</td>
<td>22</td>
<td>24.7</td>
</tr>
<tr>
<td>Between 1,000 and 5,000 euro</td>
<td>14</td>
<td>15.7</td>
</tr>
<tr>
<td>Between 5,001 and 10,000 euro</td>
<td>4</td>
<td>4.5</td>
</tr>
<tr>
<td>More than 10,000 euro</td>
<td>3</td>
<td>3.4</td>
</tr>
<tr>
<td>Don’t know/no response</td>
<td>46</td>
<td>51.7</td>
</tr>
<tr>
<td>Total</td>
<td>89</td>
<td>100.0</td>
</tr>
</tbody>
</table>

Estimates from the other available research give similar results ranging from €2,229 to €2,800 per individual victim:

- **France** - the survey of a representative sample of the French population carried out by Credoc in 2009 stated that in total the cost of ID theft per individual was calculated as EUR 2,229 per capita, i.e. EUR 474 million for all victims in France. Of the costs per capita, EUR 1,520 represented the amount of misappropriation; EUR 563 represented the amount spent for administrative and legal procedures, while EUR 143 was additional expenditure (such as medical expenses, postal expenses, etc.). The amount of reimbursements received was of EUR 662, so that each individual was left with EUR 1,567 of net loss.

- A slightly higher figure is provided for a specific type of identity theft, namely phishing, in **Germany**; at the conference “Cybercrime – a global challenge?” in 2010 by the Federal Criminal Police Office and Federal Office for Information Security in Germany, the average loss per case of identity theft to primary and

---

100 Credoc (Study Centre for study and observation of living conditions), 2009
Quantification of Identity Theft

Secondary victims was indicated to amount to 4,000 euro for cases of phishing in the context of online banking.\footnote{111}

- A survey in Italy provided lower estimates.\footnote{112} According to the study, the amount of money stolen by means identity theft was EUR 500 (41.8% of cases), with only a low percentage above the threshold of EUR 1,000 (9.4%), and a small percentage (11.9%) between EUR 500 and EUR 1,000. The remaining 36.9% could not indicate the amount of money stolen.

- Netherlands - according to a presentation at an Expert Meeting on Identity Theft in Brussels, the loss for victims of identity theft is EUR 2,800 on average in the Netherlands.\footnote{113} Research\footnote{114} in the Netherlands suggests that between 3.08% and 3.64% of the Dutch population has encountered a financial loss as a result of identity fraud. This research also indicates that the average loss as a result of identity fraud is €2,800 per individual.

- UK - an online survey in 2009, representative of the British population suggests that the average identity fraud costs each victim EUR 2,560.\footnote{115} According to the study, one in five victims never recovered the full loss.

The effects of different types of identity crime are likely to result in different levels of losses. For example, while Portuguese police estimates the average costs relating to identity theft, if the case is related to the robbery of identity documents, the costs are estimated to be much lower (around 100 euro).

**Not all of the victims of identity theft also suffer a consequent financial loss.** Using the figures from the Dutch case, 65% of all people affected by identity theft within the EU could be victims of financial loss. Our survey suggests that the average loss is €2,500. Based on the same scenarios that were used to estimate the number of victims (see Section 4.1), the following estimates can be made of the cost of identity theft to primary victims at the EU level.

### Table 4.6: EU Level Estimates - Cost of Identity Theft (Individuals)

<table>
<thead>
<tr>
<th>Scenarios</th>
<th>No. Victims</th>
<th>Cost (€m)</th>
</tr>
</thead>
<tbody>
<tr>
<td>EU population over 15 years</td>
<td>411,468,085</td>
<td></td>
</tr>
<tr>
<td><strong>Scenario 1</strong> – Lower estimate (1% of pop)</td>
<td>4,114,680</td>
<td>6,686</td>
</tr>
<tr>
<td><strong>Scenario 2</strong> – Higher estimate (5%)</td>
<td>20,573,404</td>
<td>33,432</td>
</tr>
<tr>
<td><strong>Scenario 3</strong> – Mid Range average (2%)</td>
<td>8,229,560</td>
<td>13,373</td>
</tr>
</tbody>
</table>

\footnote{111} See https://www.bsi.bund.de/ContentBSI/Presse/Pressemitteilungen/Presse2010/BKA_luK-Kriminalitaet_120510.html.
\footnote{112} Adiconsum, “Il furto d IDENTITA' e l'esperienza dei consumatori”, which translates in “identity theft in consumers' experience”, 2010.
\footnote{114} Scale of Identity Fraud and social damage in the Netherlands, PwC, July 2011.
\footnote{115} Which, “Beat the ID fraudsters”, 2009.
Quantification of Identity Theft

From a slightly different perspective, in one of the most detailed and comprehensive attempts to estimate the costs of cybercrime, a recent study estimated the cost to the UK economy as being some €14bn.\textsuperscript{16} Although identity theft is only one driver of cybercrime it is nevertheless a very significant factor. It is difficult to extrapolate from the UK estimates to the EU level because of the relatively high prevalence of cybercrime in the UK.

Effects on business

Businesses are primary victims when their corporate identity is misappropriated and misused. Such corporate identity fraud may be used, for example, to lure individual victims to provide personal data. Furthermore, businesses may be affected due to additional enforcement costs and reduced trust among customers. However, in the interviews carried out as part of the assignment, it was emphasised that businesses are also used as a source of information to access personal data of data subjects, including staff and clients.

The online survey sheds some light on the costs for businesses although opinions are divided on the magnitude of the problem. As can be seen below, around half of the respondents who answered this question, and who did not give a don’t know response, estimated the cost of identity theft to be less than €50,000 on average with the other half suggesting it was more than this. Out of 89 responses, 65.2\% did not reply.

Table 4.7: Businesses - Do you have any insights into the direct costs (not including preventative measures, insurance etc.) of identity theft for victims?

<table>
<thead>
<tr>
<th>Options</th>
<th>N\textsuperscript{o}</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 10,000 euro</td>
<td>8</td>
<td>9.0</td>
</tr>
<tr>
<td>Between 10,000 and 50,000 euro</td>
<td>8</td>
<td>9.0</td>
</tr>
<tr>
<td>Between 50,001 and 100,000 euro</td>
<td>6</td>
<td>6.7</td>
</tr>
<tr>
<td>More than 100,000 euro</td>
<td>9</td>
<td>10.1</td>
</tr>
<tr>
<td>Don't know/no response</td>
<td>58</td>
<td>65.2</td>
</tr>
<tr>
<td>Total</td>
<td>89</td>
<td>100.0</td>
</tr>
</tbody>
</table>

Taking the survey data for this study as a starting point, if the lower range of costs shown in Table 4.9 is taken as a guide, with a mid-range estimate of €25,000 used per case of identity theft, and it is assumed that this applies mainly to smaller businesses (micro-businesses and SMEs on the grounds that they are the most vulnerable, and all SMEs are affected by identity theft at some time or another, then the total cost at the EU level could be as follows:

\textsuperscript{16} Anderson et al., “Measuring the Cost of Cybercrime”. A full breakdown of the statistics is provided in Appendix 1.
Table 4.8(a): EU Level – estimate of cost of identity theft (assumption: all businesses are victims)

<table>
<thead>
<tr>
<th>Options</th>
<th>€ Per Case</th>
<th>€ EU total</th>
<th>% EU GDP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of SMEs in the EU/EU GDP (2011)</td>
<td>20 million</td>
<td>€12.629 trillion</td>
<td></td>
</tr>
<tr>
<td>Scenario 1 – Lower estimate</td>
<td>€10,000</td>
<td>200bn</td>
<td>0.16%</td>
</tr>
<tr>
<td>Scenario 2 – Mid range estimate</td>
<td>€25,000</td>
<td>500bn</td>
<td>0.39%</td>
</tr>
<tr>
<td>Scenario 3 – Higher estimate</td>
<td>€50,000</td>
<td>1,000bn</td>
<td>0.79%</td>
</tr>
</tbody>
</table>

The above estimates are reasonable insofar as it likely to be smaller businesses that are most vulnerable to identity theft problems. On the other hand, not all SMEs are likely to suffer from identity theft-related losses. If the same assumption (65%) is made regarding the proportion of businesses affected by identity theft is made as for individuals, then the lower estimate would be as follows:

Table 4.8(b): EU Level estimate of cost of identity theft (assumption: some businesses are victims)

<table>
<thead>
<tr>
<th>Options</th>
<th>€ Per Case</th>
<th>€ EU total</th>
<th>% EU GDP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of SMEs in the EU/EU GDP (2011)</td>
<td>20 million</td>
<td>€12.629 trillion</td>
<td></td>
</tr>
<tr>
<td>Scenario 1 – Lower estimate</td>
<td>€10,000</td>
<td>130bn</td>
<td>0.10%</td>
</tr>
<tr>
<td>Scenario 2 – Mid range estimate</td>
<td>€25,000</td>
<td>325bn</td>
<td>0.25%</td>
</tr>
<tr>
<td>Scenario 3 – Higher estimate</td>
<td>€50,000</td>
<td>650bn</td>
<td>0.51%</td>
</tr>
</tbody>
</table>

Turning to other sources of information, research in the Netherlands indicates that very little is known in the private sector on the scale of identity and the resulting financial losses, due to a lack of reporting systems and since private organisations are not adequately equipped to recognise identity fraud. Also, in order to avoid reputational and competitive damage private companies withhold making these figures publicly known. However, a Dutch telecom operator interviewed as part of the assignment indicated that the average loss of an identity fraud case is around 650 euro.\(^{17}\)

Some information on the costs for businesses resulting from identity theft exists in the UK. This source which covers the UK takes into account both the financial loss to organisations and costs incurred for the adoption of systems to identify, prevent, deter and prosecute cases of identity fraud. The following figures are provided by two quite recent studies, the first by IdentityTheft.org.uk\(^{18}\) (first three sources below) and the other by the National Fraud Office (other sources).\(^{19}\)

\(^{17}\) Scale of Identity Fraud and social damage in the Netherlands, PwC, July 2011.
\(^{19}\) National Fraud Authority, “Annual Fraud Indicator”, 2011.
Quantification of Identity Theft

Impact of Identity Theft on Business (UK)

- There were losses of around €245 million for the members of a payments association (APACS) in the UK due to card identity theft including costs for prevention, detection and investigation during the time between 1 April 2006 and 31 March 2007.

- Losses of around €29 million were incurred by member firms, mainly banks, reporting to the UK’s Fraud Prevention Service (CIFAS) including preventing fraud during the time between 1 April 2006 and 31 March 2007.

- The UK banking industry lost EUR 19.5 million in 2009 as a result of forged cheques (a genuine cheque, stolen and used by a fraudster with a forged signature). The loss of the UK banking industry due to plastic card, online banking fraud and telephone banking fraud in 2009 sums up to around EUR 624.4 million. The source, however, does not provide an explanation whether the banking industry or the customers have to bear these costs.

- The UK telecommunication industry suffered losses in 2009 of around EUR 830 million (on average 2.4% of their annual revenue). The study does not provide a breakdown of the losses, making it impossible to identify the portion of costs related to identity theft. However, “subscription fraud”, i.e. the use of a false identity to acquire telecommunication services and equipment, is mentioned as an example of telecommunications fraud.

- The UK telecommunication sector had to pay for goods and services used abusively with false identity in the amount of €592 million during the time between 1 April 2006 and 31 March 2007.

A more recent report for the UK Government on cybercrime estimates that of the €3.7bn (£3.1bn) annual economic cost of cybercrime to UK citizens, an estimated €2.0bn (£1.7bn) is accounted for by identity theft and €1.7bn (£1.4bn) for online scams. Overall, the report argues that whilst government and the citizen are affected by rising levels of cybercrime, at an estimated €2.6bn (£2.2bn) and €3.7bn (£3.1bn) cost respectively, business bears most of the cost. The report indicates that, at a total estimated cost of €25.2bn (£21bn), over three-quarters of the economic impact of cybercrime in the UK is felt by business. In all probability, and in line with worst-case scenarios, the real impact of cybercrime is likely to be much greater.

Outside Europe, a study dealing with this issue in the US estimated the costs for banks and businesses stated a loss of around EUR 37.6 billion per year. Furthermore, according to the OECD, the US IT sector had direct costs from identity related crimes of EUR 41 billion in 2008.

---

120 See http://www.cifas.org.uk/cifas_members for member firms.
Secondary Victims

In many cases, the primary victims of identity theft will not themselves bear the eventual cost of any crime linked to the misuse of their identity.

It is, for example, possible to obtain insurance against identity theft and under such a policy, the insurance company will reimburse any losses to the victim. Similarly, banks and other issuers of credit cards will usually not debit sums from an individual's account if identity theft is suspected and eventually confirmed. However, the costs do of course have to be borne by the third party and as such, unless sums are retrieved from the perpetrators of identity theft, the estimates represent the costs of such activity although not necessarily in terms of the financial loss to victims.

4.3.2 Other Indirect and Non-Financial Impacts

In addition to direct financial losses to individual victims, there can be other adverse consequences. These effects can be grouped into three categories:

- Impacts on financial standing including adverse effects with regard to the availability and cost of credit.

- Costs linked to rectifying the consequences of identity theft - replacing identity documents, possible legal action, insurance, etc.

- Non-financial effects including psychological and social effects, reputational damage.

Taking the first category, there can be an impact on the availability and cost of credit. If an individual is affected by identity theft involving the fraudulent use of credit cards or other ways of making financial transactions, this can increase the risk for financial institutions and lead to a person's credit rating being reduced.

In relation to costs linked to rectifying the consequences of identity theft, this includes, for example, the need to replace identity documents. In an extreme case, it may be necessary to take legal action to rectify a case where somebody's identity has been stolen. Other costs include those relating to insurance (there are an increasing number of ways of insuring against the consequences of identity theft which is an added cost to potential and actual victims). Some very general estimates of the proportion of costs recovered were given by the respondents to the online survey (three respondents suggested that around 50% could be recovered this way, another three that only 5% could be recovered, while two respondents suggested 75% and 80% respectively). Hence, it is difficult to draw any conclusions on the basis of the information obtained.

There are few estimates of the costs of ‘cleaning up’ the identities of those affected by identity theft. In 2003, the Federal Trade Commission estimated that the time that is needed by a victim to “clean up” after an identity theft ranges between 15 and 60 hours, depending on the case of misuse (identity theft related crime on existing
Quantification of Identity Theft

accounts may cost the victim up to four times more hours than on newly created accounts). The large range in the number of hours spent can result from a non-comparable base of cases, but may also result from changes in behaviour (e.g. risk awareness raised over time) and/or support provided to victims. The Information Commissioner’s Office in the UK has estimated that the average financial loss per victim (direct costs and the hours spent for cleaning up one’s identity) ranges between approximately EUR 540 and EUR 1,270.

Taking the last point above, victims of identity theft may suffer psychological and social effects. The costs of identity theft are also seen through loss of trust in service providers/companies and loss of time used to resolve the issue, having its negative effect on consumers’ behaviour. People become more hesitant to use e-Commerce services or online banking as they become afraid of financial losses they might face after their personal data has been obtained by the fraudster.

The time and stress connected with solving the problem of one’s identity being stolen can also cause serious psychological and social distress, having a serious effect on job, family, health and social life. In a study, the majority of persons who had been victims of identity theft expressed an increase in maladaptive psychological and somatic symptoms post victimisation. Identity theft victims with unresolved cases, in contrast to those with resolved cases, were more likely to have clinically elevated BSI (Brief Symptom Inventory) scores when compared with a normative sample. Relatively similar coping mechanisms were utilised across victims. The results from this study suggest that victims of identity theft do have increased psychological and physical distress, and for those whose cases remain unresolved, distress is maintained over time.

There could also be reputational damage. Identity theft can lead to the victim being falsely accused of certain deeds and/or of not taking precautions to protect their identity. Although the victim may be blameless, and action can be taken to prove this, an individual’s reputation may nevertheless suffer by association.

4.4 Impact on the EU Economy and Wider Society

In this section we examine the overall costs of identity theft to Member States (and other countries) and then analyse the research feedback on the costs for individuals, businesses and others.

4.4.1 Costs to the European economy

There are some studies investigating this issue for UK and France and non-European countries (Australia and US) have been identified. The following estimates were made in these studies:

Quantification of Identity Theft

Estimates of Cost of Identity Theft to National Economies

- Several studies concerning the costs to the UK economy suggests that the overall cost to the UK economy is approximately EUR 2 billion per year.\textsuperscript{126}
- A CREDOC study estimated the annual cost to the French economy at approximately EUR 474 million for victims only.\textsuperscript{127}
- Studies in Australia stated a loss due to identity theft in a range between EUR 0.8 billion to EUR 3.6 billion per year.\textsuperscript{128}
- Canada’s financial loss for consumers, banks, credit card firms, stores and other businesses are estimated on approximately EUR 1.9 billion for the year 2002.\textsuperscript{129}
- Studies in the US estimated the financial loss to the economy (including individuals and corporate) in a wide range up to EUR 67.7 billion for 2004.\textsuperscript{130}

Based on in 2011 by the International Financial Statistics\textsuperscript{131}, this amounts to the following proportions of GDP. The range of 0.1% to 0.5% of GDP is not out of line with our estimates (0.1% to 0.8% of EU GDP).

Table 4.9: GDP Costs of Identity Theft (2011)

<table>
<thead>
<tr>
<th>Country</th>
<th>Costs (billion per year)</th>
<th>% of GDP (2011)</th>
</tr>
</thead>
<tbody>
<tr>
<td>UK (whole economy)</td>
<td>2.055</td>
<td>0.11%</td>
</tr>
<tr>
<td>FR (only victims)</td>
<td>0.474</td>
<td>0.02%</td>
</tr>
<tr>
<td>AUS (min)</td>
<td>0.800</td>
<td>0.07%</td>
</tr>
<tr>
<td>AUS (max)</td>
<td>3.600</td>
<td>0.31%</td>
</tr>
<tr>
<td>CAN</td>
<td>1.923</td>
<td>0.14%</td>
</tr>
<tr>
<td>US (max)</td>
<td>67.678</td>
<td>0.57%</td>
</tr>
</tbody>
</table>


\textsuperscript{127} CREDOC (Study Centre for for study and observation of living conditions), 2009


\textsuperscript{129} OECD, “Report on identity fraud: tax evasion and money laundering vulnerabilities” (unknown year of publishing), http://www.oecd.org/document/55/0,3746,en_2649_33767_42223607_1_1_1_1,00.html.

\textsuperscript{130} OECD, “Report on identity fraud: tax evasion and money laundering vulnerabilities” (unknown year of publishing), http://www.oecd.org/document/55/0,3746,en_2649_33767_42223607_1_1_1_1,00.html.

\textsuperscript{131} See http://www.principalglobalindicators.org/default.aspx.
In addition to the economic and social impacts already identified, identity theft has potentially serious implications for the digital market. e-Commerce is important for the economies of the EU Member States and an important policy objective of the EU. The growing importance of e-Commerce for the retail service sector in particular in recent years is illustrated in the following figure. Information has not been identified for the EU, but globally. Nevertheless, the figure illustrates recent trends.

![Figure 4.3: Traditional retail growth vs e-Commerce growth (global)](image)


As concerns the importance of this type of economic activity for the EU, it can be noted that the e-Commerce of enterprises via the Internet doubled (as a percentage of turnover) in the EU between 2003 and 2006, as indicated in the following table. The table shows the percentage of enterprises' total turnover from e-Commerce.132 E-Government services also increased significantly in the same time period and continued to increase until 2009.

---

132 The information comes from a survey carried out by the National Statistical Institutes on usage of Information and Communication Technologies (ICT) by enterprises. The indicator is calculated as the enterprises' receipts from sales through the Internet as percentage of their total turnover. Only enterprises from NACE sections manufacturing, distributive trades, hotels and accommodation, transport and communication and real estate, renting and business activities with 10 or more employees are covered. Eurostat, code TSHR100, last update 05.10.2011.
## Quantification of Identity Theft

### Table 4.10: Development of e-Commerce and e-Government – enterprises

<table>
<thead>
<tr>
<th></th>
<th>2003</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
<th>2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>e-Commerce (% of company turnover)</td>
<td>2.1</td>
<td>2.7</td>
<td>4.0</td>
<td>4.2</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>% of enterprises using e-Government services</td>
<td>n/a</td>
<td>51</td>
<td>57</td>
<td>63</td>
<td>65</td>
<td>68</td>
<td>72</td>
</tr>
</tbody>
</table>

**Source:** Eurostat

However, as concerns the share of turnover related to e-Commerce, the following table indicates that there has been a stagnation of this development in the EU27 in 2011. The table shows the percentage of enterprises’ total turnover from e-Commerce which did not change between 2010 and 2011 at European level.

### Table 4.11: Enterprises’ turnover from e-Commerce (2010-2011)

<table>
<thead>
<tr>
<th></th>
<th>2010</th>
<th>2011</th>
<th>Change (%-points)</th>
</tr>
</thead>
<tbody>
<tr>
<td>EU27</td>
<td>14</td>
<td>14</td>
<td>0</td>
</tr>
<tr>
<td>Belgium</td>
<td>18</td>
<td>13</td>
<td>-5</td>
</tr>
<tr>
<td>Bulgaria</td>
<td>2</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>19</td>
<td>25</td>
<td>6</td>
</tr>
<tr>
<td>Denmark</td>
<td>17</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Germany</td>
<td>18</td>
<td>17</td>
<td>-1</td>
</tr>
<tr>
<td>Estonia</td>
<td>9</td>
<td>9</td>
<td>0</td>
</tr>
<tr>
<td>Ireland</td>
<td>24</td>
<td>17</td>
<td>-7</td>
</tr>
<tr>
<td>Greece</td>
<td>:</td>
<td>4</td>
<td>:</td>
</tr>
<tr>
<td>Spain</td>
<td>11</td>
<td>11</td>
<td>0</td>
</tr>
<tr>
<td>France</td>
<td>13</td>
<td>14</td>
<td>1</td>
</tr>
<tr>
<td>Italy</td>
<td>5</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>Cyprus</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Latvia</td>
<td>7</td>
<td>6</td>
<td>-1</td>
</tr>
<tr>
<td>Lithuania</td>
<td>14</td>
<td>12</td>
<td>-2</td>
</tr>
<tr>
<td>Luxembourg</td>
<td>:</td>
<td>:</td>
<td>:</td>
</tr>
<tr>
<td>Hungary</td>
<td>16</td>
<td>19</td>
<td>3</td>
</tr>
<tr>
<td>Malta</td>
<td>:</td>
<td>14</td>
<td>:</td>
</tr>
<tr>
<td>Netherlands</td>
<td>14</td>
<td>11</td>
<td>-3</td>
</tr>
<tr>
<td>Austria</td>
<td>13</td>
<td>14</td>
<td>1</td>
</tr>
<tr>
<td>Poland</td>
<td>8</td>
<td>11</td>
<td>3</td>
</tr>
</tbody>
</table>

133 Excluding financial sector and businesses with less than 10 employees.
134 The information comes from a survey carried out by the National Statistical Institutes on usage of Information and Communication Technologies (ICT) by enterprises. The indicator is calculated as the enterprises’ receipts from sales through the Internet as percentage of their total turnover. Only enterprises from NACE sections manufacturing, distributive trades, hotels and accommodation, transport and communication and real estate, renting and business activities with 10 or more employees are covered. Eurostat, code TSHIR100, last update 05.10.2011.
Quantification of Identity Theft

<table>
<thead>
<tr>
<th>in % of total turnover</th>
<th>2010</th>
<th>2011</th>
<th>Change (%-points)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Portugal</td>
<td>12</td>
<td>11</td>
<td>-1</td>
</tr>
<tr>
<td>Romania</td>
<td>4</td>
<td>3</td>
<td>-1</td>
</tr>
<tr>
<td>Slovenia</td>
<td>10</td>
<td>9</td>
<td>-1</td>
</tr>
<tr>
<td>Slovakia</td>
<td>11</td>
<td>16</td>
<td>5</td>
</tr>
<tr>
<td>Finland</td>
<td>18</td>
<td>20</td>
<td>2</td>
</tr>
<tr>
<td>Sweden</td>
<td>18</td>
<td>19</td>
<td>1</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>17</td>
<td>17</td>
<td>0</td>
</tr>
</tbody>
</table>

Source: Eurostat, NACE code G47 (retail trade except for motor vehicles and motorcycles)

In line with the development for business, Internet purchases by individuals have increased over the last years.\textsuperscript{135} The next table shows the share of individuals that have used e-Commerce no longer than 12 months ago relative to the total population (ages 16 to 72 years).\textsuperscript{136} In 2010, approximately 40% of the EU population used e-Commerce in the EU27. The countries with the largest proportion of individuals using e-Commerce were Norway, Denmark, the Netherlands, Sweden and the United Kingdom, where more than 65% of the population purchased goods or services online.

Table 4.12: e-Commerce and e-Government – individuals (EU 27)

<table>
<thead>
<tr>
<th>in % of population</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
<th>2009</th>
<th>2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>e-Commerce</td>
<td>20</td>
<td>24</td>
<td>26</td>
<td>30</td>
<td>32</td>
<td>37</td>
<td>40</td>
</tr>
</tbody>
</table>

Source: Eurostat

Exceeding the level of 40% in 2010, overall 43% of the EU population aged between 16 and 74 years purchased goods or services online in 2011. Except for France, all EU Member States showed an increase of e-Commerce in 2011 compared to 2010. In 2011, the highest proportion of e-Commerce in the EU was observable in Sweden and the UK (over 70% of their citizens).

Regarding especially EU intra cross-border e-Commerce the proportion was low (10% of the EU population). Furthermore, there is a diverging trend between countries with very low cross-border e-Commerce usage rates (Romania, Poland and Bulgaria) and countries with high levels (Luxembourg, Malta and Austria). The countries with low levels experience smaller growth rates than the countries with high levels. The difference between the lowest cross-border usage rate and the highest one increased from 52%-%points in 2010 to 55%-%points in 2011.\textsuperscript{137}

\textsuperscript{135} Eurostat, the statistical office of the European Union, last update 27.05.2011.
\textsuperscript{136} In general, the data relates to the first quarter of the reference year.
\textsuperscript{137} http://ec.europa.eu/information_society/digital-agenda/scoreboard/docs/2012/scoreboard_life_online.pdf, p. 18 et seq.
Quantification of Identity Theft

As concerns the cross-border aspect, it can be noted that a relatively low proportion of individuals buy goods or services electronically outside their country. It can be noted that in particular the following goods have been bought via the Internet: entertainment and educational material (57% of all e-Commerce users in the EU), travel and holiday accommodation, and clothes and sport goods (52% of all e-Commerce users in the EU), household goods (38%) and tickets for events (37%).

Figure 4.4: Cross-border e-Commerce purchaser (2009)

Identity theft is generally seen, according to the survey results, as having a negative impact on consumer behaviour, particularly in relation to e-commerce. The following table combines the results for ‘quite’ and ‘very’ high negative impacts. In some cases, it can be seen that the effect is clearly negative from an e-commerce point of view (e.g., 32% saying they are less likely to provide personal details on websites) whilst in other cases the consequences of identity theft seems to be to increase awareness of the risks of online activity and the need to take sensible precautions.

---

Quantification of Identity Theft

Table 4.13: To what extent does identity theft negatively affect consumer behaviour?

<table>
<thead>
<tr>
<th>Impacts</th>
<th>Nº</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are less likely to purchase goods online</td>
<td>27</td>
<td>30.3</td>
</tr>
<tr>
<td>Are less likely to bank online</td>
<td>23</td>
<td>25.8</td>
</tr>
<tr>
<td>Are less likely to give personal details on websites</td>
<td>29</td>
<td>32.6</td>
</tr>
<tr>
<td>Give fewer personal details and/or more restrictive settings</td>
<td>19</td>
<td>21.3</td>
</tr>
<tr>
<td>Only visit websites they know and trust</td>
<td>13</td>
<td>14.6</td>
</tr>
<tr>
<td>Are likely to use different passwords for different sites</td>
<td>10</td>
<td>11.2</td>
</tr>
<tr>
<td>Do not open emails from people they do not know</td>
<td>22</td>
<td>24.7</td>
</tr>
<tr>
<td>Are likely to only use their own private PC</td>
<td>7</td>
<td>7.9</td>
</tr>
<tr>
<td>Are likely to install anti-virus software</td>
<td>43</td>
<td>48.3</td>
</tr>
</tbody>
</table>

According to a study on the delivery of parcels[^140], 60% of consumers agree that worries about falling victim of fraud or scams are a reason not to shop online cross-border because of fears in relation to payment security, privacy concerns (identity theft) or the risk of finding fraudulent vendors are a deterrent for consumers.

Effects on public authorities

Public authorities are also victims of identity theft when their means of identification are used by someone else. This could be done via illegal access to data bases, the forgery of official documents etc. Similar to businesses, public authorities are also used as a source of information to access personal data of data subjects, including staff and clients. Also, governments may have to invest more resources into enforcement activities and the reestablishment of trust among individuals. This result in costs ultimately to be paid by the taxpayers.

The same source that provided some figures for the costs for businesses also provided the following figures for public authorities in the UK between 1 April 2006 and 31 March 2007:[^141]

<table>
<thead>
<tr>
<th>Impact of Identity Theft on the Public Sector (UK)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Losses of around EUR 44 million for the public sector occupational pension schemes due to, for example, next of kin continuing to claim pension payment following the death of a relative.</td>
</tr>
<tr>
<td>• Further losses of around EUR 61 million for the Criminal Justice System of the total police investigation, prosecution, court and disposal costs for cases of identity fraud.</td>
</tr>
<tr>
<td>• The Drivers and Vehicle Licensing Agency incurred costs of around EUR 6 million for detecting and investigating applications for driving licenses using false identities. The Driving Standards Agency bore costs of around EUR 2 million for detecting and investigating identity fraud in the driving test process.</td>
</tr>
</tbody>
</table>

Quantification of Identity Theft

- Around EUR 58 million costs of prevention, detection, investigation and direct financial loss due to identity tax credit fraud.
- The Ministry of Justice bore costs related to unpaid fines due to no trace of identity or address (e.g. false or inaccurate information being provided and offenders not attending court to verify their detail) of around EUR 44 million.
- The Home Office incurred costs of around EUR 347 million relate to the work of its agencies in safeguarding and validating the identities of its customers, as well as costs around deterrence, prevention and investigation of identity fraud.

4.5 Conclusions – Impact of Identity Theft

Quantifying the impact of identity theft is beset with methodological complications and estimates need to be treated with great caution. The complications stem from a number of factors: firstly, the absence of a common definition of identity theft, making it difficult to aggregate estimates for different countries; and secondly, the lack of data even in those countries where a clear definition exists. Overall, there is better information available on the impact of identity theft on individual citizens than on business.

4.5.1 Current Situation

In terms of the primary victims, it is clear that identity theft and identity-related crime is affecting a considerable proportion of the population, and that the problem is increasing. Our mid-range estimate suggests that around 8 million individuals are affected by identity theft (2% of the EU’s population) with an average loss of around €2,500 or €20bn at the EU level. There are also indirect financial costs of identity theft arising from damage to an individual’s credit rating, the cost of rectifying the consequences of identity theft (e.g. replacing documents), as well as non-financial impacts of an adverse nature such as stress and reputational damage.

The costs of identity theft to European business are more difficult to estimate because very little research has been undertaken. Our best estimate is that business losses are around €300bn or 0.25% of EU GDP and perhaps as high as €500bn (0.4% of EU GDP). Businesses are affected both as ‘primary’ and ‘secondary’ victims. Of these two categories, the second is easier to estimate and is likely to equate to a figure that is similar to the estimate provided above for the number and value of identity theft cases for individual European citizens because these losses are ultimately borne by businesses (insurers, banks, etc.), either directly as a result of settling claims for reimbursement, or because of the need to invest in systems to help minimise the risk of identity theft. (The ultimate net loss, i.e. cases of identity theft-related financial losses where is not possible to recover the sums involved from the perpetrators, is not possible to estimate).

Public authorities can also be victims of identity theft when their means of identification are used by someone else. This could be done via illegal access to data
Quantification of Identity Theft

Identity theft is generally seen, according to the survey results, as having a negative impact on consumer behaviour, particularly in relation to e-commerce. Close to 50% of the respondents believe that individuals are less likely to purchase online as a result of the risk of identity theft.

Identity theft and identity-related crime has a clear cross-border dimension because the victim and the perpetrator are often not based in the same country and / or a person / organising who focus on acquiring and transferring on identity information to others who then use it. Problems in relation to international cooperation have also been pointed out, including problems getting access to evidence, a lack of understanding of what is possible to investigate and what the proceedings are, as well as extensive bureaucracy and formalities that need to be complied with in international cases.

4.5.2 Projected Future Trends

Looking ahead, there is a clear view that the amount of identity theft and identity-related crime will increase in the coming years. As is shown below, more than half (51.7%) of the respondents to the CSES online survey stated that there would be a ‘significant increase’ with a further 20.2% arguing that there would be at least some increase. Most of the remainder did not know.

Figure 4.5: Do you think that the overall number of cases of identity theft and identity-related crime will increase, decrease or remain stable in the next ten years?

Recent technological trends also suggest that more and more services and activities will take place in an online environment, including e-Government services, leading to an increased scope for online ID theft, although preventative measures are being taken.
Quantification of Identity Theft

As a conclusion, it is clear that identity theft and identity-related crime is affecting a not negligible proportion of the population, and that the problem is increasing. Despite a number of measures planned at the EU level, it is likely that this type of crime will continue to increase in the next years. More specific projections have not been possible to carry out at this point.
National Perspectives & Existing Measures to Combat Identity Theft

Any new EU initiative should add value to what is being done at a Member State level to combat the problem of identity theft. In this section we examine national legal and institutional frameworks that are relevant to combating identity theft, as well as non-legislative measures. We also examine the extent and effectiveness of cross-border collaboration.

The types of legal provisions at the national level dealing with identity-related crimes, their punishment and support mechanisms for victims vary. EU Member States can be grouped together in the following three clusters:

- **Cluster 1**: Countries that only have a small number of measures in place and have low punishments for identity-related crimes (14 Member States): AT, CZ, DE, DK, FI, HU, IT, LU, MT, PL, SE, SI;
- **Cluster 2**: Countries that have an average to high number of measures in place and have low to average punishments for identity-related crimes (7 Member States): BE, EE, FR, IE, NL, PO, UK;
- **Cluster 3**: Countries that have a low to average number of measures in place and high punishments for identity-related crimes (6 Member States): CY, LT, SK, BU, GR, RO.

In the following subsections we examine these different elements in detail, starting with national legislation. This part of the assessment draws on the 2011 RAND study and our more recent research that included a survey of experts to obtain up-to-date information on national legislation and measures.

### 5.1 Identity Theft Legislation and Institutional Set Up in Member States

We start by examining the extent to which specific legislation to combat identity theft is in place in the various EU Member States, turning then to the question of whether primary and secondary victims are covered by national legislation.

#### 5.1.1 Extent to which specific legislation on identity theft is in place

As noted earlier (Section 2), only some EU Member States have enacted specific 'identity-related crime' or 'identity theft' legislation. According to the 2011 RAND report, these are Estonia, France and Slovenia. Furthermore, in the present assignment it was established that Poland introduced specific provisions in 2011.

For example, in France, legislation on identity theft has introduced the important consideration of non-financial loss to the victim of such crime, and thus moves the discussion on from the area of pure fraud. A recent Article in the Criminal Code (Article 226-4-1) states (our unofficial translation):

---

142 Comparative study on legislative and non-legislative measures to combat identity theft and identity related crime
National Perspectives & Existing Measures to Combat Identity Theft

“Appropriating the identity of a third person or using one or several pieces of information of whatever nature which allow for the identification of a third person with the intention to harass this person or others, or to damage the person’s honour or reputation, is punishable by a year’s imprisonment and a fine of 15,000 EUR”

The same punishment applies where this offence is committed via an electronic communications network open to the public. Any attempt to commit the offences is punishable by the same penalties. On its face, this provision deals with acts committed with the intent to either harass a person or damage the person’s reputation and not ones where the offender intends to cause financial losses.

A more detailed discussion on the different definitions is provided in Section 2. Our analysis summarising the information in the RAND report is included in Appendix A.

The absence of specific legislation on identity theft does, however, not mean that identity theft is not criminalised in the Member States whose laws do not refer to the identity-related element of the act concerned. Most of the other Member States instead use legal provisions on fraud or forgery and thus do not commonly refer to identity “theft”, but rather to “fraud” or other types of crime committed by means of identity information. Furthermore, the “mere theft” of an identity or identity information is not always considered a crime, but rather it is the use made of the identity acquired illegitimately that takes the conduct into the criminal area. In this way, identity theft is considered as a method for committing another crime and not as an act that is criminalised “on its own merit”.

A distinction can thus be made between primary victims (i.e. persons, whose identity is “stolen”) and secondary victims (e.g. persons that are defrauded by means of the identity information that had been acquired from the primary victim). In this respect it can be noted that the secondary act (i.e. the use of the identity information for various types of criminal acts) would in many cases be a criminal act regardless of whether identity information was being abused to commit it or not.

Based on a review of the existing national legislation, the 2011 RAND report identified a number of different approaches to legislation on identity theft and related crime, including the following:

- Specific identity theft legislation that criminalises varying types of misuse;
- Legislation relating to identity documents and numbers that governs the existence, use and forgery of specific identity tokens or credentials
- General penal provisions on fraud, forgery and usurpation of titles;
- Regulations specific to a particular type of crime such as organised crime or terrorism; and

140 P. 35
National Perspectives & Existing Measures to Combat Identity Theft

- **Non-criminal regulations**, including administrative infractions, civil suits and torts, on which basis non-criminal fines may be given and/or the awarding of damages to victims, and legislation on the protection of personal data (including when personal data can be collected, for what purposes it may be processed and security breach notification laws)

According to the RAND report, most national legal frameworks in the EU are “sufficiently comprehensive” to cover cases of identity theft and related crime although specific legislation is not in place. The following conclusions were drawn:

In 19 Member States\(^{144}\), the legislation was explicitly stated to be sufficiently comprehensive. In two further countries (MT, PL) it can be derived that the framework is sufficiently comprehensive.

Legislation was only clearly stated to not cover all cases of identity theft in one country (Finland). This conclusion was drawn as the Criminal Code only covers certain types of identity thefts. In addition, in cases of fraud the injured party is not considered to be the person whose identity has been stolen, but, for example, the store where the purchase was made with the false identity. This said, as concerns the latter point, the situation in Finland does not seem to be much different from that in the other Member States; this argument concerns the distinction between primary and secondary victims, which has not been systematically assessed in the RAND report. Therefore, a similar gap may exist in other Member States. A question to clarify the current situation has been sent to the Member States by the Commission. An analysis of the answers received to the survey by 8 October 2012 is provided in the following sub-section.

The legal frameworks in the remaining five countries (CZ, GR, IT, RO and ES) were not pointed out as inadequate, but some weaknesses were noted. For example, in some countries (GR, RO, MT) it was explained that not all cases of identity theft were covered, whereas for others statements were made such as legislation is under development. Information concerning the situation in each of these countries is provided in Appendix J. It can be noted that two of these countries, Romania and Greece, at the same time were pointed out to have comparatively high punishments (see above).

The conclusions concerning whether national legal systems are sufficiently comprehensive or not seems to be primarily based on whether any cases could be identified that were not covered by legislation as well as on-going developments.

5.1.2 Primary and Secondary Victims

The extent to which primary and secondary victims are covered by national legislation was not assessed systematically in the 2011 RAND report. This is an important aspect, not the least with regard to the types of situations where a victim can be identified on the basis of existing legislation: if national legislation does not cover e.g.
National Perspectives & Existing Measures to Combat Identity Theft

the act of acquiring identity information without a further crime being committed with this information, it is not possible to speak about victims in the sense of the law. As a consequence, this group of “potential” (primary) victims would also not be covered by the recently proposed Directive on the protection of victims, since the application of this Directive will depend on whether the person is legally recognised as a victim.

As noted above, in order to gather some more detailed insights concerning the situation in the Member States with the existing legislation in place concerning primary victims, a follow-up survey with the Member States was launched in August 2012 within the framework of the present study. The purpose of the survey was to gather information concerning the legislative situation in relation to primary victims of identity theft, i.e. those victims whose identity information is “stolen”. The findings from the survey are as follows:\[^{145}\]

- Only three of the eighteen survey responses received, from Czech Republic, Ireland and Italy indicated that the primary victim of identity theft is covered by legislation even though the identity information acquired by unauthorised means has not yet been used in a criminal offence itself\[^{146}\].

- However, nine countries (Austria, Bulgaria, Estonia, Greece, the Netherlands, Poland, Slovakia, Spain and United Kingdom) referred to some possibilities to obtain redress. In Estonia, anyone who finds that his / her personal rights have been violated by someone else can submit a civil claim to a court and request that the violation is ended as well as compensation for the damages. The same accounts for the case of the Netherlands and Poland.

- In the case of Bulgaria, the acquisition of information through computer systems is an exception to the general rule that the act of acquiring identity information by unauthorised means is not considered to be a criminal offence itself. In this case, however, the criminal offence is the unauthorised access rather than the acquiring of information itself. In Bulgaria, administrative sanctions are also provided for failure of the administrators of personal data when processing such data.

\[^{146}\] This following analysis provides an overview of the situation in the 18 countries that had replied to the survey by November 2012 (Austria, Belgium, Bulgaria, Croatia, Czech Republic, Estonia, Germany, Greece, Hungary, Ireland, Italy, the Netherlands, Poland, Romania, Slovakia, Spain, Sweden, and the United Kingdom), i.e. ten EU15 Member States, seven EU12 countries and Croatia. Overview tables where the answers are given by Member State are provided in Appendix J.

\[^{145}\] Only Ireland answered the affirmative to the following question: Legislation addressing the process of taking someone’s identity (obtaining identity information) - Are persons whose identity has been stolen / compromised considered to be victims in your country independently of whether a related crime is carried out through the use of this information or not? That is, is the act of acquiring identity information by unauthorised means considered to be a criminal offence in itself or addressed by other measures? Please specify whether this is addressed by means of criminal, administrative, or private law measures, if applicable.
National Perspectives & Existing Measures

to Combat Identity Theft

- **In Slovakia**, obtaining information is only covered when the act of obtaining identity information itself can be considered as theft (according to section 212 of the domestic Criminal Code).

- **Spain** does not generally cover the acquisition of identity information, unless obtained photos are of pornographic nature and distributed, for example, through the Internet.

- In the **United Kingdom**, possession of identity information with the intention to use this data fraudulently can be considered an “article” for the use in fraud and therefore is an offence under the Fraud Act 2006. The legislation in the UK is deliberately unspecific in order to capture all kinds of occurrences regarding identity theft. However, this also implies that it cannot be assessed what exact occurrences the UK legislation covers and not.

A number of countries (**Belgium, Croatia, Germany, Hungary, Italy, Romania and Sweden**) do not have any criminal, administrative or private law measures that the “victim” can use to enforce his / her interests. In the reply from Sweden it was specified that the acquisition of identity information cannot be covered as theft since official documents such as passports and driver’s licenses are missing an economic value.

This said, the answers to questions concerning the **types of actions that are covered in national legislation** suggest that the situation in different EU Member States is more nuanced than what the answers to the question of whether legislation exists or not. Gaining access to the victim’s **computer and / or bank accounts** is covered in most of the Member States that have answered the survey, except e.g. Estonia and Poland. The situation in Hungary, Ireland, the Netherlands and the United Kingdom is unclear.

Ten Member States (Belgium, Bulgaria, Croatia, Germany, Greece, Italy, Romania, Slovakia, Spain, and Sweden) cover **gaining access to accounts** leading to the unauthorised person obtaining a pecuniary advantage for him-/herself or for a third person, thereby damaging the assets of another person (Germany, Slovakia), the transfer of personal data “which are not generally accessible” (Germany), identity fraud committed by electronic means, for example, in social networks such as Facebook (Romania, Spain, Sweden), the breach of the secret of transferred messages (Slovakia), and the abusive access to an informatics system (Italy). In Belgium, fraud does not fit explicitly in the material element, although the notion of identity deception is a form of commission of the offense of computer fraud.

Legislation in Estonia, Germany, Greece and Poland specifically covers the **provision of information to third parties free of charge as well as selling identity information**. In Estonia, the act of providing the data or making it otherwise available with the

---

14 The following question was posed: If this is the case, what is the scope of the current legislation in terms of acts covered (obtaining identity information, providing it to third parties free of charge, selling it, etc.)? It may be that some cases are covered, but not all. For example, acquiring identity information by stealing a credit card may be covered, but not acquiring identity information available online, e.g. on social networking sites. Please comment on the situation in your country.
National Perspectives & Existing Measures to Combat Identity Theft

knowledge that it would be used in order to commit an offence, is covered by criminal law. In Germany, a person who purchases, procures, disposes, or assists in disposing items that have been stolen or otherwise acquired by an unlawful act directed against the assets of another person, the criminal offence of handling stolen goods is applicable. Polish legislation, i.e. Article 49 (1) and art. 51 (1) of the Act on Protection of Personal Data, refers to the issue of providing identity information to third parties free of charge or selling it. In Hungary, the misuse of personal data is a crime in accordance with section 177/A of Act IV of 1978 on the Criminal Code, if a person who, in violation of the statutory provisions governing the protection and processing of personal data, is engaged in the unauthorized and inappropriate processing of personal data.

Turning to legislation in place concerning secondary victims, in many countries, identity theft is tackled mainly through legislation on fraud (e.g. Belgium, Czech Republic, Bulgaria and the UK). Other types of legislation are also used. For example, according to one Finnish respondent to the CSES online survey: “Several other criminalisations with wider coverage are used, e.g. fraud, means of payment fraud, defamation, dissemination of information violating personal privacy, data protection offence, registration offence, giving false identifying information, criminal damage, unauthorised use, interference in a computer system, computer break-in, message interception etc. depending on the circumstances of the case. Even the preparation of means of payment fraud has separate criminalisation.” An overview of the legislation that is used in the Member States is provided in Appendix A.

As concerns the link between secondary crime and primary victims, out of the eighteen countries that have replied to the CSES survey, only Croatia and Romania stated that they do not provide legal rights and benefits to primary victims when a secondary crime has effects on them. This answer was also given by Ireland, where primary victims are, on the other hand, stated to be covered independently of whether a secondary crime has been carried out or not. In the other Member States, primary victims are considered a victim of the secondary crime (for example fraud, an offence and conceal of the true identity of the perpetrator, or further criminal offences) as well.

Generally it can be stated that in the majority of Member States that have replied to the survey, the matter of whether or not the person affected by “identity theft” is to be considered an aggrieved person depends on whether his / her rights, objects of legal protection, or legally recognised interests have been directly compromised by the injurious act. In such cases, the primary victim of identity theft can benefit from victims’ rights that are stipulated in the legislation.

---

\(^{148}\) The following question was posed: If the person whose identity is compromised is considered a victim independently of whether a crime is committed by means of the identity information or not. In particular, where a (secondary) crime is committed using the identity information, such as a fraud, is the person whose identity has been misused also considered a victim of that secondary crime? Does he or she have the rights attributed to victims in the code of criminal procedure in your Member State, i.e. can benefit from any victim’s rights etc. that presuppose “official” victim status?
National Perspectives & Existing Measures to Combat Identity Theft

5.1.3 Effectiveness of legislation in combating identity theft

In the survey we asked for opinions on how effective legislation is in relation to the prosecution of identity theft and identity-related crime (e.g., whether all cases of identity theft and identity-related crime currently covered or there are gaps).

As can be seen from the following table, a relatively low proportion of the respondents consider existing national legislation to be effective in combating identity theft.

Table 5.2: How effective is the legislation in place in your country in relation to the prosecution of identity theft and identity-related crime?

<table>
<thead>
<tr>
<th>Options</th>
<th>Total</th>
<th>Specific legislation</th>
<th>Not specific legislation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Nº</td>
<td>%</td>
<td>Nº</td>
</tr>
<tr>
<td>Not very effective at all</td>
<td>2</td>
<td>2.9</td>
<td>1</td>
</tr>
<tr>
<td>Not very effective</td>
<td>15</td>
<td>22.1</td>
<td>6</td>
</tr>
<tr>
<td>A little effective</td>
<td>11</td>
<td>16.2</td>
<td>4</td>
</tr>
<tr>
<td>Somewhat effective</td>
<td>11</td>
<td>16.2</td>
<td>5</td>
</tr>
<tr>
<td>Quite effective</td>
<td>16</td>
<td>23.5</td>
<td>7</td>
</tr>
<tr>
<td>Very effective (no gaps)</td>
<td>4</td>
<td>5.9</td>
<td>2</td>
</tr>
<tr>
<td>Don’t know/ no opinion</td>
<td>9</td>
<td>13.2</td>
<td>5</td>
</tr>
<tr>
<td>Total</td>
<td>68</td>
<td>100.0</td>
<td>30</td>
</tr>
</tbody>
</table>

According to the survey results, the views are divided: there are no major differences between respondents from those countries that have indicated to have and those that do not have specific legislation on identity theft in place. This means that the survey results could suggest that the effectiveness of legislation is not linked to whether identity theft is a specific crime or not. However, it could be that some of the answers to the survey may also be linked to the effectiveness of the enforcement of existing legislation or even the degree to which enforcement takes place at all, depending on how the question has been interpreted by the respondents. Therefore, some caution should be taken with regard to the conclusions that can be drawn.

Furthermore, some stakeholders that are against a common definition argued that introducing identity theft as a specific crime would lead to problems in their country in view of the fact that the effect of identity theft (e.g., fraud, harassment) is already covered in specific legislation and that there could be an overlap. It has also been commented in interviews that some countries have explicitly taken the approach to not intervene at such an early stage that no further crime has been committed with the acquired identity information.

Note that the total number of 68 responses refer to those respondents that answered the following question positively: "Do your Member State have specific criminal legislation in place on identity theft and identity-related crime or is this dealt with through legislation with a broader focus, e.g., fraud legislation?"
National Perspectives & Existing Measures to Combat Identity Theft

deeply rooted in the national legal traditions and that the EU Member States have different approaches in this regard.

Those countries that have recently amended their criminal law to respond more effectively to identity related crime must be presumed to have done so, whether in answer to public or political pressure or to meet the concerns of police or law enforcement agencies, in order to remedy gaps that existed in their criminal statutes. For example, in the UK the Fraud Act 2006 was drafted with a view to remediating deficiencies that had appeared in the Theft Act 1968 by focusing criminality on the conduct of the perpetrator rather than on the result of the act. Internet crime was referred to in Section 2(5) of the Act where the making of a false representation was defined as including one that is “submitted in any form to any system or device designed to receive, convey or respond to communication (with or without human intervention”).

The change in legislation in Estonia in 2009 to explicitly cover transmission of identity information (see Section 2) was, according to a stakeholder from the Ministry of Justice, not motivated by a specific episode, but rather by a series of events. Around this time, both the Ministry of Justice and the Data Protection Inspectorate received several hundred complaints of individuals for fraudulent use of email addresses, whose personal data were used to open false profiles on social networks, etc.

In the light of this situation, the rationale for adopting specific legislation was to, on the one hand, provide support to the victims and, on the other hand, act as a deterrent against this type of crimes by making it a criminal offence. It can, however, be noted that prior to the introduction of the new legislation, citizens had the possibility to sue the offender(s) in civil court, in order to obtain restoration of damage. This option is still open for citizens. A brief comparison between the advantages and disadvantages of criminal and civil recourse is provided in the following table.

### Table 5.1: Advantages and Disadvantages of Civil and Criminal Recourse

<table>
<thead>
<tr>
<th>Type of recourse</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
</table>
| Criminal recourse | • Penalties available (fines/imprisonment) may be a more effective deterrent.  
• Demonstrates that the conduct is sanctionable in wider social terms as distinct from being a mere personal wrong.  
• More possibilities may exist for cross-border cooperation between police and judicial authorities. | • Always an element of discretion in whether a prosecution is undertaken by the police or public prosecutors.  
• Higher standards of legal proof may make successful conviction more difficult.  
• It may be more difficult to compensate the primary victim. |
| Civil recourse | • Initiative to take action remains with the person affected. | • The risk of legal costs to the victim.  
• The likelihood the proceedings will |
National Perspectives & Existing Measures to Combat Identity Theft

<table>
<thead>
<tr>
<th>Type of recourse</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Recouped compensation may result from successful judgment.</td>
<td>be more time-consuming and burdensome to the victim.</td>
</tr>
<tr>
<td></td>
<td>• Interim measures may be more easily available (e.g. injunctions).</td>
<td>• Difficulty in proving degree of loss/damage in some cases.</td>
</tr>
</tbody>
</table>

As concerns the effectiveness of the new legislation, according to the Ministry of Justice, the number of reported cases is considerably lower than the number of complaints received by the Ministry of Justice and the Data Protection Inspectorate prior to the change in the legislative framework and in Estonia it is considered that the introduction of this crime has had a deterrent effect, resulting from the existence of a specific definition of ID theft and the consequences of this (e.g. having a criminal record). This said, so far no one has been convicted for identity theft according to the relevant piece of legislation.

What is less clear, and what indeed may be doubted from the contributions made at the expert groups and the responses to our online survey, is that Member States that have not amended their criminal law to deal with any perceived gaps in connection with identity-related activities are completely satisfied that their laws adequately meet the challenges posed by the general phenomenon under discussion. While the RAND study reached the somewhat reassuring conclusion that ‘the need for new criminalising regulations is not evident’ on the basis that Member States’ existing laws ‘may well prove to be adequate to address identity theft in practice’, the study nonetheless acknowledged both that the absence of any uniform approach meant that the same behaviour might be legal in some states but not others, and that gaps might exist in different states’ legislation depending on how broadly or narrowly identity theft is defined.

5.1.5 Penalties for identity theft

Turning to the penalties, some stakeholders have noted that they in some EU Member States can be considered to be relatively low. The same conclusion was drawn in a 2007 report by the UN. In this respect, it was pointed out that it is important to have appropriate penalties in place in order to achieve a preventative effect. It can be noted that in order to be able to use the mutual legal assistance instrument put in place under the UN Convention on transnational crime, there is a need for the crime to be serious. Criminal offences for which cooperation is requested also need to meet a threshold of at least four years. This is important in view of the strong involvement of third countries, in particular as hosting perpetrators (see previous analysis). The lowest maximum level of penalties in place based on the RAND report is four years (in Finland).

150 An overview of the penalties in the Member States is provided in Appendix A.
National Perspectives & Existing Measures to Combat Identity Theft

The various levels of penalties have also been pointed out to result in "identity shopping" (or "forum shopping") in the stakeholder consultations. This means that criminals locate themselves in or focus on those countries where penalties are not significant. This problem was also reflected in a UN report, according to which it is possible for offenders to target a specific group of victims to take maximum advantage of any gaps in offence provisions or investigative powers or capacity in certain national territories ("forum shopping"). According to the same report, the establishment of flexible jurisdictional regimes plays an important role in ensuring the effectiveness of the international cooperation mechanisms used to combat identity-related crimes which are of a transnational nature.

No such conclusions can, however, be drawn based on the available information on the location of perpetrators and the available sanctions. More specifically, the EU Member State that has been pointed out most frequently in the stakeholder consultations as a common location for perpetrators is Romania, which together with Bulgaria (another of the countries that has been mentioned as a frequent location) has the highest level of penalties (20 years). The penalties actually given in these countries may, however, of course be much lower, which could potentially provide some explanation of their prominent role as hosting locations together with the level of enforcement. It could, however, also be that countries with higher penalties have adopted these in view of the extent of the problem. Such conclusions can, however, not be drawn or supported on the basis of the available evidence; information concerning the countries in which victims are based (see section 4) also does not support such conclusions. This said, in view of that the penalties do differ, there is scope for forum shopping.

5.1.6 National Institutional Frameworks

Cooperation between national institutions even within the Member States often seems to be rather ad hoc and responsibilities not always clearly identified. This is a particular problem since a large number of actors play a role in preventing and addressing the problem of identity theft. As a consequence, addressing the problem of identity theft can be hindered or at least not very efficient when more organisations or even more chains are involved. One of the interviewees described this in the following way: "Cooperation can be hindered by the fact that this framework is not the result of a 'grand design' but of a slowly evolving process." This seems to be the case in several of the case study countries. Furthermore, it has been pointed out in the case study interviews that information sharing may not always be possible due to privacy or ICT restrictions.

Another challenge is a lack of a common language and understanding of identity theft within the Member States. Such problems have, for example, been identified in Portugal, where action to address these issues is taken, e.g. as part of the development of a Portuguese National Plan on Secure Identity, which should result in a common framework. According to Portuguese stakeholders, the ongoing work on the Action Plan

National Perspectives & Existing Measures to Combat Identity Theft

involves all key institutions and is expected to result in a better cooperation between the many key actors in the near future. Also the Home Office in the UK is working to improve the co-ordination of the institutional framework, both through a newly established Home Office Identity Security Team and through the National Fraud Intelligence Bureau.

As concerns the specific public institutions involved, in all case study countries the relevant Government Ministries (normally the Ministry of Interior or Justice) play a key role together with the police. These actors collaborate with a number of other institutions (the institutions concerned vary between the Member States). Frequently mentioned agencies include data protection agencies and authorities that specialise in fraud.

In addition to collaboration between public institutions, collaboration with private actors is very important. The private sector often plays an important role both in terms of preventing identity theft and acting as a first contact point for victims that have been subject to identity theft (e.g. banks are contacted when a victim’s credit card details have been abused). This needs to be viewed in the context of that in most of the case study countries, there are no “official support initiatives” for victims that have been subject to identity theft in place, but they may e.g. contact the police, consumer organisations or NGOs that are active in the field. Interestingly, in the Netherlands an “Identity Fraud Support Office” (CMI - Centraal Meldpunt Identiteitsfraude en -fouten) was established recently, whose task is to help victims whose identity has been misused. A brief overview is provided below. Based on the available information, no equally comprehensive “one stop shops” have been identified in other Member States.

Netherlands - Centraal Meldpunt Identiteitsfraude en -fouten

- The CMI is a small organisation of three employees, but cooperating with a wide range of organisations that have committed themselves to do so. This includes any institution, business or other organisation that may be helpful to help victims.
- The support office has an agreement with most public parties involved in fighting identity crime and restoring errors in public databases. According to the CMI the annual costs for 2011 for providing support to victims amount to €400,000.
- The office deals with approximately 250 cases per annum, sometimes involving more than one individual and usually involving more organisations.

In the next sub-section, initiatives to prevent and address identity theft as well as to support victims are considered.
National Perspectives & Existing Measures to Combat Identity Theft

5.2 Identity Verification Systems and Prevention Aspects

Both public and private actors play a role with regard to identity management, both in terms of issuing identification documentation and similar, as well as the authentication process. Indeed, according to a UN study\(^{153}\) the majority of countries seem to rely on identity documentation being issued by public as well as private actors.

To illustrate the complexity of the current situation, research results from Portugal can be quoted. In Portugal, a research exercise was carried out, which was aimed at identifying the different identification documents in Portugal. The results showed that there are around 150 different identification documents that are currently accepted for identification purposes and over 30 Portuguese institutions with responsibilities in relation the register, production/issuing and control of these cards. Naturally, as a consequence, it is difficult for police officers to know and recognise all the existing documents.

Weaknesses in identity verification systems and the behaviour of data subjects and data controllers impact on the extent of the problem. Indeed, findings from the consultations carried out by us suggest that a high proportion of the problem of identity theft and related crime could be avoided if individuals were more careful with the personal data and relevant documentation. Below, we briefly explore the concept of ID management as well as the behaviour of data subjects and data controllers.

5.2.1 Identity Management

Identity management is a collection of techniques used to identify, authenticate and authorise users of a given system. This principle can be applied both to the physical world as well as to the digital world. The purpose of identity management is to create security for the system that needs protection and accountability for the users that are granted access to the system. In a typical day to day scenario, a user requesting access to e.g. the airport identifies him- or herself with his/her passport is authenticated by the security guard at the customs service and consequently authorised to enter the restricted area. Each of these terms and issues relating to them are considered below.\(^{154}\)

As a starting point, identification is the process where a person, user or other entity makes itself known to another person or system. Identification is not a formal process; it can happen with a username, a passport or just saying one’s name. Identification in itself does not per se pose a security risk as the verification of the authenticity of the identification happens in the next step, authentication. A problem with identification can, however, be that the subject does not wish to identify him- or herself, for example in criminal prosecution or cases of illegal migration. Police forces, for example, have varying degrees of investigative powers to ensure proper identification.

\(^{154}\) SANS, ISACA.
National Perspectives & Existing Measures to Combat Identity Theft

The ways in which someone may be authenticated can be clustered into three categories, based on what are known as the factors of authentication. Security research suggests that for a positive identification, elements from preferably two, or even better, all three, factors should be verified, although the elements are also sufficient without being combined. The three factors and some of the elements of each factor are as follows:

- **Ownership factor**: Something the user has (e.g. a wrist band, ID card, security or software token or a telephone);
- **Knowledge factor**: Something the user knows (e.g. a password or a pass phrase, a PIN number, a “challenge response” whereby the user must answer a question etc.);
- **Inherence factor**: Something the user is or does (e.g. unique identifiers such as fingerprint, retinal DNA sequence, pattern, face, voice, signature or other biometric identifiers).

Authorization is the process that starts after successful identification and authentication and involves the coupling of authorisations, permissions and rights to a certain identity. A user could, for example, be authorised to conduct bank transactions affecting his/her own bank account, or a person could be allowed access to a building based on his authorisations. An up-to-date database of authorisations (or authorisations matrix) is necessary to ensure that the correct authorisations are connected to the right identities. As concerns the risks associated with authorisation, some examples are provided in Appendix C for various common (combinations of) authentication methods.

Despite the increasing security features of identification systems, there are many ways to frustrate number verifications, and identity fraud using personal numbers is rising. In the following sub-sections, we consider challenges relating to national identification and insurance numbers more in-depth.

### 5.2.2 Lack of Care of Data Subjects and Controllers

Individual behaviour covers the behaviour of both natural persons (individuals) and legal persons, such as businesses and public sector institutions. The level of awareness of risks and effects is one factor impacting on individual behaviour in relation to identity information. For example, persons may or may not click on a link in a phishing email depending on whether they are aware of the potential risks.\(^{155}\)

\(^{155}\) Indeed, there are several actions that individuals can take in order to avoid (or reduce the chance) to become victim of identity frauds, including treating information as 'confidential' and 'reserved' personal data and e.g. keep personal documents in safe places and memorise passwords and PIN numbers (instead of writing them down). In addition, banks and other relevant institutions should be promptly informed on any change of address. Caution should also be placed in relation to publishing information on social networks as this information may be abused. This includes avoiding publishing personal information (such
National Perspectives & Existing Measures to Combat Identity Theft

Lack of awareness may explain why victims of identity theft have displayed various forms of risky behaviour. For example, instead of memorising their passwords people may carry them in their wallets; when using a bank ATM machine, customers might not sufficiently shield their hand thus allowing ‘shoulder surfers’ with binoculars or video cameras to get access to personal data. A study for PayPal contains a number of important insights concerning individual behaviour on the Internet and how it may encourage identity theft based on a survey. The study covered the following EU Member States: Germany, Spain, France and the UK. In addition the US and Canada were covered. As to the results of the survey:

• A quarter of the respondents expressed they are very concerned about identity theft, while approximately 50% - 60% is slightly concerned. Nevertheless, approximately one in six users of online social networks displays information on their profile that is also used for their passwords.

• In terms of differences between countries the study found that identity theft is more pronounced in English speaking countries than in non-English speaking countries. Around 25% - 30% of users in the countries covered by the study have more than seven passwords, while 30% to 40% of users only have 1-3 passwords.

• The majority of users (55% - 65%) change their passwords less than once a year and about 20% of users write down their passwords in order to remember them, which increases the risk of theft of identity information. In addition, about half of the online consumers use important dates, family members’ names or nicknames or pet’s names as their password.

A 2011 Eurobarometer survey on Internet Security indicates that more than 40% of European Internet users have been asked to disclose more information than required for accessing or using a service on the Internet. However, they also feel that disclosure of information is part of modern life. While not all of this information that is being disclosed is likely to refer to identity information, it points to an increasing trend of making more and more information available, which can potentially be abused. Indeed, the research points to that sophisticated systems that combine pieces of information from various sources are already in use.

---

as telephone number, email address, or physical address] on profiles, put high privacy protection filters (to restrict access to the personal profile) and using a strong password.


---

Centre for Strategy & Evaluation Services
National Perspectives & Existing Measures to Combat Identity Theft

Eurobarometer Survey on Internet Security

- 60% of the interviewees think that one needs to log onto several systems using several usernames and passwords. Furthermore, 58% of the respondents commented that there is no alternative than to disclose personal information if one wants to obtain products or services.

- While 63% of the interviewees indicate that disclosing personal information is a big issue to them, nearly one third (28%) does not feel obliged to disclose personal information online. Regarding identity theft, this is considered to be a risk of using online services, but not considered to be the most important risk. A majority of Europeans do not want to disclose personal information in return for free services online, such as a free email address. Nevertheless, 29% of the respondents do not mind disclosing this type of information.

- Only 32% of Europeans trust telephone companies or Internet providers and 70% are concerned that personal data collected and stored by companies could be used for other purposes than for which they agreed on.

- As concerns the type of information which is disclosed most online, according to the survey 79% of the users of social networks or sharing sites make their names known, followed by pictures of themselves (51%) and nationality (47%). It can be noted that none of these types of data were identified as “most risky” data in the CSES survey. This said, this type of information may be linked to other information and the combination may be abused for criminal offences.

- About 13% disclose their national identity number, identity card number or passport number. 10% of respondents reveal financial information (e.g. salary, bank details and credit record). 72% of respondents who had experienced unnecessary disclosure of personal information when obtaining access to or using online services were very or fairly concerned about this over-disclosure.

- To protect their identity in daily life, 62% of Europeans give the minimum required information or do not disclose their bank details or PIN numbers (56%)19, while almost half disclose information only to people and organisations they trust (47%) or do not disclose their user names and passwords (45%). Around three out of ten respondents use cash instead of recorded transactions such as bank cards and transfers (30%), shred old bills, bank statements and so on (29%), do not disclose payment card details online (29%), and adjust the information they disclose to different contexts (27%). A few interviewees provide wrong information to protect their identity in daily life (7%). (p. 100).

- Approximately 42% of Europeans who use Internet apply tools and strategies to limit unwanted emails. 39% of them use anti-spy software, 35% delete cookies. Only 22% of the Internet users change the security settings of their browser to increase privacy. 15% out of the survey spontaneously say that they do nothing to protect their identity on the Internet.

19 It is not specified in the survey where and in what context.
National Perspectives & Existing Measures
to Combat Identity Theft

A 2012 Eurobarometer survey on cyber security\(^{60}\) also contained questions concerning individuals' risk behaviour in an online environment. According to this survey, the respondents who are Internet users confirmed that they have changed their online behaviour in a number of ways because of security concerns.

**Figure 5.1: Change in behaviour because of security concerns**

As can be seen from the above figure, almost 4 out of 10 (37\%) stated that they are less likely to give personal information on websites, while 43\% indicated that they do not open emails from people they do not know. Half of the respondents (51\%) have installed anti-virus software. However, at the same time, more than half (53\%) of the Internet users answered that they have not changed any of their online passwords during the past year.

According to the survey results, respondents in the 'newer' EU Member States are less prone to make changes than in the 'older' EU15 Member States. Indeed, the highest proportions of respondents who have stated that they have not made any changes were recorded in Latvia (33\%), Bulgaria (29\%), Poland (29\%) and Cyprus (25\%). The survey also included questions about disclosing personal information and views on related risks. The vast majority of the Internet users agreed that they avoid disclosing personal information online (89\%, of which 51\% strongly agreed). Findings are similar across most EU Member States.

These results can be considered together with views on whether information provided is kept secure or not; the clear majority stated that they are concerned

---

60 European Commission (2011): "Special Eurobarometer 390 – Cyber Security"
National Perspectives & Existing Measures to Combat Identity Theft

that their online personal information is not kept secure by websites (72%), while 25% disagreed. These results are similar to those recorded in the 2011 Eurobarometer (see above). Two-thirds are concerned that this information is not kept secure by public authorities (66%), while 31% disagreed with this statement. Here, some variations were noted between different Member States. More specifically, the proportion of Internet users who agreed that they are concerned that their online personal information is not kept secure by websites is highest in Spain (89% agree), followed by Portugal and Greece (82% respectively) and Luxembourg (81%). Respondents were least likely to agree in Denmark (57%), Finland (58%) and Sweden (60%). There is also between respondents in the EU Member States as regards attitudes to personal information being kept secure by public authorities. The highest proportion of respondents that stated that they are concerned that their online personal information is not kept secure by public authorities was recorded in Spain (83%), followed by Greece (81%) and Portugal (78%). Respondents in Finland (30%), Denmark (32%) and Sweden (36%) are on the other hand less concerned. Thus these patterns are similar to those with regard to personal information being kept secure by websites.

Finally, it can be noted that close to 3 out of 4 respondents (74%) stated that the risk of becoming a victim of cybercrime increased in the past year; 16% disagreed with this statement. Not surprisingly, respondents who have heard or read something about cybercrime in the past 12 months also tend to be more concerned. Of those that have heard or seen something about cybercrime, 78% stated that the risk has increased in the last year, compared with 58% who had not heard or seen anything.

The Generation Y Online Security Survey of April 2010 from the US emphasises that young adults often engage in risky online behaviour. More than 1,000 young adults between the ages of 18 and 24 were polled with regard to their online behaviour and security precautions. Over seven out of ten stated that they were not always as careful as they should be when posting and accessing information online. More than 50% of all respondents admitted to both using the same password for all of their online accounts and staying logged in to their personal sites, thus seeking to avoid the time and hassle of logging in every time anew. Fifty-five percent of those surveyed indicated they never check their credit report, and 35% do not always check bank records after making online purchases. 31% admit they do not always take steps to verify a website is legitimate before submitting credit card information. According to the study, convenience trumps safety.

As concerns the behaviour by businesses and public institutions that lead to problems or risks of identity theft, the examples that were provided in the online survey are summarised below. It can be noted that the same behaviours as were indicated for businesses were also mentioned in relation to public institutions. However, a number of additional behaviours were mentioned, which are also listed below. Many of

361 Generation Y Online Security Survey (2010):
http://www.rsa.com/maintenanceprivacy/Gen_Y_Int_Sec_Surv_Res_TRU_RSA.pdf More than 1,000 young U.S. adults between the ages of 18 and 24 were questioned in the course of the Generation Y Online Security Survey of April 2010.
National Perspectives & Existing Measures to Combat Identity Theft

The respondents seem to have focused on behaviour that does not necessarily lead to the identity of specific public institutions being obtained, but rather personal information about individuals.162

Table 5.3: Risk behavior by businesses and public institutions

<table>
<thead>
<tr>
<th>Organisation</th>
<th>Company level</th>
<th>Staff level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Companies and public institutions</td>
<td>• Employing insufficiently verified persons.</td>
<td>• Not shredding documents, papers, letters, contracts, etc.</td>
</tr>
<tr>
<td></td>
<td>• Insufficient security of computer networks and</td>
<td>• The use of the same password for different accounts and having a written</td>
</tr>
<tr>
<td></td>
<td>anti-virus systems, fire walls and other security</td>
<td>note on the passwords.</td>
</tr>
<tr>
<td></td>
<td>features.</td>
<td>• Replies to phishing emails.</td>
</tr>
<tr>
<td></td>
<td>• Inadequate implementation standards. Credit</td>
<td>• Offline activities (stealing invoices to obtain account banking numbers).</td>
</tr>
<tr>
<td></td>
<td>Cards are still too easy to copy. An upcoming</td>
<td></td>
</tr>
<tr>
<td></td>
<td>issue is the now-common mTAN-process, which was</td>
<td></td>
</tr>
<tr>
<td></td>
<td>set up to use two different channels (mobile and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>online) which now appear to be on the same devices.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Lack of a risk analysis.</td>
<td></td>
</tr>
<tr>
<td>Public institutions only</td>
<td>• Financial constraints / Other (political)</td>
<td>• Use of the same password for various accounts.</td>
</tr>
<tr>
<td></td>
<td>priorities</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Inadequate sanctions in case violations are</td>
<td>• Issuing documents with full personal data</td>
</tr>
<tr>
<td></td>
<td>detected</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Inadequate security of systems</td>
<td>• Storage of personal data without encryption</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Simple identity verification with only one document or detail</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Procedures without recurring contact with the individual so that control</td>
</tr>
<tr>
<td></td>
<td></td>
<td>data can be verified.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Not being careful with emails containing confidential data.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Spreading personal information on social networking sites.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Not detecting information leaks and not reacting appropriately when such</td>
</tr>
<tr>
<td></td>
<td></td>
<td>are detected.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Corruption of employees.</td>
</tr>
</tbody>
</table>

162 In the survey, the respondents were not asked to provide actual examples, so these problems may be a combination of actual and hypothetical problems.
National Perspectives & Existing Measures to Combat Identity Theft

In the survey carried out as part of the present study, the respondents were also asked if identity theft and identity-related crime could be avoided if users were more careful with information. As the following table shows, quite a high proportion of survey respondents indicated that problems could be avoided if this was so.

Table 5.4: What proportion of cases of identity theft and identity-related crime could, in your opinion, be avoided if users were more careful?

<table>
<thead>
<tr>
<th>Options</th>
<th>N</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>1-20%</td>
<td>7</td>
<td>7.9</td>
</tr>
<tr>
<td>21-40%</td>
<td>15</td>
<td>16.9</td>
</tr>
<tr>
<td>41-60%</td>
<td>17</td>
<td>19.1</td>
</tr>
<tr>
<td>61-80%</td>
<td>26</td>
<td>29.2</td>
</tr>
<tr>
<td>81-100%</td>
<td>9</td>
<td>10.1</td>
</tr>
<tr>
<td>Don't know/ no response</td>
<td>15</td>
<td>16.9</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>89</td>
<td>100.0</td>
</tr>
</tbody>
</table>

These figures are only “guessimates” and caution should be taken with regard to the results. Nevertheless, the clear conclusion that can be drawn is that experts working in the field suggest that a high number of cases could be avoided if individuals changed their behaviour.

One further problem in relation to ID theft is that it may go unnoticed as individuals may not, for example, check their credit card statements and discover that unauthorised payments have been made. Here, banks can play a role: some banks have, for example, implemented systems to identify when cards are used in locations where individuals are not usually based (to use the card abroad, individuals usually need to inform the bank of their travel in advance of the journey in order for the card to be 'unlocked').

As a conclusion, both individuals and staff from the public and private sectors engage in risky behaviour, which may lead to that criminals are able to ‘steal’ identity information. Furthermore, an increasing amount of personal information, including identity information, is made available online. This information may be subject to abuse. According to the stakeholder consultations carried out as part of the present assignment, one of the key measures to be taken to address this problem is to reduce the risk behaviour by individuals, businesses and public institutions.

5.2.3 e-Government

A national identification number or a national insurance number is used by the governments of many countries to identify citizens, permanent residents and temporary residents. They are used in relation to work, taxation, government benefits, health care and other governmentally related functions. In some countries the number appears on the ID card issued by the country. The implementation of identity
National Perspectives & Existing Measures to Combat Identity Theft

(verification) numbers varies from country to country. Twenty-four out of twenty-seven EU Member States (93%) have implemented ID cards, whose use is compulsory in eighteen of them (67%). Denmark, Ireland and United Kingdom do not use ID cards.

As part of the evolution of e-Government services (information on trends is provided below), national ID cards have become the main tool to access e-Government services. Indeed, as part of the on-going technological evolution, identity cards have been progressively transformed into electronic identity cards (eID), which is a government-issued document for online and offline identification. In addition to online authentication, many eID cards also give users the option to sign electronic documents with a digital signature.

More specifically, eID cards are normally equipped with a chip card, and embed additional electronic features, such as the eID function, biometric data as well as additional software that make it possible to digitally sign documents and forms. However, some stakeholders have raised doubts concerning whether eIDs will solve the problems of ID theft and ID fraud. A first consideration concern the diffusion of these devices; the wider the market penetration of eID cards, the more likely future attacks will be (as the market size will make them worthwhile). In addition, the use of eID cards alone will not stop identity frauds, as hackers can find loopholes.

The table below shows the use of e-Government services by individuals (e.g. downloading official forms, obtaining information from public authorities or to sending completed forms). More than a third of the EU27 population used e-Government services in 2010, which corresponds to a 9 percentage-point increase in comparison to 2005.

<table>
<thead>
<tr>
<th>Table 5.5: Development of e-Government - individuals and enterprises (EU27)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2004</td>
</tr>
<tr>
<td>-------</td>
</tr>
<tr>
<td>e-Government: Individuals (in % of population)</td>
</tr>
<tr>
<td>% of enterprises## using e-Government services</td>
</tr>
</tbody>
</table>

National and EU institutions make continuous efforts to improve the security features of identification systems, as a way to combat identity thefts and fraud, e.g. through the use of biometric data for identification purposes. Regulation (EC) 2252/2004 requires biometric data to be collected and stored with regard to passports and travel documents issued by Member States.

---

## Footnotes

163 A full inventory of the ID cards adopted in each of the EU Member States, containing indications on their compulsory use (when it is the case), description and integration in the national eGovernment service provision, can be found in annex.

164 Excluding financial sector and businesses with less than 10 employees.
National Perspectives & Existing Measures to Combat Identity Theft

The Regulation does, however, not apply to identity cards issued by Member States to their nationals or to temporary passports and travel documents having a validity of 12 months or less.\(^{165}\) The benefits of biometrics include that they are unique identifiers. In order to be able to fully take advantage of these benefits, the way in which checks of e.g. identity documents are carried out are essential. It is also imperative that a possibility to verify the integrity of the fingerprints on a passport after issue is provided for. This is at present not always possible as no copies of e.g. fingerprints or the passport are stored in the database of issuing authorities in at least some Member States, due to privacy protection provisions.\(^{166}\) As concerns the risk of abuse, one challenge is that once stolen, biometric characteristics cannot be reset like a PIN number.\(^{167}\)

Furthermore, Member States also make efforts in terms of addressing problems once an identity document has been stolen, e.g. the Belgian CheckDoc initiative\(^{168}\), where stolen identity documentation can be blocked. Public and private entities using this system can check whether an identification document presented to them has been blocked or not. Private actors also implement this type of systems. For example, in Sweden “Soliditet”\(^{169}\) provides the possibility to block the possibility to take credits based on personal information in order to avoid (further) misuse of personal data. In one of the experts workshops that was arranged in April 2012 as part of the present assignment, it was, however, recognised, that many Member States struggle with developing responses to online identity theft and that many are, in a first instance, working on addressing problems relating to physical theft of identity documentation.

Online identification is also used by the private sector. For example, to be able to use e-Commerce services, users (enterprises as well as individuals) often have to provide their debit or credit card details, address information and other personal or identity-related information. Furthermore, users often use the possibility to create an online account to facilitate future purchases from the same business. One problem in this context is the fact that customers cannot assess from the website alone how well their data will be protected. Furthermore, data owners often share data amongst each other.

One way to reduce the potential for abuse of identity information is the use of ‘CAPTCHAs’ (Completely Automated Public Turing test to tell Computers and Humans Apart), which is increasingly implemented by private companies in their online purchase channels. The CAPTCHAs make it possible to distinguish between humans and computer. They are easy to solve for a human brain but need enormous resources on a computer (pattern recognition). However, methods to attack CAPTCHAs have also been developed.

\(^{165}\) 2010c-0707 PIIRS and IDFR in Innovating Government Manuscript_100707
\(^{166}\) Grijpink Snijder; 2008b Biometrics security, trend report on biometric CLSR.
\(^{167}\) 2004d Identity fraud as a challenge to the constitutional state
\(^{168}\) https://www.checkdoc.be/CheckDoc/
\(^{169}\) http://www.soliditet.se/cms/lang/en_GB/soliditet/AboutSoliditet
National Perspectives & Existing Measures to Combat Identity Theft

To conclude, secure identity management to identify, authenticate and authorise users of a given system both in the physical and online world is key to prevent the problem of identity theft. This is a process that involves public as well as private actors, both in terms of issuing identification documentation and with regard to the authentication process. Despite the increasing security features of identification systems, there are many ways to frustrate number verifications – some of which have been pointed out above. The importance of proactive action to ensure the security of identity management systems is recognised by public authorities as well as by the private sectors, and as reflected above, action is being taken at the EU and national levels, and also by the private sector.

5.2.4 Collaboration between key stakeholders at the national level

Turning to cooperation between national institutions, collaboration even within the Member States often seems to be rather ad hoc and responsibilities not always clearly identified. Furthermore, there seems to be a lack of a common language and understanding of identity theft within the Member States. This is a particular problem since a large number of actors play a role in preventing and addressing the problem of identity theft.

In addition to collaboration between public institutions, collaboration with private actors is very important. Both public and private actors play a role with regard to identity management, both in terms of issuing identification documentation and similar, as well as the authentication process. The private sector often plays an important role both in terms of preventing identity theft and acting as a first contact point for victims that have been subject to identity theft (e.g. banks are contacted when a victim’s credit card details have been abused). This needs to be viewed in the context of that in most of the case study countries, there are no “official support initiatives” for victims that have been subject to identity theft in place, but they may e.g. contact the police, consumer organisations or NGOs that are active in the field. Interestingly, in the Netherlands an “Identity Fraud Support Office” (CMI - Centraal Meldpunt Identiteitsfraude en -fouten) was established recently, whose task is to help victims whose identity has been misused. Based on the available information, no equally comprehensive “one stop shops” have been identified in other Member States.

5.3 Identity Theft Reporting Systems and Victim Support

As indicated at the start of this section, a number of measures to address identity theft and identity related crime has been put in place in the Member States. This includes reporting mechanisms for victims and awareness raising campaigns. The following measures were reported on in the 2011 RAND report:\textsuperscript{170}:

- Specific reporting point (4 Member States): IE, NL, RO, UK;

\textsuperscript{170} An overview of the reporting points and portals that are in place in the Member States is provided in Appendix J.
National Perspectives & Existing Measures to Combat Identity Theft

- Dedicated **online portal for identity-related crimes** (2 Member States): NL, UK and for **all crimes** (11 Member States): AT, BE, BG, FI, GR, IT, LT, LV, MT, NI, UK.

- **Offline portal for all crimes** (2 Member States): EE, PT and for **all crimes as well as specifically for identity theft** (one Member State); IE;

- **Portal with feedback on cases** (one Member State): NL; and

- **Public awareness campaign** (9 Member States): LU, SE, BE, EE, FR, DE, NL, UK, GR.

Thus, based on the information in the RAND report, only one Member State has a reporting mechanism in place that covers identity theft specifically as well as other crimes, plus a feedback mechanism, namely the Netherlands. One further Member State (the UK) provides a reporting mechanism focusing specifically on identity theft as well as other crimes, but no feedback mechanism; the UK. Additionally, nine Member States (AT, BE, BG, FI, GR, IT, LT, LV, MT) provide for online reporting mechanisms for all crimes, while three Member States (EE, IT, PT) provide an “offline” portal. According to the RAND report, it cannot be concluded that portals covering other crimes than identity theft only are not as effective or efficient. In total 13 Member States do not provide for any reporting mechanism (CY, CZ, DE, DK, ES, FR, HU, LU, PL, RO, SI, SK and SE).

In the RAND Report online/offline portals and dedicated reporting point are not defined explicitly. However, by looking at the contents of the report the following distinctions/definitions can be made. Online portals and specific reporting points are reporting mechanisms as well as information portals for (Internet-based) crimes (e.g. identity theft). A dedicated reporting point focuses specifically on identity theft and identity-related misuse while other portals are characterised by a more general approach which means that they do not exclusively focus on identity theft. Examples of dedicated reporting points and online portals are provided below:

**Example of a specific reporting point**

A specific reporting point is the CMI in the Netherlands, referred to above, which is the Central Reporting and Information Point for identity fraud and identity errors (http://www.overheid.nl/identiteitsfraude). The CMI is an initiative of the Dutch government. The main objective is to assist individuals faced by identity fraud or mistakes in the registration of personal data. Furthermore, the website provides information on the prevention of abuse as well as warning signs. Inquiries can be made via a contact sheet.

**Example of an online portal**

Austria has an online portal. This includes websites for the provision of information on

---

172 Rand Report, p. 67
National Perspectives & Existing Measures to Combat Identity Theft

Offline portals are websites that support offline reports. For example, in Ireland, a website service (www.hotline.ie) is identified in the RAND report which provides a facility for the public to report suspected illegal content encountered on the Internet, including complaints concerning identity theft and phishing, although it is mainly concerned with material such as child pornography.

As concerns the conclusions that can be drawn concerning the level of available support to victims, according to RAND 2011, although there are some initiatives to establish reporting mechanisms in several Member States, interactive online reporting mechanisms were in 2011 not yet prevalent, and in those cases when they were available, their functionality was stated to generally be limited. More specifically, even when they allow victims to register complaints, the follow-up of the complaint was stated to in many cases be unclear. Furthermore, investigations into specific incidents were often not treated as a high priority or closed relatively quickly when damages were unclear or perceived to be limited.

Some information concerning whom individuals would turn to in case of identity theft is available in a 2012 Eurobarometer on cybercrime (i.e. if they would contact the police or other organisations / reporting mechanisms). According to the results of the Eurobarometer, the majority of survey respondents would contact the police (85%) in case of an identity theft incident whereas 13% of the respondents stated that they would contact the relevant website or vendor (13%), their Internet service provider (13%) or a consumer protection organisation (10%). In case of an online fraud incident, the majority of Internet users indicated that they would contact the police (57%), while 34% say they would contact the website or vendor. 22% of the respondents would contact a consumer protection organisation (22%) followed by 12% who would contact their internet service provider.

As concerns differences between respondents in various countries, respondents in Germany (72%), Sweden (68%) and Portugal (67%) indicated that they would most likely contact the police, while this proportion is relatively low in countries such as Slovenia (32%), Luxembourg (34%), Bulgaria (35%) and Ireland (35%). In Ireland a high proportion said that they are more likely to contact their internet service provider (27%). Respondents in the Netherlands (55%), Luxembourg (54%), Slovenia (52%) and Denmark (51%) recorded the highest proportion of respondents - compared to the other EU27 countries - who indicated that they are would contact the website or vendor.

As concerns the proportion that is likely to contact a consumer protection organisation is particularly high in Estonia (39%). The Eurobarometer results thus overall suggest that most victims would use established channels such as the police, while a minority

173 Rand Report, p. 45
174 Rand Report, p. xiv
175 Eurobarometer 390, 2012, p. 63
National Perspectives & Existing Measures to Combat Identity Theft

would use other reporting mechanisms, although the results vary between the Member States.

Overall, research shows that most Member States do not have a clear division of responsibilities relating to victims and that limited reporting systems are in place, although cases may of course be reported to the police when a crime has been committed. Indeed, almost half of the Member States do not have any reporting mechanisms other than turning to the police and where reporting mechanisms are in place, their functionality is limited. For example, according to the RAND report, the interactivity of the online sites identified above is limited as the individuals who report cases are not typically informed of how their reports will be treated, and the cross-border dimension of many identity theft incidents is largely not addressed by the reporting mechanism; it is not possible to transmit reports to investigative authorities in other Member States. On this basis, it can be concluded that there is room for improvement, in particular when considering that the reporting mechanisms could also be used as a useful data collection tool. 176 As concluded by RAND:

"Setting up one-stop shops is a key part of the solution, as these allow identity victims to more easily report identity crimes and can also act as a communications device to enable investigators to keep the victims updated on the status of specific investigations solution, as these allow identity victims to more easily report identity crimes and can also act as a communications device to enable investigators to keep the victims updated on the status of specific investigations". 177

Our survey also included a specific question on measures taken to improve the support to victims. The survey results confirmed that while some countries have a dedicated institution in place that deals with various types of aspects concerning identity theft and identity-related crime, including support to victims (e.g. CIFAS in the UK and the National Identity Fraud Office in the Netherlands), in many countries support is provided by consumer organisations (e.g. AT, BG), which work both with prevention and assistance in case of problems. Some respondents indicated that victims are referred to the police.

As concerns the budget for running these types of schemes, one respondent working for the National Identity Fraud Office in the Netherlands indicated an annual budget of €400,000 with assistance provided in approximately 250 cases (some of which some involve more than one victim). As concerns the number of cases or victims supported, the following figures were also provided: a Belgian organisation stated that they provide assistance to around 1,000 victims on annual basis; in Austria, a consumer organisation provides assistance to around 300 victims each year. A few other organisations indicated that they assist between 20 and 50 victims annually.

Some examples of reporting systems in place were identified in the case study interviews:

176 Rand Report, p. xiv
177 P. xii.
National Perspectives & Existing Measures to Combat Identity Theft

Examples of Identity Theft Reporting Systems

- In Poland the RESTRICTED DOCUMENTS system\(^{178}\) (System DOKUMEN Y ZASTRZEZONE) protects people who have lost their identity documents. Anyone who has lost documents or had documents stolen should immediately inform its bank. Information from one bank is then rapidly communicated to all banks and other institutions via the RD system.

- In the Netherlands, in addition to the National Identity Fraud Office there is a general fraud helpdesk (telephone, email), referring victims of ID fraud to the CMI. This helpdesk is an initiative of the Ministry of Security and Justice. There is also a centre of expertise & documents at Schiphol airport, which is a collaboration between the Police and the Royal military police (the CMI also has an office located there). This organisation provides support to organisations that suspect identity fraud. It has a long standing reputation for its expertise on documents - not only travel documents but also money etc.

- In France, a direct line called “Info Escroqueries” is operational since 2009. This service allows all victims of ID theft to contact the police or the gendarmerie to have information about risks and procedures to follow\(^{179}\). In addition, a website for signalling cases (www.internet-signalement.gouv.fr) has been created within the Central Office for fight against crimes linked to ICT (Office Central de Lutte Contre la Criminalité liée aux technologies de l’Information et de la Communication – OCLCTIC) of the Central Direction of Judicial Police (Direction Centrale de la Police Judiciaire – DCPJ). This website allows Internet users and service providers to point immediately any attempt of fraud on the Internet, and in general any illegal content.

- The UK, on the other hand, does not have a central system of recording identity, but instead they are seeking to ensure that information on criminality is shared wherever possible to tackle the growing problem of identity crime.

In terms of public awareness raising campaigns, some examples can be given to illustrate the nature and scope. Safer in the net\(^{180}\) is joint initiative of public institutions and the private sector in Poland, which aims to provide information on how to safely and easily use the Internet. One of the partners is the Ministry of Economy.

There are also various initiatives in the UK to promote an awareness of identity theft amongst individuals and organisations. The Home Office and the NFA work to raise public awareness of identity crime and what someone should do if they are a victim. This includes access to a free service from the Credit Reference Agencies who will repair any damage done to an individual’s personal credit file. Further examples of specific initiatives are provided below.

---


\(^{179}\) The service is available via phone (08/11/02/02/17) from Monday to Friday from 9 am to 6 pm.

\(^{180}\) [http://www.bezpieczniejsziecie.org/](http://www.bezpieczniejsziecie.org/)
National Perspectives & Existing Measures to Combat Identity Theft

NL and UK – Raising Awareness of Identity Theft

- The Home Office Identity Fraud Steering Committee launched the www.identity-theft.org.uk website which contains tips about how to avoid ID theft.
- In addition, the Information Commissioner’s Office has produced educational materials on ID theft through an information toolkit, television advertisements; and a training DVD. The UK Department of Trade and Industry (DTI) has likewise developed - Consumer Direct, a telephone and Internet advice service providing consumers with information on fraud and notably on phishing. Another initiative – GetSafeOnline is a private-public initiative between the UK Government, the Serious Organised Crime Agency, companies and various banking and payment associations, to educate both their own members (i.e. banks, and companies) and their customers on the computer safety and dangers connected with identity theft.
- In the Netherlands a number of initiatives have been taken to increase the awareness of the risks of identity fraud and provide support to victims. For example, having started modestly a few years ago, citizens can log on to the “MyGovernment” website and check the growing number of data about them that is provided through this site. The goal is to provide citizens with all available data; not just personal data, but also files and data that are connected to their identity (crime investigations etc. are the exception of course).
- Connected to “Mygovernment” will be the option to report errors with the request to repair these errors. Transparency helps fighting errors or possible crime, since people can check their own data. Furthermore, in 2012 the public will be warned of risks of copies of identification documents. Since false documents of Dutch IDs are rather uncommon, ‘lookalike fraud’ (fraudsters using a passport of someone they look like) is supposed to get serious. Also, rather common in the private sector for identification and registration purposes are copies of IDs. These copies play a dominant role in simple but effective identity crime, since copies are accepted and widely stored. Campaigning against illegal distribution of copies will take place in the second half of 2012. For this campaign, the Ministry of the Interior (through the support office) will cooperate with municipalities, the Civil Service Road and the Dutch Data Protection Authority.

In view of the importance of awareness raising that has been pointed out both in desk research and the stakeholder consultations as preventative measures, it seems that while initiatives are taken, they are not taken on a broad scale and in some countries it has specifically been pointed out that no specific awareness raising campaigns are planned.

5.4 International Cooperation in Investigations

In view of the strong transnational element in cases of identity theft and related crime, effective and efficient cross-border collaboration is key, both within the EU and with third countries. In this regard, the CSES survey included a question on the extent to which there are problems in working across borders to tackle the problem of identity theft. A high proportion of respondents did not know the answer to this
National Perspectives & Existing Measures to Combat Identity Theft

question but of those who did, most indicated that there were problems, and that these are greatest where there is a need to collaborate with the law enforcement authorities in countries outside Europe.

Table 5.6: Are there any problems with regard to (international) cooperation/investigations between law enforcement authorities in the field of identity-related crime?

<table>
<thead>
<tr>
<th>Option</th>
<th>EU Member States</th>
<th>Non EU countries</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Nº</td>
<td>%</td>
</tr>
<tr>
<td>Yes</td>
<td>28</td>
<td>31.5</td>
</tr>
<tr>
<td>No</td>
<td>10</td>
<td>11.2</td>
</tr>
<tr>
<td>Don’t know</td>
<td>51</td>
<td>57.3</td>
</tr>
<tr>
<td>Total</td>
<td>89</td>
<td>100.0</td>
</tr>
</tbody>
</table>

The following examples were given of problems relating to cooperation between EU Member States (it can be noted that many of the respondents pointed out different problems):

- A respondent from Ireland suggested that the most serious are delays in getting access to evidence, conflicting priorities in different Member States and human resources deployed to cybercrime. Related to this, one Portuguese respondent pointed out that it is very difficult, if not even impossible to obtain information concerning the owner of a bank account used on ID fraud online.

- Other respondents (from Belgium and Ireland) pointed to a lack of understanding of what is possible to investigate and what the proceedings are in other countries, e.g. if there are certain financial damage thresholds for a prosecution. This, according to one respondent, calls for better training in the understanding of the other national prosecution and classification systems; ultimately, in the EU: harmonised legal framework.

- A respondent from Italy was of the view that there is a lack of collaboration in cross border e-crimes that are not related to drugs, terrorism, weapons and child pornography. Furthermore, better capacity and know-how to investigate online identity-related crime was seen as imperative.

- Respondents from Belgium and the Netherlands stated that the bureaucracy and formalities involved in international cooperation means that it is not used as much as it could. For example, in the Dutch respondent’s experience, international police requests are usually mainly done in large cases, leaving “some smaller though clear cases on the shelf”.

- One respondent from The Netherlands suggested that the starting point should be to facilitate fingerprint checking and identity investigation in the country of nationality and/or residence.
National Perspectives & Existing Measures to Combat Identity Theft

Finally, problems relating to privacy legislation were also identified: data protection legislation was indicated to sometimes protect criminals and prohibits public/private fraud entities to exchange ID's of fraudsters.

One issue of particular relevance to the present assignment is the question concerning whether the lack of a common definition on identity theft results in problems in cross-border cases or not. Whereas according to the survey results as much as 64% of the respondents consider the introduction of a common definition to be very important and another 17% it to be important, when it comes to identifying actual problems to confirm this need, only scarce anecdotal evidence has been given. More specifically, when asked why it would be useful to introduce a common definition, most stakeholders generally referred to the problem of a lack of data and the likely benefits a common definition could have in relation to measuring the scale of the problem, rather than problems in cross-border collaboration. Thus, while most stakeholders are in favour of introducing a common definition, there is little evidence to confirm the need for this in practice.

Furthermore, it was argued that problems are rather due to a more general lack of cooperation in cross-border cybercrime that are not related to drugs, terrorism, weapon and child pornography than varying legal definitions and legislative frameworks. Other stakeholders were of the view that differences in legal provisions do not as such lead to problems, but instead practical problems may occur if authorities do not know how to use mutual legal assistance instruments or do not get the legal assistance needed. Improving the mutual recognition takes away the problems of substantive criminal law.

The respondents were also asked if the current varying levels of penalties cause problems in cross-border collaboration. Close to two thirds of those who answered this question were of the view that the different penalties lead to problems. It can, however, be noted that as many as 57 out of 89 respondents (64%) did not answer this question.

This was, for example, stated by participants to the second workshop, but also in interviews that have been carried out. Only one stakeholder pointed out that problems result from the fact that what is possible to investigate or prosecute in a country is not necessarily so in another country, however, without giving any more concrete examples. Another stakeholder indicated that the lack of a common language and minimum legal common standards constrain the efficiency of information exchanges and therefore the efficiency of law enforcement action. However, again, no specific examples were given.

While being unable to provide any concrete evidence, one workshop participant was of the opinion that the absence of uniform criminalisation of identity theft could have an adverse effect on the freedom of movement of EU citizens and that identity should be protected to the same extent in all Member States. While taking account of this comment by the workshop participant, it can be highlighted that based on the assessment of legislation carried out by RAND, most Member States seem to have legislation in place that cover all or most incidences of identity theft. Thus the validity of this comment may be questioned. There is also currently no evidence that legislation on identity theft is a factor that is taken into account by citizens when they move to other countries.
National Perspectives & Existing Measures
to Combat Identity Theft

Table 5.7: Do the varying levels of penalties for identity-related crime/ lack of penalties in different Member States lead to problems, e.g. in cross-border police cooperation?

<table>
<thead>
<tr>
<th>Options</th>
<th>N</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>21</td>
<td>23.6</td>
</tr>
<tr>
<td>No</td>
<td>11</td>
<td>12.4</td>
</tr>
<tr>
<td>Don't know/no opinion</td>
<td>57</td>
<td>64.0</td>
</tr>
<tr>
<td>Total</td>
<td>89</td>
<td>100.0</td>
</tr>
</tbody>
</table>

Relating to the problem of forum shopping that has been identified in the stakeholder consultations (which has been stated to be due to the variations of levels of penalties), in cross-border cooperation any accumulation of cases in one country leads to resistance to help in other EU countries ('downward spiral'). However, others were of the opinion that harmonising the level of penalties is not critical.

5.5 Conclusions – National Perspective and Existing Measures

As noted at the start of this section, any new EU initiative should add value to what is being done at a Member State level to combat the problem of identity theft.

5.5.1 Overall Position – Existing National Measures

As concerns the current measures in place in the EU, the Member States can be grouped together in the following three clusters in terms of the types of legal provisions that are in place at the national level dealing with identity-related crimes, their punishment and support mechanisms for victims:

- **Cluster 1**: Countries that only have a small number of measures in place and have low punishments for identity-related crimes (14 Member States): AT, CZ, DE, DK, FI, HU, IT, LT, LU, MT, PI, ES, SE, SI;
- **Cluster 2**: Countries that have an average to high number of measures in place and have low to average punishments for identity-related crimes (7 Member States): BE, IE, FR, IE, NL, PO, UK;
- **Cluster 3**: Countries that have a low to average number of measures in place and high punishments for identity-related crimes (6 Member States): CY, LT, SK, BU, GR, RO.

Only a few EU Member States have enacted specific 'identity-related crime' or 'identity theft' legislation. According to our research, at the time when the report was prepared, these are Estonia, France, Poland and Slovenia.

The absence of specific legislation on identity theft does, however, not mean that identity theft is not criminalised in the Member States whose laws do not refer to the identity-related element of the act concerned. Most of the other Member States
National Perspectives & Existing Measures to Combat Identity Theft

Instead use legal provisions on fraud or forgery and thus do not commonly refer to identity “theft”, but rather to “fraud” or other types of crime committed using stolen identity information. Furthermore, the “mere theft” of an identity or identity information is not always considered a crime, but rather it is the use made of the identity acquired illegitimately that takes the conduct into the criminal area. In this way, identity theft is considered as a method for committing another crime and not as an act that is criminalised “on its own merit”. Overall, according to the RAND report, most national legal frameworks in the EU are “sufficiently comprehensive” to cover cases of identity theft and related crime even though specific legislation is not in place.

5.5.2 Extent to which primary and secondary victims are covered by national legislation

The extent to which primary and secondary victims are covered by national legislation was, however, not assessed systematically in the 2011 RAND report. This is an important issue, not the least with regard to the types of situations where a victim can be identified on the basis of existing legislation: if national legislation does not, for example, cover the act of acquiring identity information without a further crime being committed with this information, it is not possible to speak about victims in the sense of the law. As a consequence, this group of “potential” (primary) victims would also not be covered by the recently proposed Directive on the protection of victims, since the application of this Directive will depend on whether the person is legally recognised as a victim.

According to the results of a CSES questionnaire that was circulated the Member States as part of the present assignment, out of eighteen responses:

- Only three Member States (Czech Republic, Italy and Ireland) indicated that the primary victim of identity theft is covered by legislation even though the identity information acquired by unauthorised means has not yet been used in a criminal offence itself.

- Another eight countries (Austria, Bulgaria, Estonia, the Netherlands, Poland, Slovakia, Spain and United Kingdom) referred to some possibilities to obtain redress.

- This said, the answers to questions concerning the types of actions that are covered in national legislation suggest that the situation in different EU Member States is more nuanced than suggested by the answers to the question of whether legislation exists or not. For example, gaining access to the victim’s computer

184 As noted elsewhere, distinction can thus be made between primary victims (i.e. persons, whose identity is “stolen”) and secondary victims (e.g. persons that are defrauded by means of the identity information that had been acquired from the primary victim). The secondary act (i.e. the use of the identity information for various types of criminal acts) would in many cases be a criminal act regardless of whether identity information was being abused to commit it or not.
National Perspectives & Existing Measures to Combat Identity Theft

and/or bank accounts is covered in most of the Member States that have answered the survey.  

Generally it can be stated that in the majority of Member States that have replied to the survey, the matter of whether or not the person affected by "identity theft" is to be considered an aggrieved person depends on whether his/her rights, objects of legal protection, or legally recognised interests have been directly compromised by the injurious act. In such cases, the primary victim of identity theft can benefit from victims' rights that are stipulated in the legislation.

5.5.3 Effectiveness of national legislation in combating identity theft

A relatively low proportion of the respondents to the wider CSES survey consider existing national legislation to be effective in combating identity theft. Indeed, the views are divided: there are no major differences between respondents from those countries that do or do not have specific legislation on identity theft. This means that the survey results could suggest that the effectiveness of legislation is not linked to whether identity theft is a specific crime or not. However, it could be that some of the answers to the survey may also be linked to the effectiveness of the enforcement of existing legislation – or even the degree to which enforcement takes place at all – depending on how the question has been interpreted by the respondents. Therefore, some caution should be exercised with regard to the conclusions that can be drawn.

Those countries that have recently amended their criminal law to respond more effectively to identity-related crime must, however, be presumed to have done so, whether in answer to public or political pressure or to meet the concerns of police or law enforcement agencies, in order to remedy gaps that existed in their criminal statutes.

What is less clear, and what indeed may be doubted from the contributions made at the expert groups and the responses to our online survey, is that Member States that have not amended their criminal law to deal with any perceived gaps in connection with identity-related activities are completely satisfied that their laws adequately meet the challenges posed by the general phenomenon under discussion. While the RAND study reached the somewhat reassuring conclusion that "the need for new criminalising regulations is not evident" on the basis that Member States' existing laws 'may well prove to be adequate to address identity theft in practice', the study nonetheless acknowledged both that the absence of a uniform approach meant that the same behaviour might be legal in some Member States but not others, and that

Furthermore, as concerns the link between secondary crime and primary victims, out of the fifteen countries that replied to the CSES questionnaire, only Croatia and Romania stated that they do not provide legal rights and benefits to primary victims when a secondary crime has effects on them. This answer was also given by Ireland, where primary victims are, on the other hand, stated to be covered independently of whether a secondary crime has been carried out or not. In the other twelve Member States primary victims are considered a victim of the secondary crime (for example fraud, an offence and conceal of the true identity of the perpetrator, or further criminal offences) as well.
National Perspectives & Existing Measures to Combat Identity Theft

gaps might exist in different states' legislation depending on how broadly or narrowly identity theft is defined.

As concerns potential problems caused by the differences between the national legal frameworks, while a vast majority of stakeholders have pointed out that a common definition of identity theft would be useful, only anecdotal evidence exists as to why a common definition would be needed other than to improve the availability of data concerning the nature and scale of the problem. Problems that have been identified in cross-border collaboration are generally not stated to result from a lack of a common definition, but other challenges, including e.g. getting access to evidence as well as extensive bureaucracy and formalities that need to be complied with in international cases. Furthermore, as noted above, national legislation seems to cover most cases of identity theft and be sufficiently comprehensive in the vast majority of countries, as assessed in the RAND study from 2011. Some stakeholders have, however, pointed to a problem of "identity shopping", whereby criminals chose to base themselves in countries with less rigid legislation. However, only anecdotal information is available and this problem has not been possible to verify when examining links with penalties and legislation in place.

5.5.4 National measures to prevent identity theft

Prevention is critical to reducing the number of cases. According to the results of the online survey, more than 50% believe that more than 50% of the cases can be prevented if data subjects were more careful. In this regard, it can be noted that EU level action in terms of prevention by means of e.g. making electronic identification systems safer are already ongoing and seems to be key. National and EU institutions make continuous efforts to improve the security features of identification systems, as a way to combat identity thefts and fraud, e.g. through the use of biometric data for identification purposes.

Secure identity management to identify, authenticate and authorise users of a given system both in the physical and online world is imperative to prevent the problem of identity theft. This is a process that involves public as well as private actors, both in terms of issuing identification documentation and with regard to the authentication process. Despite the increasing security features of identification systems, there are many ways to frustrate number verifications – some of which have been pointed out above. The importance of proactive action to ensure the security of identity management systems is recognised by public authorities as well as by the private sectors, and as reflected above, action is being taken at the EU and national levels, and also by the private sector.

A lack of care of data subjects and controllers also impact on the magnitude of the problem. Both individuals and staff from the public and private sectors engage in risky behaviour, which may lead to that criminals are able to "steal" identity information. Lack of awareness may explain why victims of identity theft have displayed various forms of risky behaviour in terms of answering phishing emails, and
National Perspectives & Existing Measures to Combat Identity Theft

providing and posting personal information online. Furthermore, an increasing amount of personal information, including identity information, is made available online. This information may be subject to abuse. According to the stakeholder consultations carried out as part of the present assignment, one of the key measures to be taken to address this problem is to reduce the risk behaviour by individuals, businesses and public institutions.

5.5.5 National measures to assist victims of identity theft

Finally, it can be noted that on the Member States have put a number of measures in place to assist victims of identity theft, collect information about the problem and raise awareness, including:

- Specific reporting point (4 Member States): IE, NL, RO, UK;
- Dedicated online portal for identity-related crimes (2 Member States): NL, UK and for all crimes (11 Member States): AT, BE, BG, FI, GR, IT, LT, LV, MT, NL, UK.
- Offline portal for all crimes (2 Member States): EE, PT and for all crimes as well as specifically for identity theft (one Member State): IE;
- Portal with feedback on cases (one Member State): NL; and
- Public awareness campaign (9 Member States): LU, SE, BE, EE, FR, DE, NL, UK, GR.

While the Member States are working also on improving the access to redress, it can be noted that only one Member State has a reporting mechanism in place that covers identity theft specifically as well as other crimes, plus a feedback mechanism, namely the Netherlands. Overall, research shows that most Member States do not have a clear division of responsibilities relating to victims and that limited reporting systems are in place, although cases may of course be reported to the police when a crime has been committed. Indeed, almost half of the Member States do not have any reporting mechanisms other than turning to the police and where reporting mechanisms are in place, their functionality is limited.

5.5.6 Overall conclusions – National Perspectives and Existing Measures

Overall, therefore, it can be concluded that whilst existing national legislation enables the problem of identity theft to be tackled in most countries, there are shortcomings, particularly in relation to the transnational dimension, that cannot be tackled by Member States on their own.

Below we have summarised the main conclusions with regard to the five questions that are provided in the Impact Assessment Guidelines, which serve to guide the assessment
National Perspectives & Existing Measures to Combat Identity Theft

of whether the subsidiarity principle is respected or not. Two of the questions are treated together:

1. Does the issue being addressed have transnational aspects which cannot be dealt with satisfactorily by action by Member States?

Based on the research carried out, it can be concluded that identity theft is a transnational problem where in the majority cases the perpetrator and victim are not located in the same country. More than two thirds of the respondents to the CSES survey stated that there is a quite significant or very significant cross-border dimension. In many cases more than two countries are involved. Indeed, according to the CSES survey with experts in the area, one third of the cases can be estimated to involve either two or three EU27 Member States with a significantly higher proportion – just over half of cases – involving countries outside Europe. Hence, in many cases, the problem is not restricted to the EU, but non-EU countries are also involved. A disproportionate number of perpetrators were, in the survey, indicated to be based in and the proceeds of identity theft go to countries mainly outside of the EU, although a few EU Member States were mentioned by the respondents. These were Romania, Spain, UK, “Eastern Europe”, France, Italy and Poland.

When considering the types of criminal offences for which identity theft is used, several of the crimes, such as smuggling of people and illegal migration, are inherently transnational. There is also a strong transnational component in money laundering. On the other hand, a few of the criminal offences identified, such as stalking, bullying and harassment are rather carried out within individual countries, although this may not always be the case. Damage reputation may be a direct aim, but also a result of the acquisition of identity information e.g. from companies. Fraud may or may not have international elements. It can further be noted that identity-related information is used as an enabler for other criminal purposes.

Cross-border collaboration between LEAs is necessary to deal with identity theft cases. Hence, it is clear that identity theft and related crime are a multilevel and multistate phenomenon. Action by individual Member States can therefore be deemed as inadequate to address the identified problems; cross-border collaboration is necessary.

2. Would actions by Member States alone, or the lack of Community action, conflict with the requirements of the Treaty?

A number of the crimes for which identity theft is being used as evidenced from our research are serious crimes with a clear cross-border dimension in relation to which the EU may act where there is a special need to combat them on a common basis (Article 83(1)). This includes terrorism, trafficking, money laundering etc.

Furthermore, although influenced by the precise definition used, identity theft has a number of implications for fundamental rights, as established in the Charter of Fundamental Rights of the European Union. The rights set out in the following Articles are, in addition to the Articles in the Chapter 3 on Equality, particularly affected:

National Perspectives & Existing Measures
to Combat Identity Theft

- **Right to liberty and security** (Art. 6): Identity theft and related crime have a negative impact on the security of EU citizens.

- **Respect for private and family life (Art. 7) and protection of personal data** (Art. 8): Identity theft and related crime implies the abuse of personal identity data and a lack of respect for private life. Thus, in order to safeguard these rights, it is imperative to combat identity theft as well as related crime.

- **Right to property** (Art. 17): This right is directly affected where property is the target of the related (secondary) crime. In relation to primary victims, this Article can also be interpreted to cover identity documentation and other (physical) sources containing identity information.

- **Consumer protection** (Art. 38): Identity information may be acquired and abused in relation to online shopping, as well as shopping in the offline world and thus have a negative impact on consumer protection.

- **Right to an effective remedy and to a fair trial** (Art. 47): This right is closely related to the protection of victims, who according to this Article have a right to an effective remedy.

Hence, insufficient action to address the problem conflicts with the requirements of the Treaty.

Would actions by Member States alone, or the lack of Community action, significantly damage the interests of Member States? Would action at Community level produce clear benefits compared with action at the level of Member States by reason of its scale?

Common action would produce clear benefits compared to action by the Member States not only because of the cross-border dimension of the problem, but also by reason of its scale. Because of the reason of its scale and negative impacts on individuals, business, public authorities and the overall economy, the interests of the Member States would be significantly damaged in a situation where the EU would not act.

More specifically, our research suggests that identity theft and identity-related crime affects a considerable proportion of the population, and the problem is increasing. Our mid-range estimate suggests that as many as 8.2 million individuals are affected by identity theft (2% of the EU’s population) with an average loss of around €2,500 or €20bn at the EU level. There are also indirect financial costs of identity theft arising from damage to an individual’s credit rating, the cost of rectifying the consequences of identity theft (e.g. replacing documents), as well as non-financial impacts of an adverse nature such as stress and reputational damage. Fundamental rights issues are also relevant. Bearing in mind that some identity theft goes undetected or is not made known for statistical purposes, this estimate is likely to be on the low side.

Our estimate is that business losses could be as high as €500bn or 0.4% of EU GDP.
National Perspectives & Existing Measures to Combat Identity Theft

Public authorities can also be victims of identity theft when their means of identification are used by someone else. This could be done via illegal access to data bases, the forgery of official documents etc. Similar to businesses, public authorities are also used as a source of information to access personal data of data subjects, including staff and clients.

Ultimately, these effects will impact on the extent to which the European area of justice, freedom and security can be realised.

Would action at Community level produce clear benefits compared with action at the level of Member States by reason of its effectiveness?

Action at Community level is likely to be more effective than action at national level because of the transnational dimension of the problem. The problem is not restricted to a limited number of Member States, but spans over the entire EU. Therefore, action by individual Member States is unlikely to be equally effective as action at the EU level, where the problem can be better addressed across the EU.

With regard to the legal base for common legislative action, Article 83 in Chapter 4 of the Treaty on the Functioning of the European Union concerning judicial cooperation in criminal matters establishes the situations where Directives on criminal offences may be adopted:

<table>
<thead>
<tr>
<th>Article 83 (1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>The European Parliament and the Council may, by means of directives adopted in accordance with the ordinary legislative procedure, establish minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension resulting from the nature or impact of such offences or from a special need to combat them on a common basis.</td>
</tr>
<tr>
<td>These areas of crime are the following: terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime and organised crime.</td>
</tr>
<tr>
<td>On the basis of developments in crime, the Council may adopt a decision identifying other areas of crime that meet the criteria specified in this paragraph. It shall act unanimously after obtaining the consent of the European Parliament.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Article 83 (2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>If the approximation of criminal laws and regulations of the Member States proves essential to ensure the effective implementation of a Union policy in an area which has been subject to harmonisation measures, directives may establish minimum rules with regard to the definition of criminal offences and sanctions in the area concerned. Such directives shall be adopted by the same ordinary or special legislative procedure as was followed for the adoption of the harmonisation measures in question, without prejudice to Article 76.</td>
</tr>
</tbody>
</table>

Policy Objectives and Policy Options

This section first summarises the policy objectives that would underpin any initiative at the EU level to help combat identity theft. Next, we present the intervention logic for action in this area, followed by a presentation of the policy options.

6.1 Definition of Policy Objectives

Below we set out the policy objectives that have been identified based on the problem assessment. The general and specific objectives are defined as follows:

<table>
<thead>
<tr>
<th>General objectives</th>
<th>Specific objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>To combat identity theft and identity-related crime</td>
<td>• To reduce identity theft and related crime.</td>
</tr>
<tr>
<td></td>
<td>• To improve the capacity to prevent and tackle identity theft and related crime both in the public</td>
</tr>
<tr>
<td></td>
<td>and private sectors, including in relation to cross-border aspects of the problem, at national and</td>
</tr>
<tr>
<td></td>
<td>EU level.</td>
</tr>
<tr>
<td></td>
<td>• To ensure that primary and secondary victims of identity-related crime obtain support and redress.</td>
</tr>
<tr>
<td></td>
<td>• More generally, to safeguard fundamental rights, including in particular:</td>
</tr>
<tr>
<td></td>
<td>- Right to liberty and security (Art. 6);</td>
</tr>
<tr>
<td></td>
<td>- Respect for private and family life (Art. 7) and protection of personal data (Art. 8);</td>
</tr>
<tr>
<td></td>
<td>- Right to property (Art. 17);</td>
</tr>
<tr>
<td></td>
<td>- To protect consumers (Art. 38), whose identity information may be acquired and abused in relation</td>
</tr>
<tr>
<td></td>
<td>to online shopping, as well as shopping in the offline world and thus have a negative impact on</td>
</tr>
<tr>
<td></td>
<td>consumer protection. This is also a fundamental right.</td>
</tr>
<tr>
<td></td>
<td>- Right to an effective remedy and to a fair trial (Art. 47)</td>
</tr>
<tr>
<td></td>
<td>• To protect business, in particular SMEs which tend to be more vulnerable to identity theft and its</td>
</tr>
<tr>
<td></td>
<td>consequences than larger firms.</td>
</tr>
<tr>
<td></td>
<td>• To improve the knowledge base regarding identity theft and related crime.</td>
</tr>
<tr>
<td></td>
<td>• To prevent the risk of forum shopping in relation to identity theft and related crime in the EU.</td>
</tr>
</tbody>
</table>

In a more general sense, the objective of any EU intervention is to add value to national initiatives to combat identity theft. As noted in Section 3, EU Member States already

---

*Operational objectives will be identified for each of the policy options. The link between the policy options and the objectives is examined in the section on the impacts of the options in achieving the policy objectives (see section 6).*
Policy Objectives and Policy Options

have legislation in place to tackle many of the consequences of identity theft. However, given the cross-border nature of the problem, and the fact that many aspects stem from use of the Internet which is global in nature, an EU-wide response to the phenomenon is essential to supporting national efforts.

6.2 Intervention Logic

The diagram below sets out the broader framework for assessing the case for EU intervention, i.e. going beyond the diagrammatic portrayal of the identity theft problem and its drivers (Figure 3.1 in Section 3) and showing how possible actions at an EU level could help tackle the problem. The intervention logic takes account of the findings of the problem assessment and provides an overall framework linking the problem definition to the policy objectives and then to policy options and their effects.

Figure 6.1: Overview of Intervention Logic

In the above diagram, the ‘intervention logic’ for possible EU action is defined in relation to various factors:

- **Relevance** – how relevant the objectives of EU intervention are to the problem that has been identified;
- **Efficiency** – the extent to which outcomes are proportionate to the various inputs;
Policy Objectives and Policy Options

- **Effectiveness** – to what degree the specific and general objectives of EU intervention/specific policy options are achieved through the outcomes;

- **Impacts and added value** – effect on key target groups (e.g. individuals, businesses) and added value, i.e. the difference between this and what would have happened without intervention. From a different perspective, added value is what is achieved through EU intervention that could not have been achieved by Member States cooperating bilaterally.

These factors provide part of the framework used later to evaluate and compare the impacts of different policy options.

In the above diagram a distinction is made between outputs, results and impacts. ‘Outputs’ in this context are the activities that should result from EU intervention (e.g. more networking between Member States to share information on identity theft) whilst ‘results’ are the intermediate outcomes (e.g. more effective prevention) that lead to impacts on the problem (in this case, reduced identity theft).

The above framework has been used as a basis for developing the policy options that are described in the next section.

### 6.3 Overview – Policy Options

The Commission’s Impact Assessment Guidelines[^1] specify a range of policy options that need to be considered in an Impact Assessment, including the following:

- No action (Status Quo);
- Discontinuing current EU action;
- EU non-legislative action (e.g. Recommendation, Communication, Awareness Raising Campaign, Funding Programme); and
- EU legislative action (e.g. Regulation, Directive).

As concerns the relevance of these different types of options for the present assignment, it can be noted that a Regulation is outside the scope of action the Commission could take. However, the Terms of Reference included a list of the types of policy options to be considered. Based on this list and additional research and consultations, the following policy options have been identified in response to the current problems:

## Policy Objectives and Policy Options

### Table 6.2: Overview of policy options

<table>
<thead>
<tr>
<th>Policy Option</th>
<th>Sub-Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Option 1:</td>
<td></td>
</tr>
<tr>
<td>Status Quo</td>
<td>None</td>
</tr>
<tr>
<td><strong>Policy Option 2:</strong></td>
<td></td>
</tr>
<tr>
<td>Non-legislative Action to Help</td>
<td>• Policy Option 2.1: Sharing of experience and knowledge concerning the</td>
</tr>
<tr>
<td>Combat Identity Theft</td>
<td>problem of identity theft via an electronic platform.</td>
</tr>
<tr>
<td></td>
<td>• Policy Option 2.2: Establishment of a network of national contact points,</td>
</tr>
<tr>
<td></td>
<td>which would be tasked with running, in each Member State, a one stop shop</td>
</tr>
<tr>
<td></td>
<td>for victims of identity theft, act as a monitoring body and organise</td>
</tr>
<tr>
<td></td>
<td>awareness raising activities.</td>
</tr>
<tr>
<td></td>
<td>• Policy Option 2.3: Commission Recommendation on a common definition,</td>
</tr>
<tr>
<td></td>
<td>establishment of reporting mechanisms for victims, collection of</td>
</tr>
<tr>
<td></td>
<td>information on the problem of identity theft and related crime and the</td>
</tr>
<tr>
<td></td>
<td>organisation of EU-supported awareness raising campaigns.</td>
</tr>
<tr>
<td></td>
<td>• Policy Option 2.4: Combination of non-legislative policy options 2.1 and</td>
</tr>
<tr>
<td></td>
<td>2.2.</td>
</tr>
<tr>
<td></td>
<td>• Policy Option 2.5: Combination of non-legislative policy options 2.1, 2.2</td>
</tr>
<tr>
<td></td>
<td>and 2.3.</td>
</tr>
<tr>
<td><strong>Policy Option 3:</strong></td>
<td></td>
</tr>
<tr>
<td>Legislative Action to Help</td>
<td></td>
</tr>
<tr>
<td>Combat Identity Theft</td>
<td>• Policy Option 3.1: Adoption of a Directive on identity theft, focusing on</td>
</tr>
<tr>
<td></td>
<td>primary victims (minimalistic approach)</td>
</tr>
<tr>
<td></td>
<td>• Policy Option 3.2: Adoption of a Directive on identity theft and related</td>
</tr>
<tr>
<td></td>
<td>crime, i.e. including both primary and secondary victims (maximalist</td>
</tr>
<tr>
<td></td>
<td>approach)</td>
</tr>
<tr>
<td><strong>Policy Option 4:</strong></td>
<td>Combination of Policy Option 2 (including all three sub-options) and</td>
</tr>
<tr>
<td>Combined Action</td>
<td>Policy Option 3.1: Adoption of a Directive on identity theft (minimalistic</td>
</tr>
<tr>
<td></td>
<td>approach).</td>
</tr>
</tbody>
</table>

It should be noted that emphasis has been placed on identifying options that do not concern prevention (it has been agreed with the Commission that while prevention should be considered as an option or as part of a package, it should not be the central focus). As concerns the content of the two legislative options (3.1 and 3.2) it can be noted that whilst in theory possible, adopting a definition without criminalising this offence has been discarded as it would not make sense in practical terms.

When defining the policy options, the proportionality principle has been taken into account. The Impact Assessment Guidelines include seven questions[^190], which were used to guide this assessment. In relation to the proportionality principle, under this rule, the involvement of the institutions must be limited to what is necessary to achieve the

[^190]: Including e.g. whether the option goes beyond what is necessary to achieve the objective satisfactory, and if the form of Community action (choice of instrument) is as simple as possible, and coherent with satisfactory achievement of the objective and effective enforcement.
Policy Objectives and Policy Options

objectives of the Treaties. In other words, the content and form of the action must be in keeping with the aim pursued. To this can be added the need to ensure that the action is also proportionate to the problem in terms of the resources needed for its implementation.

As concerns the assessment concerning whether the proportionality principle is respected or not, distinction can be made between the legislative and the non-legislative policy options. The non-legislative policy options clearly respect the proportionality principle to the greatest extent insofar as they involve relatively straightforward interventions that largely build on existing legislation and practices rather than (as with Policy Option 3) requiring a new initiative at the EU level. Thus, assuming the foreseen interventions is effective in tackling the problem of identity theft and related criminal activities, this would be achieved with measures that are quite limited in scope and in terms of the financial and other resources needed for their implementation.

Of the two legislative policy options, the minimalist version addresses a legislative gap concerning primary victims in many Member States. The maximalist option would in addition involve intervention with existing national legislation on secondary crime. In terms of proportionality, these policy options are more ambitious and would require a much more substantial commitment of resources at the EU and Member State levels for their implementation. That said, given the scale of identity theft, and the likelihood that it will continue to grow, the legislative option is still not disproportionate to the problem.

Below we set out a more detailed qualitative description of each of the policy options. More specifically, for each of the options described above, the following aspects are considered: the rationale for considering the policy option; type of instrument; content and scope; timeframe for implementation; and coherence with other EU initiatives.

6.4 Policy Option 1: Status Quo

Under this policy option, there would be no new intervention at the EU level. The Commission would continue current action, e.g. funding of expert meetings, including planned actions, but not take any new initiatives.

<table>
<thead>
<tr>
<th>Elements</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rationale</td>
<td>The status quo policy option should always be considered, since the other options are compared against the baseline (no further EU action).</td>
</tr>
<tr>
<td>Type of instrument</td>
<td>n/a (no new EU action).</td>
</tr>
<tr>
<td>Content</td>
<td>• Existing and planned initiatives at the EU and national levels in the field of identity theft, identity management systems and cybercrime.</td>
</tr>
</tbody>
</table>
### Policy Objectives and Policy Options

<table>
<thead>
<tr>
<th>Elements</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Two of the key initiatives from 2012 are:</td>
<td></td>
</tr>
<tr>
<td>- Proposal for a <strong>European Cybercrime Centre (EC3)</strong>, whose aims are to help protect European citizens and businesses against the increased cyber-threats by: Improving the evaluation and monitoring of existing preventative and investigative measures; Supporting the development of training for the criminal justice community across the Member States; and establishing co-operation between all stakeholders involved in combating cybercrime.</td>
<td></td>
</tr>
<tr>
<td>- Proposal for a <strong>Directive establishing minimum standards on the rights, support and protection of victims of crime</strong>. Notably, Art. 8 of the Directive stipulates that Member States shall ensure that victims, in accordance with their needs, have access to confidential victim support services, free of charge, acting in the interests of the victims before, during and for an appropriate time after criminal proceedings. Family members shall also have access to victim support services in accordance with their needs and the degree of harm suffered. Furthermore, the Member States shall promote the establishment of specialist support services in addition to general victim support services. The Member States are also to facilitate the referral of victims to victim support services. Access to any victim support services shall not be dependent on a victim making a formal complaint.</td>
<td></td>
</tr>
<tr>
<td>- Other relevant recent initiatives include, for example:</td>
<td></td>
</tr>
<tr>
<td>- Revision of the eSignature Directive (1999/93/EC) and a Decision of the European Parliament and Council on the mutual recognition of e-Identification and e-Authentication should be carried out.</td>
<td></td>
</tr>
<tr>
<td>- Large-Scale Project for the establishment of a European eID Interoperability Platform named STORK (launched in 2008).</td>
<td></td>
</tr>
<tr>
<td>- Revision of the Framework Decision on Attacks against Information Systems</td>
<td></td>
</tr>
<tr>
<td>- Proposal for an Internal Security Fund to support the implementation of the five strategic objectives established in the Internal Security Strategy: Disrupting international crime networks; Preventing terrorism and addressing radicalisation and recruitment; Raising the levels of security for citizens and businesses in cyberspace; Strengthening security through border management; and Increasing Europe’s resilience to crises and disasters.</td>
<td></td>
</tr>
<tr>
<td>- Proposal on the 8th FP.</td>
<td></td>
</tr>
<tr>
<td>- Work on a European Strategy for Internet Security to ensure a safe, secure and resilient digital environment to all EU citizens, businesses and public authorities.</td>
<td></td>
</tr>
</tbody>
</table>
Policy Objectives and Policy Options

<table>
<thead>
<tr>
<th>Elements</th>
<th>Description</th>
</tr>
</thead>
</table>
|                              | - Technical specifications for the introduction of biometric identifiers (fingerprints) into the passport and other travel documents.  
|                              |  
|                              | • A more extensive summary, including earlier initiatives, is provided in Appendix D.                                                                                                                     |
| Scope                        | Focus is placed on preventative measures in the framework of DG CONNECT initiatives. Identity theft and related crime may be covered as part of the wider horizontal instruments on cybercrime within the remit of DG HOME and not be addressed as a specific instrument. |
| Timeframe                    | n/a                                                                                                                                                                                                        |
| Coherence with other EU initiatives | n/a                                                                                                                                                                                                     |

6.5 Policy Option 2: Non-legislative EU action

The following three non-legislative policy options have been identified in the course of the assignment:

Policy Option 2.1: Sharing of experience and knowledge concerning the problem of identity theft via an electronic platform. This policy option would allow for real time communication between law enforcement authorities by means of an electronic platform. The electronic platform would also have two more static parts. One part would provide information to citizens concerning risks, contact points and reporting mechanisms in the different Member States, while the other part would serve as an electronic public library, where reports concerning the problem of identity theft and related crime could be uploaded.

Policy Option 2.2: Establishment of a network of national contact points, which would be tasked with running, in each Member State, a one stop shop for victims of identity theft, act as a monitoring body and organise awareness raising activities. Policy Option 2.2 would imply the establishment of a EU27 network of experts or ‘contact points’ at the operational level, which would provide support to victims and act as a monitoring body. Furthermore, the option would allow for information exchanges through face to face meetings between law enforcement authorities and other actors (including from the private sector and from third countries) on specific topics that would be identified by the network. The actors that would be gathered would be determined on a case by case basis. Working Groups would be tasked with the preparation of these meetings. Best practices would also be identified. The network would in addition convene on a regular basis (e.g. four times per year).
Policy Objectives and Policy Options

A difference between Policy Options 2.2 and 2.1 is that Policy Option 2.1 would involve a component of awareness-raising via a dedicated section on the platform concerning (e.g. rights, contact points and risks). Policy Option 2.2 does not involve any actions directed at individuals. EU funding would need to be provided to implement both Policy Options 2.1 and 2.2.

Policy Option 2.3: EU Recommendation on a common definition, establishment of reporting mechanisms for victims, collection of information on the problem of identity theft and related crime and the organisation of awareness raising campaigns. Policy Option 2.3 would take the form of a Commission Recommendation to encourage the Member States to on the one hand adopt a more harmonised approach by introducing a common definition of identity theft, and on the other hand step up the fight against identity theft and related crime. This would include the establishment of reporting mechanisms for victims based on best practice and collection of data to improve the knowledge base about the problem of identity theft and related crime.

Policy Option 2.3 is different from Policy Options 2.1 and 2.2 as it in practice is “one step short” of a legislative proposal. More specifically, by means of a Recommendation, it would encourage harmonisation by suggesting a common definition of identity theft as well as the establishment of reporting mechanisms for victims. Collection of data to improve the knowledge base would also be encouraged.

Policy Option 2.4 – policy options 2.1 and 2.2 are combined:

- Policy Option 2.1: Sharing of experience and knowledge concerning the problem of identity theft via an electronic platform; and
- Policy Option 2.2 Establishment of a network of national contact points, which would be tasked with running, in each Member State, a one stop shop for victims of identity theft, act as a monitoring body and organise awareness raising activities.

Policy Option 2.5 - all of the individual non-legislative options (2.1, 2.2 and 2.3) are combined into one non-legislative option.

The content of each of the individual policy options (2.1, 2.2 and 2.3) is described in more detail below. Policy options 2.4 and 2.5 are not described as they consist of different combinations of the individual non-legislative options.
Policy Objectives and Policy Options

Policy Option 2.1 – Sharing of experience and knowledge concerning the problem of identity theft via an electronic platform

<table>
<thead>
<tr>
<th>Elements</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rationale</td>
<td>The limited awareness of the extent of identity theft and how to best deal with these issues, as well as the insufficient information for victims of identity theft on risk behaviour and preventative action that can be taken by individuals.</td>
</tr>
<tr>
<td>Content</td>
<td>Policy Option 2.1 would involve setting up an online platform to share information on identity theft and to promote networking. The website/platform could be divided into three main parts:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Part 1</strong> – for individuals, where contact details to reporting mechanisms are provided for the Member States, information on legislation in place would be provided in an easily understandable format (examples of cases could be provided) as well as information on risks and preventative action that can be taken. This part of the website would be open to all.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Part 2</strong> – for experts and/or law enforcement authorities, where legislation would be provided with a more technical focus, as well as information on relevant actors working in the field in the Member States and a closed community for sharing information real time and good practices would be established. Information could also be shared on risks. This section could be based on registration.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Part 3</strong> – with public reports containing statistics etc. It would be possible to upload reports etc. and thereby create an online knowledge centre.</td>
</tr>
<tr>
<td>Scope</td>
<td>• Since a common definition of identity theft would not be in place, the information that is made available on the portal is likely to be rather broad and dependent on national approaches to tackle the problem of identity theft and related crime. Information could be uploaded in all official EU languages.</td>
</tr>
<tr>
<td></td>
<td>• The platform would primarily target individuals as well as experts and/or law enforcement authorities in the EU. However, all stakeholders would be able to benefit from the public library (Part 3 above).</td>
</tr>
<tr>
<td></td>
<td>• If a separate portal would be set up, the role of the Commission would involve funding and procuring the website and the content management, including managing the relations with the contractor (see below). For this purpose, a Steering Group could be set up, which could involve a limited number of relevant actors at the EU level, including e.g., a representative of the EC3, Europol, Eurojust etc., as well as from the academia and business side.</td>
</tr>
<tr>
<td></td>
<td>• If the Platform is established on the eJustice Portal, a similar structure would be set up, but the work of the external contractor would be focused on the content management.</td>
</tr>
</tbody>
</table>
Policy Objectives and Policy Options

<table>
<thead>
<tr>
<th>Elements</th>
<th>Description</th>
</tr>
</thead>
</table>
| Timeframe for implementation | • In terms of the separate Platform, it is expected that it would take approximately six months to one year to set up the platform. If managed by an external contractor, the platform would then run for a (renewable) period of 3 years with a review at that point and possible retendering.  
• If the Platform is established on the eJustice Portal, it is expected that it would take up to six months to finalise the content and functionalities of the Portal. |
| Coherence with other EU initiatives | • In addition to the eJustice Portal, there are in particular links with the European Cybercrime Centre (EC3) and the Directive establishing minimum standards on the rights, support and protection of victims of crime:  
  • The European Cybercrime Centre: One objective of the EC3 is to improve the evaluation and monitoring of existing preventative and investigative measures. The information gathered on the public library and the relevant analyses carried out on this basis could inform the work by the EC3. Under policy option 2.1, an online cooperation mechanism focusing on experts and LEAs in the field of identity theft would also be set up, which would contribute to the objectives of the EC3 to establish co-operation between all stakeholders involved in combating cybercrime and capacity building. The collaboration established under policy option 2.1 could be further strengthened under the umbrella of the EC3, e.g. through face to face meetings. Overlaps between the activities carried out within the framework of policy option 2.1 and the EC3 would be avoided through the involvement of the EC3 in the Steering Group for the platform.  
  • Directive establishing minimum standards on the rights, support and protection of victims of crime. Under the Directive, the Member States are to facilitate the referral of victims to victim support services. The provision of information to victims of relevant victim support structures in each Member State would be relevant in this regard and thereby facilitate the implementation of the Directive. |

Policy Option 2.2 – Establishment of a network of national contact points, which would be tasked with running, in each Member State, a one stop shop for victims of identity theft, act as a monitoring body and organise awareness raising activities

<table>
<thead>
<tr>
<th>Elements</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rationale</td>
<td>Insufficient support to victims of identity theft; the lack of (a forum for) communication and sharing of best practices on how to combat identity theft and related crime between various stakeholders; and the limited awareness of the extent of identity theft and how to best deal with these issues.</td>
</tr>
</tbody>
</table>
## Policy Objectives and Policy Options

<table>
<thead>
<tr>
<th>Elements</th>
<th>Description</th>
</tr>
</thead>
</table>
| Content  | A network of contact points would be established. The contact points would have the three-fold role of providing support to victims (serve as “one stop shops”), collect information concerning the problem of identity theft and measures taken in the relevant Member State to address the current challenges and awareness raising on the basis of this work. In order to ensure added value, EU level meetings would be held, which would allow the members of the network in different Member States to meet and share information and knowhow. More specifically, the contact points, which would meet on a regular basis (e.g. four times per year), would:  
  - Identify topics for information sharing and knowledge gathering, including on best practices, as well as the relevant stakeholders to involve.  
  - Working Groups would be created for the purpose of the preparation of these sessions.  
  - On this basis, face to face information exchanges and awareness raising campaigns targeting law enforcement authorities and the judiciary could be organised concerning e.g.: existing legislation; best practices in dealing with cases of identity theft and identity-related crime; the need to protect and support victims of identity theft; and best practices in doing so etc.  
  - The network could also be tasked with the collection of information on identity theft and for the preparation of annual or biannual threat assessments for the Member States. |
Policy Objectives and Policy Options

<table>
<thead>
<tr>
<th>Elements</th>
<th>Description</th>
</tr>
</thead>
</table>
| Scope        | • A network of contact points in each Member State would be created. The network members would meet four times a year. Working Groups could be established to develop additional workshops and EU level meetings. There would be scope for involving actors from the private sector as well as actors from third countries in these initiatives. Best practices could be identified in relation to the dealing with cases of identity theft and information spread to practitioners. Awareness raising activities could involve the development of short brochures / papers on the various topics discussed in the workshops and be based on the best practices.  
• As concerns the support to victims, the role could involve providing information to victims about their rights, where and how to report the case etc. As part of this work, information concerning the contacts made by (potential) victims would also be collected in order to improve the information base.  
• It is role as a monitoring body, the contact points would be responsible for collecting information on the nature and extent of the problem of identity theft in the relevant Member State, as well as on measures taken to tackle the problem. In order to ensure EU added value and the smooth running of the network of contact points, the Commission could procure the management of the network to an external contractor. A similar Steering Group as is foreseen under policy option 2.1 could be established. |
| Timeframe    | The programme would run throughout the new programming period.                                                                                                                                                                                                                                                                               |
| Coherence with other EU initiatives | Similar to policy option 2.1, there are in particular links with the European Cybercrime Centre (EC3) and the Directive establishing minimum standards on the rights, support and protection of victims of crime:  
• The European Cybercrime Centre: Similar complementarities as those identified for policy option 2.1.  
• Directive establishing minimum standards on the rights, support and protection of victims of crime. Under the Directive, the Member States are to promote the establishment of specialist support services in addition to general victim support services. The establishment of one-stop shops for victims of identity theft under this policy option would facilitate the implementation of the Directive. |

### Policy Option 2.3: EU Recommendation on a common definition, establishment of reporting mechanisms for victims, collection of information on the problem of identity theft and related crime and the organisation of awareness raising campaigns

<table>
<thead>
<tr>
<th>Elements</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rationale</td>
<td>Problems in cross-border investigations due to the use of various types of legislation in the Member States to deal with the relevant crimes, limited awareness of the extent of identity theft and how to best deal with these issues, as well as inadequate support and redress for victims.</td>
</tr>
</tbody>
</table>
Policy Objectives and Policy Options

<table>
<thead>
<tr>
<th>Elements</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type of instrument</td>
<td>EU Recommendation</td>
</tr>
<tr>
<td>Content</td>
<td>In the Recommendation the Commission would encourage the Member States to:</td>
</tr>
<tr>
<td></td>
<td>• Adopt a common definition (covering both primary and secondary victims; to be defined in the Recommendation) or at least to ensure that all elements that are covered in the suggested definition are also covered in national legislation.</td>
</tr>
<tr>
<td></td>
<td>• Collect statistics and monitor the development of identity related crime, as well as the drivers for this.</td>
</tr>
<tr>
<td></td>
<td>• Provide a reporting mechanism for victims (this would also have the objective of increasing the available statistics) and to launch awareness raising campaigns on the risks and preventative action that could be taken by individuals, businesses and public authorities.</td>
</tr>
<tr>
<td></td>
<td>A network of national contact points would be established to help implement these provisions.</td>
</tr>
<tr>
<td>Scope</td>
<td>• The Recommendation would cover identity theft and related crime in the wide sense. The geographical scope would be the Member States.</td>
</tr>
<tr>
<td></td>
<td>• The scope would depend on the willingness of the Member States to take the recommended action.</td>
</tr>
<tr>
<td>Timeframe for implementation</td>
<td>• This would depend on the Commission’s priorities and ability to secure Member State agreement to the measures. As an indication, a timeframe of 1-2 years could be set as a target for adoption of the Recommendation.</td>
</tr>
<tr>
<td>Coherence with other EU initiatives</td>
<td>• Similar to those identified for options 2.1 and 2.2. The level of coherence would, however, be dependent on the actions by the Member States, since no EU-level coordination would be provided.</td>
</tr>
</tbody>
</table>

6.6 Policy Option 3: EU Legislative Action

The following legislative policy options have been developed:

- **Policy Option 3.1**: Adoption of a Directive on identity theft, focusing on primary victims (minimalistic approach); and

- **Policy Option 3.2**: Adoption of a Directive on identity theft and related crime (maximalist approach).

Definitions of identity theft and related crime have not been included in the report at this stage, but can be provided. The content of these two options is described below.
### Policy Objectives and Policy Options

#### Policy Option 3.1 – Adoption of a Directive on identity theft crime  
(minimalistic approach)

<table>
<thead>
<tr>
<th>Elements</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Rationale</strong></td>
<td>The lack of coverage of primary victims in national legislation and limited awareness of the extent of identity theft.</td>
</tr>
<tr>
<td><strong>Instrument</strong></td>
<td>EU Directive.</td>
</tr>
</tbody>
</table>
| **Content**               | • Under this policy option a Directive would be adopted, which would:  
  • Establish a common definition covering “primary victims”, i.e. those victims whose identity is “stolen”, and that identity theft is a criminal offence in the EU.  
  • Introduce a requirement to collect information concerning investigations, prosecutions and convictions relating to this new offence would also be established. In order to ensure that comparable data are compiled, more specific monitoring and reporting requirements could be set out. Data to be collected could, for example, include: number of reported cases, number of prosecutions, number of losses etc. Examples of cases could also be requested to be provided. Consequences for victims could also be reported on as well as the methods used. Annual reports should be submitted to the Commission by the Member States based on the information collected. These reports would be additional to general provisions on Member States reporting on transposition and COM reporting to Council and Parliament with a view to proposing more legislation. |
| **Scope**                 | The Directive would cover primary victims, thus it would be restricted to the act of the identity theft and not cover related crime. The geographical scope would be the EU.                                                                                                                                                                |
| **Timeframe for**         | • After adoption (see Policy Option 2.3 as a guide) and implementation of the Directive by the Member States, no time limit.                                                                                                                                                                                                                     |
| **Coherence with**        | • Currently, not all Member States have legislation in place concerning primary victims, implying that these therefore are not recognised as victims under the Directive establishing minimum standards on the rights, support and protection of victims of crime. The Identity Theft Directive would give further individuals access to the support provided in the framework of the Victims Directive.  
  • The information collected as part of the information requirements under the Directive could be used by the EC3, to the extent that they relate to cybercrime. |
| **other EU initiatives**  |                                                                                                                                                                                                                                                                                                                                             |
**Policy Objectives and Policy Options**

**Policy Option 3.2 – Adoption of a Directive on identity theft and related crime (maximalist approach)**

<table>
<thead>
<tr>
<th>Elements</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Rationale</strong></td>
<td>Lack of coverage of primary victims in national legislation and problems in cross-border investigations due to the use of various types of legislation in the Member States to deal with the relevant crimes, limited awareness of the extent of identity theft, as well as inadequate redress for victims.</td>
</tr>
<tr>
<td><strong>Instrument</strong></td>
<td>EU Directive.</td>
</tr>
</tbody>
</table>
| **Content**       | Under this option, a Directive – maximalist approach – would be established. The Directive would cover all elements that are set out above in relation to Policy Option 3.1. In addition, the following aspects would be covered:  
• Secondary victims (i.e. natural and legal persons who are e.g. defrauded through the use of a person’s identity information); and  
• Approximation in the level of penalties for not only identity theft (i.e. targeting primary victims) but also related, secondary crime. |
| **Scope**         | The Directive would cover both identity theft and related crime. The geographical scope would be the EU.                                    |
| **Timeframe for implementation** | After adoption and implementation of the Directive by the Member States, no time limit.                                                  |
| **Coherence with other EU initiatives** | See option 3.1.                                                                                                                             |

**6.7 Policy Option 4: Combined Action**

See descriptions of policy options 2.1, 2.2, 2.3 and 3.1 above.
This section provides our assessment of impact of the various policy options. The expected impacts have been rated in relation to the status quo. At the end of the section, the ratings of the policy options are compared.

7.1 Assessment Framework

As summarised in Section 6, the framework for assessing the impacts is structured around the following criteria\(^\text{191}\):

<table>
<thead>
<tr>
<th>Summary – Assessment Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>Relevance</strong> – the extent to which the different policy options are relevant to the problem;</td>
</tr>
<tr>
<td>• <strong>Effectiveness</strong> - the degree to which the policy options are capable of achieving the policy objectives;</td>
</tr>
<tr>
<td>• <strong>Efficiency</strong> - the input or effort required to achieve a given output, where the latter is determined by the policy objectives;</td>
</tr>
<tr>
<td>• <strong>Impacts on different societal groups</strong> - potentially affected by the policy options (e.g. individuals, businesses and households);</td>
</tr>
<tr>
<td>• <strong>Economic and financial impacts</strong> – i.e. the extent to which different policy options are likely to reduce the negative effects analysed in Section 4; and</td>
</tr>
<tr>
<td>• <strong>Feasibility</strong> - the feasibility of the policy options includes considerations of the practical feasibility in implementing the policy option, including the likely support from stakeholders as well as enforcement considerations.</td>
</tr>
</tbody>
</table>

A certain degree of relevance can be taken for granted given that the policy options have been defined after extensive consultations with key stakeholders.

The assessment of the **effectiveness and efficiency** of the policy options has been carried out with reference to the specific policy objectives. To do so, we have assessed for each of the policy options how effective they are in achieving the policy objectives.

**Efficiency** is assessed at the level of the policy option. With regard to the assessment of the **effectiveness** of outcomes in achieving the policy options, it should be noted that safeguarding fundamental rights has been included as a specific objective and is assessed separately. In this regard, it is acknowledged that according to the Impact Assessment Guidelines on fundamental rights, such aspects should be an integral part of all steps of the assignment and be assessed as part of all assessment criteria. While this integral assessment has been done, it is considered important to highlight certain aspects relating

---

\(^{191}\) The policy options and objectives also need to be **coherent**, i.e. in line with the EU policies as well as with the Treaty and its high level objectives. This analysis is provided in section 5.
to fundamental rights under one heading. The assessments take into account possible (unintended) consequences in areas that are not covered by the policy objectives.

The impacts of the policy options have been rated on a scale from -5 to +5 in terms of the expected changes compared to the Status Quo. To reflect this, Policy option 1 – Status Quo (no further EU action) has been rated with 0, since the other policy options are compared against the status quo situation. A rating of 0 implies that the other options would not result in any major change compared to the status quo. A minus rating implies that the situation is expected to worsen and a rating on the plus side that the situation would be improved. The ratings are relative and therefore serve to compare the policy options towards each other rather than serve as an absolute assessment. Hence, a rating of 5 would not necessarily imply that the problem would be solved and the objective be achieved.

Estimates of the reduction of the magnitude of the problem have been made based on the relative expected achievements of the policy options. A scale of -1% to -5% reduction of the problem has been used for illustrative purposes. For each policy option, the impacts on reducing the problem have been calculated based on the ratings of the impacts.

7.2 Overview – Impacts of the Policy Options

The detailed assessments of the policy options are provided in Appendix L (qualitative impacts and Appendix M (quantitative estimates). Summaries of the assessments are provided in the following sub-section.

While it is outside the scope of the present assignment to identify a preferred policy option, based on the above assessments, before providing summaries of the detailed assessment of impacts, the following table provides a comparison of the ratings of the impacts of the policy options. The table also provides a comparison of the expected impacts of the policy options in terms of the expected reduction of the problem. In this regard, it can be emphasised that also these figures are calculated in relative terms in order to illustrate the different effects that could be achieved, and that the reductions should not be viewed as absolute figures.

The following table provides a summary of assessment of the various policy option impacts:

- **Contribution to EU policy objectives** – i.e. ranking of relative impact of the policy options against the objectives defined in Section 6

- **Impact on the problem of identity theft** – impact of the different policy options in terms of legal/constitutional, economic and social impacts (how the different policy options affect the problem of identity theft as it affects individual citizens, business and wider society);
Impact Assessment

- Overall assessment of impacts – structured around the above assessment criteria relevance, effectiveness, efficiency, impacts and added value as well as feasibility.

The detailed workings for Tables 7.1 (a), (b) and (c), together with the estimate of the cost of implementing the various policy options, are provided in Appendix L.
# Impact Assessment

Table 7.1 (a): Overview of impacts of the policy options - Ranking of relative impacts in achieving the policy objectives

<table>
<thead>
<tr>
<th>Type of impacts / criteria: Policy objectives</th>
<th>PO 1: Status Quo</th>
<th>PO 2: Non-legislative Options</th>
<th>PO 3: Legislative Options</th>
<th>PO 4: Combined Option (PO 2.1, 2.2, 2.3 and 3.1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>To reduce identity theft and related crime</td>
<td>0</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>To improve the capacity to prevent and tackle identity theft and related crime</td>
<td>0</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>To ensure that primary and secondary victims of identity-related crime obtain support and redress</td>
<td>0</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>To safeguard fundamental rights</td>
<td>0</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>To protect business, in particular SMEs</td>
<td>0</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>To improve the knowledge base regarding identity theft and related crime</td>
<td>0</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>To prevent the risk of forum shopping in relation to identity theft and related crime in the EU</td>
<td>0</td>
<td>0</td>
<td>●</td>
<td>●</td>
</tr>
</tbody>
</table>
### Impact Assessment

#### Table 7.1 (b): Overview of impacts of the policy options – Other assessment criteria

<table>
<thead>
<tr>
<th>Type of impacts / assessment criteria</th>
<th>Status Quo</th>
<th>Non-legislative policy options</th>
<th>Legislative policy options</th>
<th>Combined option</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PO1</td>
<td>PO2.1</td>
<td>PO2.2</td>
<td>PO2.3</td>
</tr>
<tr>
<td><strong>Economic impacts</strong></td>
<td>0</td>
<td>★</td>
<td>★★</td>
<td>★★</td>
</tr>
<tr>
<td><strong>Social impacts</strong></td>
<td>0</td>
<td>★</td>
<td>★★</td>
<td>★★</td>
</tr>
<tr>
<td><strong>Legal/Institutional impacts</strong></td>
<td>0</td>
<td>0</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td><strong>Overall assessment</strong></td>
<td>0</td>
<td>★</td>
<td>★★</td>
<td>★★</td>
</tr>
<tr>
<td><strong>Relevance</strong></td>
<td>0</td>
<td>★</td>
<td>★★</td>
<td>★★</td>
</tr>
<tr>
<td><strong>Effectiveness</strong></td>
<td>0</td>
<td>★</td>
<td>★★</td>
<td>★★</td>
</tr>
<tr>
<td><strong>Efficiency</strong></td>
<td>0</td>
<td>★</td>
<td>★★</td>
<td>★★</td>
</tr>
<tr>
<td><strong>Impact and added value</strong></td>
<td>0</td>
<td>★</td>
<td>★★</td>
<td>★★</td>
</tr>
<tr>
<td><strong>Feasibility</strong></td>
<td>0</td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
</tr>
<tr>
<td><strong>Total score</strong></td>
<td>0</td>
<td>20</td>
<td>33</td>
<td>30</td>
</tr>
<tr>
<td><strong>Average score</strong></td>
<td>0</td>
<td>1.33</td>
<td>2.20</td>
<td>2.00</td>
</tr>
</tbody>
</table>
## Impact Assessment

Table 7.1 (c): Assessment of the policy options – Economic Impacts

<table>
<thead>
<tr>
<th>Other assessment criteria</th>
<th>PO1</th>
<th>PO2.1</th>
<th>PO2.2</th>
<th>PO2.3</th>
<th>PO2.4</th>
<th>PO2.5</th>
<th>PO3.1</th>
<th>PO3.2</th>
<th>PO4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reduction of the problem</td>
<td>0</td>
<td>-1%</td>
<td>-2.5%</td>
<td>-2%</td>
<td>-3%</td>
<td>-4.5%</td>
<td>-4%</td>
<td>-4%</td>
<td>-5%</td>
</tr>
<tr>
<td>Economic impacts relating to individuals (€ million)(192)</td>
<td>Current cost: 20 bn</td>
<td>-200</td>
<td>-500</td>
<td>-100</td>
<td>-600</td>
<td>-900</td>
<td>-600</td>
<td>-600</td>
<td>-1,000</td>
</tr>
<tr>
<td>(Economic) impacts relating to individuals (number of victims)(193)</td>
<td>Current no. affected: 8 million</td>
<td>-80,000</td>
<td>-200,000</td>
<td>-160,000</td>
<td>-240,000</td>
<td>-360,000</td>
<td>-240,000</td>
<td>-240,000</td>
<td>-400,000</td>
</tr>
<tr>
<td>Economic impacts relating to business (€ billion)(194)</td>
<td>Current cost: 300 bn</td>
<td>-3</td>
<td>-7.5</td>
<td>-6</td>
<td>-9</td>
<td>-13.5</td>
<td>-9</td>
<td>-9</td>
<td>-15</td>
</tr>
</tbody>
</table>

\(192\) Based on the loss of money for individuals (20 € bn)  
\(193\) Based on the number of citizens affected (8 million)  
\(194\) Based on the loss of money for businesses (300 € bn)
Based on the above overview, the policy option that combines both legislative and non-legislative action (policy option 4) is expected to have the most positive impacts in terms of reducing and tackling the problem. In this regard, it can be noted that the strengths of the non-legislative and legislative policy options relate to different aspects of the problem. While the non-legislative policy options largely are focused on capacity building, awareness raising and support to victims, the legislative options are focused on the rights of primary and secondary victims across the EU, as well as a common definition of identity theft. It can be noted that the feasibility of the two legislative options has been rated as rather low in view of the expected challenges in agreeing on a common definition as well as, for policy option 3.2, the challenge in terms of the already extensive existing legislation on secondary crimes that are linked to identity theft in the Member States.

Below we provide an assessment of the impacts by policy option. The detailed assessments are provided in the appendices. For each policy option, a short description of the content is provided first, followed by a summary of the following types of impacts that can be expected to result from the implementation of the options: achievement of the policy objectives, economic and social impacts, legislative impacts and feasibility. As concerns the latter criterion, it can be noted that the stakeholders largely agreed on the course of action to be taken, as well as the strengths and weaknesses of the different options.

Differences between different types of stakeholders (national authorities, NGOs, law enforcement authorities, businesses, experts) were not pronounced, at least so far as can be ascertained from our consultations. There was a strong consensus on the seriousness of the problem of identity theft and the fact that the severity of the problem is likely to grow. Similarly, there was agreement that given the transnational nature of the problem, action at an EU level is needed to help combat the problem. To the extent that differences exist between stakeholders, these tended to be in their views about the feasibility of EU intervention, some arguing that in the absence of a common definition, legislative policy options are unrealistic. There were also some differences between the Member States depending on perceptions of the seriousness of the problem and the effectiveness of existing national legislation and measures.

The "overall assessment" that is presented in the above table 7.1(b) has been made based on these individual, more detailed assessments.
7.3 Policy Option 1 – Status Quo

Policy Option 1: Status Quo

Existing and planned initiatives at the EU and national level in the field of identity theft, identity management systems and cybercrime.

(i) Achievement of the policy objectives (average score: 0)

The magnitude of identity theft is likely to increase because of e.g. the increased availability of data online (in particular on SNS) and the increased sophistication of criminal schemes to obtain information. Furthermore, for criminals this is often a rather cheap method to obtain data without much risk of being caught. The data is then used to commit other crimes and for funding of criminal activities.

This said, the capacity to prevent and tackle identity theft and related crime is likely to be improved compared to the current situation by means of some of on-going initiatives, including, for example, the establishment of the EC3, which will act as the umbrella for activities to improve evaluation and monitoring of existing preventative and investigative measures, supporting the development of training for the criminal justice community across the EU and establish cooperation between all stakeholders involved in combating cybercrime. This way, the EC3 will be helpful in addressing many aspects of the problem, including insufficient cross-border collaboration and availability of data.

Turning to the availability of support to victims, based on the review of current problems, it is clear that there is currently inadequate support for primary and secondary victims. Indeed, while it has been pointed in the research activities that “one-stop-shops” would be helpful, the existence of such in the Member States is limited. Furthermore, while some countries have reporting mechanisms in place, these are not very developed. Support is provided by a wide variety of organisations, which differ between the Member States and there seems to be limited knowledge of what stakeholders are involved in providing support to victims and their roles also within individual Member States. Based on available information, incremental improvements are likely to be made and some initiatives are being taken in the Member States.

However, there is no clear evidence of plans to improve reporting mechanisms or to establish better and clearer support structures for victims in most Member States. This said, under the new Victims Directive, the Member States will be obliged to ensure that support is available to victims, and they are also encouraged to establish specialised support structures. Hence, while no concrete plans have been identified to date, over the next years the situation is likely to change.

The scope of the Victims Directive is, however, limited to those persons that are acknowledged as victims in national legislation. This means that in those countries where
Impact Assessment

no legislation is in place that covers primary victims, this group will not have access to support. Moreover, the degree to which specialised support structures will be established by the Member States is not clear. To sum up, while overall the situation is likely to improve in view of the new Victims Directive, weaknesses in the support to victims of identity theft are likely to continue.

As a consequence of the current problems, the following fundamental rights may not be adequately safeguarded:

- **Right to liberty and security (Art. 6):** Identity theft and related crime have a negative impact on the security of EU citizens. The problem is likely to worsen.

- **Respect for private and family life (Art. 7) and protection of personal data (Art. 8):** Identity theft and related crime implies the abuse of personal identity data and a lack of respect for private life. Thus, in order to safeguard these rights, it is imperative to combat identity theft as well as related crime. Sufficient (common) action to tackle these problems is currently not taken.

- **Right to property (Art. 17):** This right is directly affected where property is the target of the related (secondary) crime. In relation to primary victims, this Article can also be interpreted to cover identity documentation and other (physical) sources containing identity information. As the problem is expected to worsen, this right will not be adequately safeguarded.

- **Consumer protection (Art. 38):** Identity information may be acquired and abused in relation to online shopping, as well as shopping in the offline world and thus have a negative impact on consumer protection. Based on the problem assessment, there is a clear trend that a large proportion of identity theft and related crime occur in the online environment.

   According to Eurobarometer surveys this results in that many individuals are hesitant to buy online. If no clear action is taken, the problem of identity theft and related crime is likely to continue to have a negative impact on eCommerce and related EU objectives. Furthermore, while e.g. the problem of skimming has been reduced, problems also occur in the offline environment. Overall the problem is likely to worsen, but the Victims Directive may result in some improvement of the current situation once the problem has occurred, since victims would have better access to support; if victims obtain quality support, this may have a positive impact on e.g. continued purchasing online.

- **Right to an effective remedy and to a fair trial (Art. 47):** This right is closely related to the protection of victims, who according to this Article have a right to an effective remedy. The Victims Directive can be expected to have a positive impact on those who are recognised as victims in obtaining support. For those that fall outside this group, the situation is unlikely to change.

Because there is currently no common definition of identity theft and related crime, the monitoring of the problem and ways to tackle this is problematic and is likely to remain so. While some studies have been identified that examine identity theft and related crime, such research activities are not systematic and generally do not
Impact Assessment

deal with the same themes. Furthermore, since in most countries identity theft is not a specific individual offence and because of the lack of reporting mechanisms, there is no systematic collection of data concerning the number of cases.

The existing cooperation initiatives that have been identified, for example the EU’s expert group on identity theft, are likely to make a contribution, but not at a sufficient level. The EC3 that will be established may also have some positive impacts in view of its objective to improve the evaluation and monitoring of existing preventative and investigative measures. This said, the EC3 will be focused on the cybercrime aspects and will thus not ensure comprehensive monitoring in the offline as well as online environment.

(ii) Economic and social impacts (scores: 0 and 0)

If the problem is not reduced, increasing resources are likely to (need to) be spent on investigations of criminal offences relating to identity theft. Significant resources are also likely to continue to be spent on prevention. Identity theft and identity related crime is also likely to continue to have a negative impact on individuals and businesses, including in the area of eCommerce, as well as public institutions.

The research activities have not identified any particularly vulnerable groups (problems seem to be rather evenly distributed among age groups, gender, affluence, various sizes of business etc.). However, SMEs are likely to be disproportionately affected in those cases where they are secondary victims. Furthermore, since primary victims do not seem to be covered in most Member States, they will not have access to support and redress. The problem is greater in some EU Member States than others. For example, the UK is particularly affected.

Turning to the situation for businesses, companies are likely to continue to be negatively affected and to incur costs for preventing the problem, as well as be affected as secondary victims. According to the survey carried out, small and large enterprises are equally affected. This said, the problem is likely to be particularly problematic for SMEs, which may not have the same capacity to provide for prevention as larger firms and when affected as secondary victims, problems may have a more significant impact. Companies in certain sectors, such as the banking sector and those that are active in eCommerce, are likely to be particularly affected.

(iii) Legislative impacts (score: 0)

Since no new EU action would be taken, there would be no requirement for Member States to make changes to their existing legal frameworks. While some Member States have introduced specific identity legislation, based on available information changes do not seem to be foreseen in most countries and fragmentation is likely to continue to characterise the situation. As concerns the institutional impacts, some countries have taken action to clarify the role of various stakeholders in addressing the problem, but in many countries the current unclarities in this regard are likely to remain. Some positive impacts may result from the new Victims Directive. Initiatives taken under the framework of the EC3 may contribute to capacity building of staff.
Impact Assessment

(iv) Feasibility

Stakeholders are not content with a status quo situation according to our survey and the expert workshops that were organised by the Commission and CSFS. As much as 90.3% of the respondents to the survey carried out think that there is a need for EU action to change the current situation.

Conclusions (total average score: 0)

Maintaining the status quo is not perceived as an appropriate option. Ongoing actions (e.g., the establishment of the EC3 and the Victims Directive) are likely to have positive effects. However, there is likely to be a worsening of the situation with regard to identity theft because of various factors including the increased availability of data online (in particular on SNS), and the increased sophistication of criminal schemes to obtain information. Therefore, our assessment suggests that further EU action may be needed to help prevent and tackle identity theft and related crime.

7.4 Policy Option 2: Non-legislative Action

<table>
<thead>
<tr>
<th>Policy Option 2.1: Sharing of experience and knowledge concerning the problem of identity theft via an electronic platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Option 2.1 would involve setting up an online platform to share information on identity theft and to promote networking. More specifically, the website / electronic platform could be divided into three main parts:</td>
</tr>
<tr>
<td>• Part 1 - for individuals, where contact details to reporting mechanisms are provided for the Member States, information on legislation in place would be provided in an easily understandable format (examples of cases could be provided) as well as information on risks and preventative action that can be taken. This part of the website would be open to all.</td>
</tr>
<tr>
<td>• Part 2 - for experts and / or law enforcement authorities, where legislation would be provided with a more technical focus, as well as information on relevant actors working in the field in the Member States. A closed community for sharing information real time and good practices would be established. Information could also be shared on risks. This section could be based on registration.</td>
</tr>
<tr>
<td>• Part 3 – would serve as an electronic library with public reports containing statistics etc. It would be possible to upload reports etc. and thereby create an online knowledge centre.</td>
</tr>
</tbody>
</table>

EU funding would need to be set aside to set up the proposed platform. It could either be set up as a separate portal or be part of the eJustice Portal.
(i) **Achievement of the policy objectives (average score: 1.1)**

The overall effectiveness of the policy option in achieving the policy objectives is comparatively low.

The most positive impacts are expected in relation to the objectives of improving the capacity to prevent and tackle identity theft and related crime, as well as of improving the knowledge base regarding identity theft and related crime. The positive impacts are likely to primarily result from the capacity building of LEAs through the interactive portal, as well as the existence of a public library where publications concerning identity theft can be uploaded. As concerns the main weaknesses of the policy option, it is not expected to make any contributions to the objective of preventing the risk of forum shopping in relation to identity theft and related crime in the EU. Moreover, the positive impacts will be restricted to those that access the online portal.

Turning to the contribution of the policy option to reducing the scale of identity theft, some positive effects can be expected for those individuals that access the online portal, as the portal would contain information concerning how to reduce risk behaviour. If implemented, this advice could help reducing the problem.

Victims of identity theft would benefit from the provision of contact details to relevant support structures in the Member States. Therefore, the opportunities for victims to obtain redress would increase, while stress and other non-financial consequences are likely to be reduced. The reduction of the problem and improved support for victims is in turn likely to have a positive impact on businesses, in particular on those that operate online, since the fear of the risks of buying online currently expressed by individuals in e.g. Eurobarometer surveys may be reduced. The effects are likely to be particularly important for SMEs, which are likely to be disproportionately affected as secondary victims.

In addition to improving consumer protection, the policy option is likely to have a minor positive impact in terms of safeguarding a number of other fundamental rights, such as the Right to liberty and security (due to the expected capacity building of LEAs), Respect for private and family life and protection of personal data (as a consequence of capacity building of LEAs and reduced risk behaviour by individuals), and the Right to an effective remedy and to a fair trial (again, the capacity building of LEAs will result in positive impacts, as well as the availability of information concerning existing support structures for victims).

(ii) **Economic and social impacts (scores: 1 and 1)**

The policy option is likely to only result in rather modest positive economic and social impacts. Although the option is likely to lead to more effective investigations of criminal offences relating to identity theft, which should have positive economic and social implications, the benefits would be limited to those LEAs that benefit from the portal. Furthermore, the economic and social effects rely on the willingness of individuals to proactively access and use the site and then implement the advice.
As concerns the financial resources that are required to implement the option, the main costs are likely to refer to the following elements of the option if a new, separate portal is established:

- The establishment and maintenance of the platform, as well as analysis of information could be contracted out by the European Commission to an external provider. This external provider would be responsible for the website infrastructure and for collecting the relevant information from Member States and other relevant actors for the purpose of the three Parts of the portal. In addition, stakeholders could also be invited to upload public documents to the library themselves (Part 3).

- EU funding would need to be provided for the work to be carried out by the external contractors. The costs will need to be verified but wider experience suggests that a budget of around €250,000 may be needed for the design, set up and maintenance of an internet-based platform over a 2-3 year period. This estimate is based on the DG Home EMN system which is managed by an external contractor and which we have used as a benchmark in several other studies.

- The Member States would incur costs for providing information on the legislative situation in their country for the purpose of the portal.

The costs for developing the Portal on the eJustice Portal are likely to be similar in terms of the costs for content, while the design and set up costs would be lower than what is indicated above.

To sum up, the policy option is likely to result in the following financial costs and economic impacts (based on the costs for a separate portal):

**Table 7.2: Financial and economic impacts**

<table>
<thead>
<tr>
<th>Financial impacts</th>
<th>Costs or benefits (EUR)</th>
<th>Change in %</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Financial costs</strong>: Separate Portal</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EU Commission</td>
<td>250,000</td>
<td>n/a</td>
<td>Design, set up and maintenance over a 2-3 years period (based on costs for EMN).</td>
</tr>
<tr>
<td>MS</td>
<td>Admin burden</td>
<td>n/a</td>
<td>See table below</td>
</tr>
</tbody>
</table>

| Economic impacts | | | |
| Economic impact on society | -200m | -1% | Reduction of the loss of money for individuals based on the actual loss of money (€20bn) |
| Businesses | -3bn | -1% | Reduction of the loss of money for businesses based on the actual loss of money (€300bn) |
Impact Assessment

<table>
<thead>
<tr>
<th>Financial impacts</th>
<th>Costs or benefits (EUR)</th>
<th>Change in %</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial costs: Separate Portal</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Individual victims</td>
<td>~80,000</td>
<td>-1%</td>
<td>Reduction of the number of citizens affected based on the actual number (8m)</td>
</tr>
</tbody>
</table>

Table 7.3: Administrative burden for the Member States

<table>
<thead>
<tr>
<th>Information obligation</th>
<th>Time spent</th>
<th>Frequency per annum</th>
<th>Av. wage rate (€ per hour)</th>
<th>Total admin cost per obligation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide information for the portal</td>
<td>1 FTE, 1 month with 20 working days</td>
<td>One-off cost (update in case of new legislation)</td>
<td>18</td>
<td>2,880</td>
</tr>
</tbody>
</table>

(iii) Legislative and institutional changes (score 0)

No major legislative changes are directly connected to the establishment of the electronic platform. Some limited benefits are likely to result in terms of improved institutional effectiveness and efficiency, which can be enhanced through the use of the platform by LEAs and the judiciary. Impacts are likely to be similar across the Member States.

(iv) Feasibility (score: 5)

Establishing the electronic platform in order to be able to share experience and knowledge regarding the problem of identity theft is strongly supported by stakeholders. It is also feasible from a practical perspective, although funding is so far not foreseen in the MFF.

Conclusions (total average score: 1.3)

To conclude, while positive impacts can be expected in relation to the majority of the policy objectives, the overall effectiveness of the policy option is comparatively low. Hence, although the policy option is feasible from a practical and political perspective, it would not sufficiently address the current problems.
Policy Option 2.2: Establishment of a network of national contact points, which would be tasked with running, in each Member State, a one-stop-shop for victims of identity theft, act as a monitoring body and organise awareness raising activities

- Policy Option 2.2 would involve the establishment of a network of ‘national contact points’ across EU Member States.
- At the national level, the contact points would act as a one-stop shop for victims (similar to what is done in the Netherlands). This entity would also, in its role as a monitoring body, be responsible for collecting data on the problem in the relevant Member State. In order to ensure that comparable data are compiled, monitoring and reporting requirements could be agreed at the EU level and annual reports be submitted. Furthermore, the contact points would be responsible for organising awareness raising activities in the Member States.
- At the EU level, information exchanges through face to face meetings would be funded, bringing together the contact points and other actors (including from law enforcement authorities, the private sector and from third countries) on specific topics that would be identified by the network. The actors that would be gathered would be determined on a case by case basis. Working Groups would be tasked with the preparation of these meetings. Best practices would also be identified. The network would in addition convene on a regular basis (e.g. four times per year).
- EU funding would need to be made available to support Policy Option 2.2.

(i) Achievement of the policy objectives (average score: 2.1)

The expected overall effectiveness of the policy option in achieving the policy objectives is medium ranked.

The main positive impacts are likely to relate to the objectives of reducing identity theft and identity related crime as a result of improved institutional capacity, as well better support to victims. Positive effects can also be expected in relation to an improved information base concerning the problem of identity theft, the safeguarding of fundamental rights, the protection of business and the prevention of forum shopping in the EU. The policy option would, on the other hand, however only result in minor positive impacts in terms of reducing the risk of forum shopping.

As concerns the elements of Policy Option 2.2 that would result in the positive impacts, the policy option would contribute to the capacity building of relevant actors in a number of ways, including by means of workshops and working groups on topics that have been identified as being important by the relevant stakeholders; identification of best practice; possibilities for actors across the public and private sectors to convene, examine various possibilities to tackle the problem of identity theft and take common action; activities to monitor the problem in the Member States by the contact points; and regular meetings between the contact points.
Impact Assessment

The foreseen annual threat assessments can play an important role in building the capacity of various stakeholders. Overall, it is expected that a limited number of LEA officials in Member States could be directly involved in information sharing activities. These could then act as multipliers. Further LEAs could be reached through the awareness raising activities. Importantly, not only LEAs and the judiciary could participate in the foreseen activities, but also actors from the private sector and from third countries. This is one of the main strengths of the policy option, since the importance of common multistate and multi-sector action is one of the findings of the problem assessment.

If the capacity of LEAs is improved and one stop shops are introduced, this is likely to increase the opportunities for victims to obtain redress and reduce their costs. If investigations are successfully completed to a greater extent than in the current situation, there are also likely to be benefits for victims in terms of reduced stress and other negative non-financial consequences. In turn, positive impacts are likely to result for business, especially SMEs. To the extent that business is involved in the workshops and other initiatives that are taken within the framework of the network, further positive impacts can be expected, e.g. in relation to companies’ capabilities to prevent the problem.

The policy option is likely to have minor positive effects on safeguarding fundamental rights such as the Right to liberty and security, Respect for private and family life and protection of personal data; the Right to property and the Right to an effective remedy and to a fair trial through the capacity building of LEAs. Furthermore, if the message of the increased capacity of LEAs is spread on to individuals, some individuals may be less reluctant to buy online and consumers that are affected by identity theft may be better protected.

(ii) Economic and social impacts (scores: 2 and 2)

As noted above, the most important social impacts relate to the introduction of one stop shops and the possibilities for victims to get support.

Furthermore, the policy option is likely to lead to more effective investigations of criminal offences relating to identity theft. The overall economic impact is expected to be medium. While a wider group of stakeholders may benefit from the threat assessments, for most of the networking measures, the increased effectiveness will be “limited” to those stakeholders that are directly involved in the foreseen activities or are reached via multipliers. As concerns the social impacts, within the framework of the activities that are organised, best practice could be identified in relation to examining cases related to different social groups, e.g. various types of businesses or age groups. Wider benefits on individuals, businesses and public institutions could result from the increased capacity of LEAs and the judiciary to deal with cases of identity theft and related crime.
Impact Assessment

As concerns the financial resources that are required to implement the option, funding would need to be set aside by the European Commission for the following activities to support this policy option:

- The network of contact points and regular meetings;
- Awareness raising campaigns;
- Working group sessions and activities.

With the exception of the last of these activities, it is assumed that Member States would contribute co-financing.

In addition, the Commission would incur costs relating to the management of the network (which could be procured).

It is difficult to estimate the funding that would be required to support the network but some guidance can be obtained from the experience of other EU-supported networks. The cost of networking could be quite modest – perhaps no more than €60,000 p.a. for four meetings p.a. for representatives from the EU27 Member States. What is less easy to estimate is the cost of supporting other activities than those that may be undertaken by the network members (as outlined above). Grants used to support similar networking activities by EU agencies (e.g. EMCDDA, EUOSHA, Eurofound) range from around €20-50,000 per Member State for data collection, information dissemination and basic awareness raising activities, to around €200,000 per country for fully-developed observatory-type functions. If support is provided, it could either be through (a) the same grant for each Member State; or (b) a grant that is adjusted to reflect differences between Member States.

As concerns the costs for support to victims, the annual costs of the Identity Fraud Support Office, which is app. €400,000, could be used as a proxy. However, some caution should be placed with regard to the possibilities to extrapolate this estimate to all Member States; it is likely that some countries would incur higher and others lower costs depending on e.g. the number of victims etc. Furthermore, it is likely that this includes some costs for information collection and analysis. Hence, this figure will be used as maximum for support to victims.

Role and Costs of the Identity Fraud Support Office in the Netherlands

Recently, an Identity Fraud Support Office was established in the Netherlands, which helps victims whose identity has been misused. The CMI is a small organisation of three employees, but cooperating with a wide range of organisations that have committed themselves to do so. This includes any institution, business or other organisation that may be helpful to help victims. The support office has an agreement with most public parties involved in fighting identity crime and restoring errors in public databases. According to the CMI the annual costs for 2011 for providing support to victims amount to €400,000. The office deals with approximately 250 cases per annum, sometimes involving more than one individual and usually involving more organisations.
Impact Assessment

To sum up, the policy option is likely to result in the following financial and economic impacts:

Table 7.4: Financial and economic impacts

<table>
<thead>
<tr>
<th>Financial impacts</th>
<th>Costs or benefits (EUR)</th>
<th>Change in %</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial costs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EU Commission</td>
<td>Min.: app. 2.2 mn</td>
<td>n/a</td>
<td>Costs per annum</td>
</tr>
<tr>
<td></td>
<td>Max.: app. 11 mn</td>
<td></td>
<td>Network: minimum and maximum costs per annum</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(60,000 euro plus 20,000 to 200,000 euro per Member State of information gathering and from 80,000 up to 400,000 for support to victims)</td>
</tr>
<tr>
<td>MS</td>
<td>n/a</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>Economic impacts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Economic impact on society</td>
<td>-500m</td>
<td>-2.5%</td>
<td>Reduction of the loss of money for individuals based on the actual loss of money (€20bn)</td>
</tr>
<tr>
<td>Businesses</td>
<td>-7.5bn</td>
<td>-2.5%</td>
<td>Reduction of the loss of money for businesses based on the actual loss of money (€300bn)</td>
</tr>
<tr>
<td>Individual victims</td>
<td>-200,000</td>
<td>-2.5%</td>
<td>Reduction of the number of citizens affected based on the actual number (8m)</td>
</tr>
</tbody>
</table>

The collection of information would be part of the activities that are funded within the network. No additional administrative burden has been possible to estimate.

(iii) Legislative and institutional changes (score 1)

The policy option would not prompt any legislative changes. However, it could contribute to increased institutional effectiveness and efficiency, e.g. through the information sharing activities and the identification of best practices, as well as the monitoring by the contact points. Impacts are likely to be similar across the Member States, except for the Netherlands, where a well-developed support structure is already in place.
Impact Assessment

(iv) Feasibility (score: 4)

Although the policy option has widespread support it is not considered to, in itself, constitute a sufficient response to the growing problem of identity theft. The policy option is also feasible from a practical perspective, although funding is so far not foreseen in the MFF.

Conclusions (total average score: 2.2)

To sum up, the main strengths of the policy option are its contributions to the reduction of identity theft and related crime, support to victims and the improvement of the LEAs' capacity to prevent and tackle these problems. Furthermore, the policy option is likely to significantly improve the knowledge base and information sharing, which may inter alia lead to more effective and efficient investigations.

The main weakness of the policy option is that the activities would need to be carried out within the existing framework including a lack of a common understanding of identity theft and related negative implications for the possibilities to share information and develop common activities.

Policy Option 2.3: Commission Recommendation on a common definition, establishment of reporting mechanisms for victims, collection of information on the problem of identity theft and related crime and the organisation of EU-supported awareness raising campaigns

In the Recommendation the Commission would encourage the Member States to:

- Adopt a common definition (covering primary and / or secondary victims; to be defined in the Recommendation) or at least to ensure that all elements that are covered in the suggested definition are also covered in national legislation.
- Collect statistics and monitor the development of identity related crime, as well as the drivers for this.

Provide a reporting mechanism for victims (this would also have the objective of increasing the available statistics) and to launch awareness raising campaigns on the risks and preventative action that could be taken by individuals, businesses and public authorities.

(i) Achievement of the policy objectives (average score: 1.9)

The policy option is expected to contribute equally to all policy objectives, except for the objective relating to the risk of forum shopping, where a slightly smaller positive effect is expected to be result than for the other objectives.
Impact Assessment

Overall, the positive impact is expected to be medium ranked. The weakness of the option is that it would be up to the individual Member States to take action. While some may do so, others may not. Therefore, national differences are likely to remain, although they may be reduced. Another weakness is that no fora for exchanging information are foreseen. This limits the EU added value.

In terms of the likely benefits stemming from the adoption of a Recommendation concerning identity theft at the EU level, as a starting point the Recommendation would make it clear that the issue is seen as a priority problem that has to be combated. The main impacts of the various elements that the Recommendation would contain are expected to be as follows:

• The establishment of a common definition: not all Member States are likely to adopt the proposed definition. Thus the positive impacts in terms of increased harmonisation and associated benefits in terms of a common understanding, reporting etc. would be restricted to those Member States that make the relevant legislative changes.

• The establishment of reporting mechanisms for victims: As outlined in section 3, a number of Member States already have some types of reporting systems in place, however, these do not seem to be functioning at their capacity. In the Recommendation the Commission would encourage the Member States to introduce or develop their reporting mechanisms based on best practice. The benefits of the policy option in terms of better support to victims and an increased information base would be dependent on the degree to which the Member States would do this.

• Collection of information on identity theft: the extent of the benefits is closely related to the adoption by the Member States of the common definition proposed by the Commission as well as the existence of reporting mechanisms / support structures. The more Member States that adopt the definition, the more aggregated and comparative analyses can be made based on the information collected. Furthermore, as noted above, the availability of reporting mechanisms will also have an impact on the availability of data.

• The awareness raising campaigns that may be launched as a result of the Recommendation are likely to result in that at least some individuals, businesses and public authorities stop or reduce their risk behaviour. Based on the feedback from the stakeholder consultations carried out, a change of risk behaviour could significantly reduce the scale of the problem.

The above activities that concern capacity building are likely – in line with their implementation in the Member States – to lead to increased capacity of LEAs and contribute to an improved knowledge base, which could increase the effectiveness of investigations and thereby also have a positive impact on the fundamental rights relating e.g. to e.g. liberty and security, an effective remedy and to a fair trial, as well as privacy and data protection.
Positive effects may also be visible in relation other fundamental rights, namely consumer protection and right to property, as LEAs may be more effective in their investigations. Further positive effects on these two fundamental rights are likely to result from the establishment of reporting mechanisms / support structures for victims, as consumers would feel more secure when purchasing online if they know that they have access to support in case they are victims of identity theft. In turn, positive effects can be expected for business, in particular those that are active online.

(ii) Economic and social impacts (scores: 2 and 2)

Ultimately, the costs of implementing this policy option would be dependent on the actions that will be taken by the Member States as a consequence of the Recommendation.

Member States that implement the foreseen actions would incur additional costs for the establishment of reporting mechanisms for victims, collection of information on the problem of identity theft and related crime and the organisation of awareness raising campaigns to the extent that such activities are not already carried out. The policy option does not include any actions that specifically target business, although they may benefit from some of the activities carried out, such as (potentially) reduced risk behaviour by individuals. Any reductions and increased awareness of the actions that are taken by the Member States to support victims may have a positive spinoff effect in terms of a higher number of individuals buying online. In turn, this may lead to that fewer companies end up being secondary victims.

To sum up, the policy option is likely to result in the following financial and economic impacts:

**Table 7.5: Financial and economic impacts**

<table>
<thead>
<tr>
<th>Financial impacts</th>
<th>Costs or benefits (EUR)</th>
<th>Change in %</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Financial costs</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EU Commission</td>
<td>App. €11,000</td>
<td>n/a</td>
<td>This is an estimate based on 2 months FTE of one Commission A8 staff.</td>
</tr>
<tr>
<td>MS</td>
<td>n/a</td>
<td>n/a</td>
<td>Member States are not required to implement the Recommendation by the Commission. The extent to which action will be taken and the type of action has not been possible to assess. For individual elements, see the assessments of PO 2.1 and 2.2.</td>
</tr>
</tbody>
</table>
Impact Assessment

<table>
<thead>
<tr>
<th>Financial impacts</th>
<th>Costs or benefits (EUR)</th>
<th>Change in %</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial costs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Economic impacts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Economic impact on society</td>
<td>-400m</td>
<td>-2%</td>
<td>Reduction of the loss of money for individuals based on the actual loss of money (€20bn)</td>
</tr>
<tr>
<td>Businesses</td>
<td>-6bn</td>
<td>-2%</td>
<td>Reduction of the loss of money for businesses based on the actual loss of money (€300bn)</td>
</tr>
<tr>
<td>Individual victims</td>
<td>-160,000</td>
<td>-2%</td>
<td>Reduction of the number of citizens affected based on the actual number (8m)</td>
</tr>
</tbody>
</table>

The policy options do not include any information obligations. Therefore, the administrative burden has not been estimated.

(iii) Legislative and institutional changes (score 1)

The policy option would not require any legislative changes, although the aim is that the Member States adopt legislation in line with the proposed common definition. As concerns the institutional impacts, better information on the nature and scale of the problem could be used to build the capacity of LEAs and the judiciary. Impacts on different Member States have not been possible to assess as it is uncertain what action would be taken.

(iv) Feasibility (score: 3)

The opinion of the overwhelming majority of the relevant stakeholders is that the implementation of a common definition is very important. This also applies to the implementation of the collection of common statistics in order to be able to get a more comprehensive view on the problem within the EU. The policy option is feasible from a practical perspective.

Conclusions (total average score: 2.0)

To conclude, the main strength of the policy option is that it would make it clear that the issue is seen as a priority problem that has to be combated. This said, the exact benefits would be dependent on the action taken by the Member States.
Impact Assessment

Policy Option 2.4: Combination of non-legislative policy options 2.1 and 2.2

Under this policy option, the following two non-legislative policy options would be combined:

- Policy Option 2.1: Sharing of experience and knowledge concerning the problem of identity theft via an electronic platform; and
- Policy Option 2.2 Establishment of a network of national contact points, which would be tasked with running, in each Member State, a one-stop shop for victims of identity theft, act as a monitoring body and organise awareness raising activities.

(i) Achievement of the policy objectives (average score: 2.3)

The overall effectiveness of the policy option is medium. The option combines two types of non-legislative action, namely the establishment of an online platform with information about identity theft and the establishment of a network of national contact points.

Hence, the focus would be on capacity building. Indeed, the strength of the policy option is that it would combine the establishment of a network of contact points that provide support to victims and monitor the situation in the Member States with the creation of an online portal that allows for real time communication, the compilation of available material online and information to victims about the available support structures and risk behaviour.

This way, the policy option is likely to have a medium positive impacts on the objectives of reducing identity theft and related crime, improving the capacity to prevent and tackle identity theft and related crime, providing support and redress to victims, safeguarding fundamental rights and building the knowledge base. Less positive impacts can be expected in relation to protection of business and preventing the risk of forum shopping.

(ii) Economic and social impacts (scores: 3 and 3)

The policy option is likely to lead to more effective investigations of criminal offences relating to identity theft because of the threat assessment that will be carried out by the contact points, information sharing possibilities, awareness raising campaigns and identification of best practice between LEAs and the judiciary as well as with actors from the private sector and from third countries.

The increased effectiveness will be “limited” to those that are directly involved in the communication via the electronic platform, the foreseen training and meetings or are reached via multipliers. Identity theft and identity related crime is likely to continue to
Impact Assessment

have a negative impact on e-Commerce, however, some improvement to the situation can be expected in view of the increased capacity of LEAs as well as the expected impacts on reduced risk behaviour by individuals and business. As concerns the likely social impacts, best practice could be identified in relation to examining cases related to different social groups, e.g. various types of businesses or age groups. Wider benefits on individuals, businesses and public institutions could result from the increased capacity of LEAs and the judiciary to deal with cases of identity theft and related crime, as well as through the awareness raising activities.

The financial and economic impacts have been estimated as follows.

Table 7.6: Financial and economic impacts

<table>
<thead>
<tr>
<th>Financial impacts</th>
<th>Costs or benefits (EUR)</th>
<th>Change in %</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial costs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EU Commission</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Portal:</td>
<td>250,000</td>
<td>n/a</td>
<td>Portal: Design, set up and maintenance over a 2-3 years period (based on costs for EMN).</td>
</tr>
<tr>
<td>Network:</td>
<td>Min.: app. 2.2 mn</td>
<td></td>
<td>Network: minimum and maximum costs per annum (60,000 euro plus 20,000 to 200,000 euro per Member State of information gathering and from 80,000 up to 400,000 for support to victims)</td>
</tr>
<tr>
<td></td>
<td>Max.: app. 11 mn</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MS</td>
<td>Admin burden</td>
<td>n/a</td>
<td>See table below</td>
</tr>
<tr>
<td>Economic impacts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Economic impact on society</td>
<td>-600m</td>
<td>-3%</td>
<td>Reduction of the loss of money for individuals based on the actual loss of money (€20bn)</td>
</tr>
<tr>
<td>Businesses</td>
<td>-9bn</td>
<td>-3%</td>
<td>Reduction of the loss of money for businesses based on the actual loss of money (€300bn)</td>
</tr>
<tr>
<td>Individual victims</td>
<td>-240,000</td>
<td>-3%</td>
<td>Reduction of the number of citizens affected based on the actual number (8m)</td>
</tr>
</tbody>
</table>
Impact Assessment

Table 7.7: Administrative burden for MS

<table>
<thead>
<tr>
<th>Information obligation</th>
<th>Time spent</th>
<th>Frequency per annum</th>
<th>Av. wage rate (€ per hour)</th>
<th>Total admin cost per obligation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide information for the portal</td>
<td>1 FTE, 1 month with 20 working days</td>
<td>One-off cost (update in case of new legislation)</td>
<td>18</td>
<td>2,880</td>
</tr>
</tbody>
</table>

(iii) Legislative and institutional changes (score 1)
The policy option would not prompt any legislative changes. In terms of institutional changes, a network of contact points would be established, which would support victims of identity theft and collect information on the problem.

(iv) Feasibility (score: 3)
There is support from stakeholders to introduce further information collection and networking activities, as well as to provide further support to victims. The policy option is feasible from a practical perspective, however, no funding is foreseen in the MFF.

Conclusions (total average score: 3.5)
The policy option will in particular achieve positive impacts in relation to capacity building and information collection, as well as support to victims of identity theft. This way, the policy option both includes preventive action as well as support for victims to obtain redress.

Similar to policy options 2.1 and 2.2, the main weakness of policy option 2.4 is that the activities would need to be carried out within the existing framework including a lack of a common understanding of identity theft and related negative implications for the possibilities to share information and develop common activities.

Policy Option 2.5: Combination of non-legislative policy options 2.1, 2.2 and 2.3

Under this policy option, all of the above three options would be combined. Overlapping elements would, naturally, be excluded.
Impact Assessment

(v) Achievement of the policy objectives (average score: 3.3)

The overall effectiveness of the policy option is comparatively high. The option combines non-legislative action and voluntary legislative action by the Member States.

The focus would be on capacity building and an increased common understanding of identity theft by the Member States by means of the proposed common definition by the Commission. Indeed, the strength of the policy option is that it would combine the establishment of a network of contact points that provide support to victims and monitor the situation in the Member States with the creation of an online portal that allows for real time communication, the compilation of available material online and information to victims about the available support structures and risk behaviour, as well as a Recommendation for a common definition by the Commission.

This way, the policy option is likely to have comparatively high positive impacts on the objectives of reducing identity theft and related crime, improving the capacity to prevent and tackle identity theft and related crime, providing support and address to victims, safeguarding fundamental rights and building the knowledge base. Slightly less positive impacts can be expected in relation to protection of business and preventing the risk of forum shopping. With regard to the latter objective, while the Commission would propose a common definition, it would be up to the Member States to decide to adopt this definition or not. Therefore, while some positive impacts could be expected to result from this initiative as well as improved enforcement through capacity building, the impacts are not expected to be significant.

(vi) Economic and social impacts (scores: 4 and 4)

The policy option is likely to lead to more effective investigations of criminal offences relating to identity theft because of the threat assessment that will be carried out by the contact points, information sharing possibilities, awareness raising campaigns and identification of best practice between LEAs and the judiciary as well as with actors from the private sector and from third countries.

The increased effectiveness will be “limited” to those that are directly involved in the communication via the electronic platform, the foreseen training and meetings or are reached via multipliers. Identity theft and identity related crime is likely to continue to have a negative impact on e-Commerce, however, some improvement to the situation can be expected in view of the increased capacity of LEAs as well as the expected impacts on reduced risk behaviour by individuals and business. As concerns the likely social impacts, best practice could be identified in relation to examining cases related to different social groups, e.g. various types of businesses or age groups. Wider benefits on individuals, businesses and public institutions could result from the increased capacity of LEAs and the judiciary to deal with cases of identity theft and related crime, as well as through the awareness raising activities.

The financial and economic impacts have been estimated as follows.
### Table 7.8: Financial and economic impacts

<table>
<thead>
<tr>
<th>Financial impacts</th>
<th>Costs or benefits (EUR)</th>
<th>Change in %</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Financial costs</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EU Commission</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Portal: 250,000</td>
<td></td>
<td></td>
<td>Portal: Design, set up and maintenance over a 2-3 years period (based on costs for EMN).</td>
</tr>
<tr>
<td>Network: Min.: 600,000 Max.: 5,500,000 Recommendation 11,000</td>
<td></td>
<td></td>
<td>Network: minimum and maximum costs per annum (60,000 euro plus 20,000 to 200,000 euro per Member State)</td>
</tr>
<tr>
<td>MS</td>
<td>Admin burden</td>
<td>n/a</td>
<td>See table below</td>
</tr>
<tr>
<td><strong>Economic impacts</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Economic impact on society</td>
<td>-900m</td>
<td>-4.5%</td>
<td>Reduction of the loss of money for individuals based on the actual loss of money (€20bn)</td>
</tr>
<tr>
<td>Businesses</td>
<td>-13.5bn</td>
<td>-4.5%</td>
<td>Reduction of the loss of money for businesses based on the actual loss of money (€300bn)</td>
</tr>
<tr>
<td>Individual victims</td>
<td>-360,000</td>
<td>-4.5%</td>
<td>Reduction of the number of citizens affected based on the actual number (8m)</td>
</tr>
</tbody>
</table>

### Table 7.9: Administrative burden for MS

<table>
<thead>
<tr>
<th>Information obligation</th>
<th>Time spent</th>
<th>Frequency per annum</th>
<th>Av. wage rate (€ per hour)</th>
<th>Total admin cost per obligation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide information for the portal</td>
<td>1 FTE, 1 month with 20 working days</td>
<td>One-off cost (update in case of new legislation)</td>
<td>18</td>
<td>2,880</td>
</tr>
</tbody>
</table>
(vii) Legislative and institutional changes (score 2)

The policy option would not prompt any legislative changes directly. Based on the Recommendation, information exchanges and the identification of good practices, some Member States may address deficiencies and gaps on their own initiative. The policy option is aimed at improving the institutional effectiveness and efficiency of LEAs and the judiciary to deal with identity theft and related crime and positive impacts can be expected in this regard because of the possibility to share information and the identification of best practices. The positive impacts would be limited to those that are directly involved in the activities or are targeted by multipliers or awareness raising activities.

As concerns impacts on different Member States, only three countries (Czech Republic, Italy and Ireland) have confirmed to have legislation in place that covers primary victims before a secondary crime has been committed. In other countries, primary victims are generally covered when a secondary crime has been committed. Hence, in all Member States except these countries, a change in the approach of the legislation would be promoted by the Recommendation. Legislative changes are also likely to need to be made in the three countries where legislation already exists to make sure that the common definition is covered.

(viii) Feasibility (score: 3)

A combination of non-legislative measures to prevent and tackle identity theft is widely accepted and welcomed by stakeholders. The policy option is feasible from a practical perspective, however, no funding is foreseen in the MFF.

Conclusions (total average score: 3.4)

The policy option is fairly comprehensive in its approach and combines several non-legislative measures. This implies that the problem of identity theft can be tackled with several instruments as well as with a multinational and multi-sector approach. Furthermore, with the adoption of a Recommendation for a common definition of identity theft, the problem gets EU-wide recognition and prioritisation. This will promote the possibilities for coordinated action and the collection of comparable data on the scale and nature of the problem in order to broaden the common knowledge base.

7.5 Policy Option 3: Legislative Action

Policy Option 3.1: Adoption of a Directive on identity theft, focusing on primary victims (minimalistic approach)

Under this policy option a Directive – minimalist approach – would be adopted, which would be restricted to primary victims. The scope of the Directive would be as follows:

- Establish a common definition of identity theft covering primary victims and that identity theft is a criminal offence in the EU.
Impact Assessment

- Establish harmonised penalties.
- Introduce a requirement to collect information concerning investigations, prosecutions and convictions relating to this new offence. In order to ensure that comparable data are compiled, more specific monitoring and reporting requirements could be set out. Data to be collected could, for example, include: number of reported cases, number of prosecutions, number of losses etc. Examples of cases could also be requested to be provided. Consequences for victims could also be reported on as well as the methods used.

Annual reports should be submitted to the Commission by the Member States.

(i) Achievement of the policy objectives (average score: 2.7)

The adoption of a Directive would be a clear statement that identity theft is not acceptable and that common action is taken to deal with this problem. The overall effectiveness of the policy option in achieving the policy objectives is expected to be medium. Particularly positive impacts are expected in relation to the objective of ensuring that both primary and secondary victims have access to support and redress and safeguarding fundamental rights.

Turning to the individual objectives, with regard to the objective of reducing identity theft and related crime, the adoption of a Directive concerning identity theft at the EU level would make it clear that it is seen as a priority to combat this type of crime and the importance of taking common action. Similar to other pieces of legislation that criminalise certain conduct, this may have a certain deterrent effect. It can be expected that there would be a positive effect in terms of reducing the problem, as some of the perpetrators may abstain from acquiring identity information if the actual gathering / collection of data would be a criminal offence. Since this option would result in that primary victims would also be acknowledged as victims in national legislation in Member States where they are currently not covered, this policy option could, at least short term, result in an increase in the number of cases that LEAs need to handle. Although this would not mean that there is an increase in the scale of the problem per se, the cases reported could increase.

Indeed, the main impact of the policy option would be that primary victims are acknowledged in law and that this group of victims has access to redress, including support foreseen under the Victims Directive. The policy option would make a positive contribution to safeguarding fundamental rights by ensuring that primary victims are covered across the EU. The policy option would not change the situation as far as secondary crimes are concerned.

As concerns the objective of improving the capacity to tackle and prevent identity theft and related crime and building the knowledge base, the policy option would ensure a common language in dealing with identity theft cases within the EU and ensure that primary victims are covered across the EU. Cross-border collaboration would also benefit from an increased knowledge base concerning the phenomenon due to the required collection of information concerning the cases in relation to primary victims.
Impact Assessment

The policy option would require the Member States to collect data concerning cases of identity theft, focusing on primary victims. While it is likely that not all cases will be reported, such data could provide insights into the extent and evolution of the problem. However, the benefits would be limited to the acquisition of identity information from primary victims; no action in relation to secondary crimes is foreseen.

(i) Economic and social impacts (scores: 3 and 4):

According to the research, primary victims tend to be individuals rather than business. Thus, the main positive impacts are likely to result for individuals, while the direct impact on business is likely to be limited. Benefits for business may result from increased eCommerce as individuals may be less reluctant to buy online if they know that if their data are “stolen” since this would be a criminal offence. Only limited positive impacts are expected in relation to the objective of preventing forum shopping. While a common offence would be established across the EU, the level of penalties and enforcement activities relating to secondary crime would not be addressed by the policy option, which is a weakness. As a consequence, the positive impacts on business can be expected to be rather limited.

Costs would relate to the development of the Directive and its transposition in the Member States. This policy option would imply that primary victims are also covered in legislation across the EU. Associated costs would refer to a potentially increased number of cases for LEAs to deal with at the outset of the implementation of the Directive. However, there could be a positive spinoff effect on eCommerce since the adoption of a Directive would be a clear statement from the EU that this type of conduct is not acceptable. In terms of social impacts, the policy option would have particular benefits for primary victims, independently of if these are individuals, businesses or public institutions. Research, however, suggest that most victims are individuals. As pointed out above, there could be a positive effect on eCommerce. The financial and economic impacts have been estimated as follows:

<table>
<thead>
<tr>
<th>Table 7.10: Financial and economic impacts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial impacts</td>
</tr>
<tr>
<td>-------------------</td>
</tr>
<tr>
<td>Financial costs</td>
</tr>
<tr>
<td>EU Commission</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>MS</td>
</tr>
</tbody>
</table>
**Impact Assessment**

<table>
<thead>
<tr>
<th>Financial impacts</th>
<th>Costs or benefits (EUR)</th>
<th>Change in %</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial costs</td>
<td></td>
<td></td>
<td>days for one FTE with average wage rate of 18€ per hour.</td>
</tr>
<tr>
<td>Economic impacts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Economic impact on society</td>
<td>-600m</td>
<td>-4%</td>
<td>Reduction of the loss of money for individuals based on the actual loss of money (€2bn)</td>
</tr>
<tr>
<td>Businesses</td>
<td>-9bn</td>
<td>-4%</td>
<td>Reduction of the loss of money for businesses based on the actual loss of money (€300bn)</td>
</tr>
<tr>
<td>Individual victims</td>
<td>-240,000</td>
<td>-4%</td>
<td>Reduction of the number of citizens affected based on the actual number (8m)</td>
</tr>
</tbody>
</table>

Table 7.11: Administrative burden for MS

<table>
<thead>
<tr>
<th>Information obligation</th>
<th>Time spent</th>
<th>Frequency per annum</th>
<th>Av. wage rate</th>
<th>Total admin cost per obligation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reporting on the Directive (one report per annum)</td>
<td>2 weeks with 8 hours à day</td>
<td>One time</td>
<td>18</td>
<td>1,440</td>
</tr>
<tr>
<td>Gathering of information</td>
<td>1 week with 8 hours à day</td>
<td>One time</td>
<td>18</td>
<td>720</td>
</tr>
<tr>
<td>Provision of information per authority</td>
<td>1 day</td>
<td>Every month per authority</td>
<td>18</td>
<td>1,728</td>
</tr>
</tbody>
</table>

(ii) Legislative and institutional changes (score: 3)

This would involve introduction of **identity theft as a criminal offence with regard to primary victims** in those Member States that currently have not adopted relevant legislation. As concerns impacts on different Member States, only three countries (Czech Republic, Italy and Ireland) have confirmed to have legislation in place that covers primary victims before a secondary crime has been committed. In other countries, primary victims are generally covered when a secondary crime has been committed. Hence, in all Member States except these countries, a change in the approach of the legislation would be required. Legislative changes are also likely to need to be made in the three countries where legislation already exists to make sure that the common definition is covered.
As concerns institutional impacts, improved capacity to deal with identity theft and related crime due to an increased knowledge base of this crime as statistics on the covered cases would need to be collected. As concerns impacts on different Member States, all Member States already cover secondary crimes for which “stolen” identity information has been used. This said, all Member States can be expected to have to change their legislation in order to comply with the common definition and establish a specific offence.

(iii) Feasibility (score: 2)

Whilst the vast majority of stakeholders (93.8%) have pointed out that a common definition would be welcome, a number of countries consider it too early to intervene at the stage of primary victims. This is deeply rooted in criminal traditions and the adoption of a Directive is therefore likely to be challenging from a political perspective. Furthermore, agreeing on a common definition has been pointed out by many to be problematic. With regard to practical feasibility, in the second expert workshop some participants pointed out difficulties in relation to enforcing aspects of the definition relating to e.g. intent and how to draw the line concerning when identity theft has occurred, in particular in the online environment.

Conclusions (total average score: 2.9)

To conclude, the adoption of a Directive would be a clear statement that identity theft is not acceptable and that common action is taken to deal with this problem. Benefits that would result from the implementation of this option are limited to primary victims, which would gain access to support and redress. The policy option would also serve a capacity building purpose by means of the information collection requirements. The policy option would have a strong focus on redress and restorative action in tackling the problem. The fact that the option does not contain any explicit preventative measures except for collecting data on cases (which could be used for capacity building purposes) is a weakness.

Policy Option 3.2: Adoption of a Directive on identity theft and related crime, i.e. including both primary and secondary victims (maximalist approach)

Under this option, a Directive – maximalist approach – would be established. The Directive would cover all elements that are set out above in relation to Policy Option 3.1. In addition, the following aspects would be covered:

- Secondary victims; and
- Harmonisation of penalties for not only identity theft (i.e. targeting primary victims) but also related, secondary crime.
(i) **Achievement of the policy objectives (average score: 3.3)**

The policy option would have similar impacts to Policy Option 3.1. However, the **impacts would extend to secondary victims**. While the option would lead to increased harmonisation and a common understanding of the problem, the added value in relation to secondary victims is expected to anyhow be rather limited, since the Member States already have legislation in place that cover secondary crime.

As concerns the individual objectives, similar to Policy Option 3.1, the adoption of a **Directive** concerning identity theft and related crime at the EU level would make it clear that it is seen as a priority to combat this type of crime and the importance of taking common action. It is likely that this would have a deterrent effect and thereby lead to a slight reduction in identity theft and related crime, as some of the perpetrators may abstain from acquiring identity information if the actual gathering / collection of data would be a criminal offence. Short term, the number of acknowledged victims could increase since primary victims would be acknowledged as victims across the EU.

As a result of this policy option primary victims are acknowledged in law across the EU and it is ensured that this group of victims has access to redress. The policy option would also ensure that secondary victims have the same right to redress across the EU. This would in turn have positive impacts on **safeguarding fundamental rights**.

As concerns the **improvement of capacity and knowledge building**, the policy option would result in the same impacts as PO 3.1, but on a greater scale, since secondary victims would also be covered and because information collection activities would cover both types of victims. Indeed, the policy option would require the Member States to collect data concerning cases of identity theft concerning both primary and secondary victims. While it is likely that not all cases will be reported, such data could provide insights into the extent and evolution of the problem.

(ii) **Economic and social impacts (scores: 4 and 4)**

Similar impacts as for PO 3.1 are expected, but on a wider scale since secondary victims would also be covered:

**Table 7.12: Financial and economic impacts**

<table>
<thead>
<tr>
<th>Financial impacts</th>
<th>Costs or benefits (EUR)</th>
<th>Change in %</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Financial costs</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EU Commission</td>
<td>Min. app.: 22,000</td>
<td>n/a</td>
<td>Costs for developing a Directive</td>
</tr>
<tr>
<td></td>
<td>Max. app.: 30,000</td>
<td></td>
<td>Min.: based on Commission FTE level A8 for five months</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Max.: one Commission FTE level A8 for eight months</td>
</tr>
<tr>
<td>MS</td>
<td>8,640</td>
<td>n/a</td>
<td>Costs are calculated at three</td>
</tr>
</tbody>
</table>
Impact Assessment

<table>
<thead>
<tr>
<th>Financial impacts</th>
<th>Costs or benefits (EUR)</th>
<th>Change in %</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial costs</td>
<td></td>
<td></td>
<td>months implying 20 working days per month for one FTE with average wage rate of 18€ per hour.</td>
</tr>
<tr>
<td>Economic impacts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Economic impact on society</td>
<td>-600m</td>
<td>-4%</td>
<td>Reduction of the loss of money for individuals based on the actual loss of money (€20bn)</td>
</tr>
<tr>
<td>Businesses</td>
<td>-9bn</td>
<td>-4%</td>
<td>Reduction of the loss of money for businesses based on the actual loss of money (€300bn)</td>
</tr>
<tr>
<td>Individual victims</td>
<td>-240,000</td>
<td>-4%</td>
<td>Reduction of the number of citizens affected based on the actual number (8m)</td>
</tr>
</tbody>
</table>

Table 7.13: Administrative burden for MS

<table>
<thead>
<tr>
<th>Information obligation</th>
<th>Time spent</th>
<th>Frequency per annum</th>
<th>Av. wage rate</th>
<th>Total admin cost per obligation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reporting on the Directive (one report per annum)</td>
<td>6 weeks with 8 hours a day</td>
<td>One time</td>
<td>18</td>
<td>4,320</td>
</tr>
<tr>
<td>Gathering of information</td>
<td>3 week with 8 hours a day</td>
<td>One time</td>
<td>18</td>
<td>2,160</td>
</tr>
<tr>
<td>Provision of information per authority</td>
<td>3 day</td>
<td>Every month per authority</td>
<td>18</td>
<td>432</td>
</tr>
</tbody>
</table>

(iii) Legislative impacts (score: 5)

The policy option would require that a common definition is adopted and that both primary victims and secondary victims are covered. More specifically, with regard to primary victims, this would imply that in all Member States except Ireland, there would be a change in the approach of the legislation. Legislative changes are also likely to need to be made in Ireland to make sure that the common definition is covered. As concerns secondary victims, while all Member States already cover secondary crimes for which “stolen” identity information has been used, it can be expected that all Member States have to change their legislation in order to comply with the common definition and
establish a specific offence. As concerns the institutional impacts of the establishment of
a network, the impacts are likely to be similar across the Member States, except for the
Netherlands, where a well-developed support structure is already in place.

(iv) Feasibility (score: 1)

Overall, the same arguments that are made for PO 3.1 can also be made for this policy
option. However, the overlap with existing national legislation concerning secondary
victims is as an additional problem that impacts negatively on the feasibility of adopting
the policy option.

Conclusions (total average score: 3.3)

Similar to PO 3.1, the adoption of a Directive would be a clear statement that
identity theft is not acceptable and that common action is taken to deal with this
problem. The main added value would result from the common language in
terms of the definition of identity theft and related crime.

The same weakness as was pointed out for PO 3.1 in terms of the focus on
redress and restorative action and no explicit preventative action is, however, also
valid for this option. Furthermore, the policy option can be viewed a highly
controversial. More specifically, agreeing on a common definition is likely to be
challenging, and the added value in terms of covering secondary victims at the
EU level when these crimes are already covered at the national level is likely to
be questioned.

7.6 Policy Option 4: Combined Action

Policy Option 4: Combination of Policy Options 2.1, 2.2 and 3.1

Combination of Policy Options 2.1, 2.2 and 3.1:

• Policy Option 2.1: Sharing of experience and knowledge concerning the
  problem of identity theft via an electronic platform

• Policy Option 2.2: Establishment of a network of national contact points,
  which would be tasked with running, in each Member State, a one stop shop
  for victims of identity theft, act as a monitoring body and organise awareness
  raising activities

• Policy Option 3.1: Adoption of a Directive on Identity Theft, focusing on
  primary victims (minimalist approach)

The impacts will be similar to those outlined for policy option 2.4, but stronger, since
there would be a requirement for the Member States to adopt common legislation on
primary victims; this would not be voluntary as in PO 2.4. The ratings are as follows:

• Achievement of the policy objectives - average score: 4.7;
Impact Assessment

- Economic and social impacts - scores: 5 and 5;
- Legislative impacts - score: 5; and
- Conclusions - total average score: 4.7.

Estimates of the financial and economic impacts are provided in the following tables:

Table 7.14: Financial and economic impacts

<table>
<thead>
<tr>
<th>Financial impacts</th>
<th>Costs or benefits (EUR)</th>
<th>Change in %</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Financial costs</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EU Commission</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Portal:           | 250,000                 | n/a         | Portal: Design, set up and maintenance over a 2-3 years period (based on costs for EMN).
| Network:          |                         |             | Network: minimum and maximum costs per annum (60,000 euro plus 20,000 to 200,000 euro per Member State) |
| Min.: 600,000     |                         |             |          |
| Max.: 5,500,000   |                         |             |          |
| Recommendation    |                         |             |          |
| App. €14,000      |                         |             |          |
| Directive         |                         |             |          |
| Min. app.: 15,000 |                         |             |          |
| Max. app.: 22,000 |                         |             |          |
| MS Directive      | 2,880                   | n/a         | Transposition of Directive Administrative burden (see below) |
| Admin burden      |                         |             |          |
| Economic impacts  |                         |             |          |
| Economic impact on society | -1,000m | -5% | Reduction of the loss of money for individuals based on the actual loss of money (€20bn) |
| Businesses        | -15bn                   | -5%         | Reduction of the loss of money for businesses based on the actual loss of money (€300bn) |
| Individual victims | -400,000 | -5% | Reduction of the number of citizens affected based on the actual number (8m) |
Impact Assessment

Table 7.15: Administrative burden for MS

<table>
<thead>
<tr>
<th>Information obligation</th>
<th>Time spent</th>
<th>Frequency per annum</th>
<th>Av. wage rate</th>
<th>Total admin cost per obligation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide information for the portal</td>
<td>1 FTE, 1 month month with 20 working days</td>
<td>One-off cost</td>
<td>18</td>
<td>2,880</td>
</tr>
<tr>
<td>Reporting on the Directive (one report per annum)</td>
<td>2 weeks with 8 hours à day</td>
<td>One time</td>
<td>18</td>
<td>1,440</td>
</tr>
<tr>
<td>Gathering of information</td>
<td>1 week with 8 hours à day</td>
<td>One time</td>
<td>18</td>
<td>720</td>
</tr>
<tr>
<td>Provision of information per authority</td>
<td>1 day</td>
<td>Every month per authority</td>
<td>18</td>
<td>1,728</td>
</tr>
</tbody>
</table>

As concerns the feasibility of the policy option, it can be noted that while the non-legislative elements are likely to be welcomed, the proposal for a common definition and establishment of identity theft as a criminal offence already at the stage of primary victims is likely to be controversial. Some Member States have expressed that they would not accept intervention at such an early stage in the process.

7.7 Political feasibility of the policy options

The results of the CSES online survey concerning the different types of options are presented below. In the online survey, close to 50% of the respondents were in favour of legislative action, whereas just over 15% were in favour of non-legislative action. Less than 5% indicated that no EU action should be taken, which is a very low figure. On the other hand, as 30% stated that they do not have an opinion, which can be considered to be high. As noted above, similar results were recorded among different stakeholder groups.

Figure 7.1: Overall, what approach do you favour to combating the problem of identity theft and identity-related crime at an EU level?
7.8 Monitoring and Evaluation

Any performance measurement system should involve establishing a baseline and then monitoring progress from this towards targets that represent the achievement of objectives.

In relation to the first of these components, a number of possible baselines have been established in this report, specifically in Sections 3 and 4 which defined and quantified the various manifestations of the identity theft problem. The performance indicators needed to monitor and evaluate progress towards the objectives of any EU level intervention could be based on the following framework:

---

Figure 7.2: What action should be taken to combat the problem of identity theft and identity-related crime? [196]

<table>
<thead>
<tr>
<th>Issue</th>
<th>Percentage 0</th>
<th>Percentage 20</th>
<th>Percentage 40</th>
<th>Percentage 60</th>
<th>Percentage 80</th>
<th>Percentage 100</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establishment of a common definition of identity theft and identity-related crime</td>
<td>02</td>
<td>34.5</td>
<td>80.0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Establishment of identity theft as a criminal offence in the EU</td>
<td>08</td>
<td>18.5</td>
<td>69.2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Harmonisation of penalties for identity theft among EU Member States</td>
<td>08</td>
<td>27.7</td>
<td>58.5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Introduction of reporting mechanisms for victims of identity theft in all EU Member States</td>
<td>08</td>
<td>21.8</td>
<td>64.6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Establishment of platforms for victims and specialists to share experience and knowledge</td>
<td>02</td>
<td>40.0</td>
<td>53.8</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information and awareness raising campaigns targeting LEAs and the judiciary</td>
<td>02</td>
<td>59.2</td>
<td>67.7</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organisation and funding of expert meetings, e.g. involving academics, representatives of LEAs</td>
<td>02</td>
<td>41.5</td>
<td>58.8</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EU funding of programmes to improve knowledge sharing, identification and validation of good...</td>
<td>02</td>
<td>30.8</td>
<td>66.2</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[196] This Chart is based on the answers by the 73% that stated that action should be taken.
**Impact Assessment**

**Table 7.16: Basic Monitoring Framework**

<table>
<thead>
<tr>
<th>Policy Options</th>
<th>Outputs</th>
<th>Results</th>
<th>Impacts</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1: Electronic platform to share know-how</td>
<td>Setting up the electronic platform</td>
<td>Extent to which the electronic platform is used to share information</td>
<td>Improved understanding by authorities of identity theft and measures to combat it</td>
</tr>
<tr>
<td>2.2: Network of contact points</td>
<td>Setting up the network of contact points</td>
<td>Extent to which contact points are used by victims and related actions (as above)</td>
<td>Dissemination of information and raised public awareness of identity theft/reduced number of cases</td>
</tr>
<tr>
<td>2.3: Commission Recommendation and other actions</td>
<td>Adoption of Recommendation</td>
<td>Agreement on common definition and related actions (as above)</td>
<td>Joint working at EU level to implement measures to combat identity theft/reduced number of cases</td>
</tr>
<tr>
<td>3.1: Directive – primary victims</td>
<td>Adoption of Directive</td>
<td>Measures to protect primary victims</td>
<td>Reduced number of identity theft cases</td>
</tr>
<tr>
<td>3.2: Directive – primary and secondary victims</td>
<td>Adoption of Directive</td>
<td>Measures to protect primary and secondary victims</td>
<td>Reduced number of identity theft cases</td>
</tr>
</tbody>
</table>

Outcomes becomes progressively more difficult to measure as the nature of the effects changes from being essentially physical (outputs) to being more socio-economic (impacts). Similarly, the cause and effect relationship becomes less easy to determine.

The precise type of monitoring and evaluation arrangements put in place will depend on which, if any, of the Policy Options is implemented. The tasks of devising the performance indicators could be entrusted to the network of experts foreseen under Policy Option 2. In addition to on-going monitoring, there would need to be periodic evaluations to assess the impact of any EU interventions.
Impact Assessment

7.9 Conclusions – Impact Assessment

As a way of combining different aspects of the assessment, the following table provides a high level summary of the impacts that the research suggests are likely to come about (vertical axis) in relation to different policy options (horizontal axis) using the ‘high level’ criteria set out as part of the intervention logic in Section 3. The status quo is not included as it is rated as neutral.

Summary of Key Impacts

Key: ● = low score; ◆◆◆◆◆ = high score

<table>
<thead>
<tr>
<th>Impact/Policy Options</th>
<th>2.1</th>
<th>2.2</th>
<th>2.3</th>
<th>2.4</th>
<th>2.5</th>
<th>3.1</th>
<th>3.2</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relevance</td>
<td>●</td>
<td>◆◆</td>
<td>◆◆</td>
<td>◆◆</td>
<td>◆◆</td>
<td>◆◆</td>
<td>◆◆</td>
<td>◆◆◆◆</td>
</tr>
<tr>
<td>Effectiveness</td>
<td>●</td>
<td>◆◆</td>
<td>◆◆</td>
<td>◆◆</td>
<td>◆◆</td>
<td>◆◆</td>
<td>◆◆</td>
<td>◆◆◆◆</td>
</tr>
<tr>
<td>Efficiency</td>
<td>●</td>
<td>◆◆</td>
<td>◆◆</td>
<td>◆◆</td>
<td>◆◆</td>
<td>◆◆</td>
<td>◆◆</td>
<td>◆◆◆◆</td>
</tr>
<tr>
<td>Impact and added value</td>
<td>●</td>
<td>◆◆</td>
<td>◆◆</td>
<td>◆◆</td>
<td>◆◆</td>
<td>◆◆</td>
<td>◆◆</td>
<td>◆◆◆◆</td>
</tr>
<tr>
<td>Feasibility</td>
<td>◆◆◆◆</td>
<td>◆◆◆◆</td>
<td>◆◆◆◆</td>
<td>◆◆◆◆</td>
<td>◆◆◆◆</td>
<td>◆◆◆◆</td>
<td>◆◆◆◆</td>
<td>◆◆</td>
</tr>
</tbody>
</table>

Overall, according to our assessment, Policy Option 4 is likely to have the biggest impact on identity theft as it would provide a comprehensive framework, addressing the current legislative gap in relation identity theft for primary victims (Policy Option 3.1), and with the legal means to enforce penalties, as well as introduce non-legislative measures in the form of an online platform and a network of contact points. Whether such a measure would be an effective deterrent to the perpetrators of identity theft beyond the modest impacts we have estimated is impossible to say but it would make it easier to tackle the consequences.

The main disadvantage of Policy Option 4 is that it would be more difficult to implement as it presupposes agreement between EU Member States on the need for action at an EU level, on adopting a common identity theft and the other provisions that a Directive would introduce. Policy Option 2 would be easier to implement but would not have the same impact on the problem.
Below we provide a summary of the main finding of the assignment ‘Study for an Impact Assessment on a proposal for a new legal framework on identity theft’. The study is being undertaken for DG Home Affairs (DG HOME) by the Centre for Strategy & Evaluation Services (CSES) in cooperation with Deloitte.

The study has been launched to inform the Commission’s Impact Assessment on a possible new legislative instrument to help combat identity theft.

8.1 Problem of Identity Theft

Stolen data that are used maliciously (either directly by the person who ‘stole’ it or by a third party that acquired it) has impacts on individuals, businesses and/or public sector institutions. A distinction can be made between the costs to the ‘primary victim’, that is, the person whose identity is abused, and the ‘secondary victim’, i.e. the third party who is defrauded or otherwise harmed by the perpetrator impersonating the primary victim.

8.1.1 Drivers of Identity Theft

The key driver of the problems is the ‘motivation’ or incitement for criminals to obtain identity information because of the benefits (in particular of financial nature) for them. Insufficient or ineffective prevention activities as well as ineffectiveness and inefficiencies in national legal and institutional frameworks, as well as lack of cross-border collaboration, make these types of criminal activities easier. In this sense, they are not drivers per se but rather weaknesses that make it easier for criminals to commit and get away with this type of crime. Lack of awareness helps explain why victims of identity theft have displayed various forms of risky behaviour.

Online identity theft accounts for the bulk of the known cases. Online ID theft activities include spamming, phishing and the use of spyware. Offline ‘real world’ ID theft activities involve, for example, passport forgery, counterfeit of fingerprint identification, forgery of administrative and official state-issued documents. According to a 2008 study for PayPal, a quarter of the respondents said they were very concerned about identity theft. More recently, a 2011 Eurobarometer survey indicates that more than 40% of European Internet users have been asked to disclose more information than required for accessing or using a service on the Internet. A Generation Y online survey in April 2010 highlighted the fact that it is often young adults often engage in risky online behaviour. Over seven out of ten stated that they were not always as careful as they should be when posting and accessing information online.

As concerns the types of crime for which identity-related information is used, according to the survey results the key incentives for criminals are financial fraud and money laundering. Human trafficking and the transfer / selling of identity information are suggested to be less frequent motivations. Identity information is, however, also used for further types of crime, including illegal health care access, terrorism, drugs trafficking, illegal immigration and bullying and damaging people’s reputation.
8.1.2 Scale of the Problem

Identity theft and identity-related crime affects a considerable proportion of the population, and that the problem is increasing. Our estimate suggests that as many as 8.2 million individuals are affected by identity theft (2% of the EU's population) with an average loss of around €2,500 or €20bn at the EU level. There are also indirect financial costs of identity theft arising from damage to an individual's credit rating, the cost of rectifying the consequences of identity theft (e.g. replacing documents), as well as non-financial impacts of an adverse nature such as stress and reputational damage. Fundamental rights issues are also relevant. Bearing in mind that some identity theft goes undetected or is not made known for statistical purposes, this estimate is likely to be on the low side.

The costs of identity theft to European business are more difficult to estimate because very little research has been undertaken. Our estimate is that business losses could be as high as €500bn or 0.4% of EU GDP. Businesses are affected both as 'primary' and 'secondary' victims. Of these two categories, the second is easier to estimate and is likely to be similar to the estimate provided above for the number and value of identity theft cases for individual European citizens because these losses are ultimately borne by businesses (insurers, banks, etc.), either directly as a result of settling claims for reimbursement, or because of the need to invest in systems to help minimise the risk of identity theft. (The ultimate net loss, i.e. cases of identity theft-related financial losses where is not possible to recover the sums involved from the perpetrators is not possible to estimate).

Although the scale of identity theft affecting the private sector directly is more difficult to estimate, there is some useful evidence from several Member States. For example, according to data from the UK, the banking industry lost EUR 19.5 million in 2009 as a result of forged cheques (a genuine cheque, stolen and used by a fraudster with a forged signature) and a further loss of EUR 624 million from plastic card, online banking fraud and telephone banking fraud in 2009. The UK telecommunication industry suffered losses in 2009 of around EUR 830 million in the same year as a result of identity theft-related fraud.

Public authorities can also be victims of identity theft when their means of identification are used by someone else. This could be done via illegal access to data bases, the forgery of official documents etc. Similar to businesses, public authorities are also used as a source of information to access personal data of data subjects, including staff and clients. Section 4 elaborates on the scale of the problem.

According to the survey results for this study, identity theft is increasing and seen as having a pronounced European/cross-border dimension. Indeed, only one of the respondents who answered this question indicated that there is no cross-border dimension to the problem, while close to 70% of the respondents considered that there is a 'quite' or 'very' significant cross-border dimension. A disproportionate number of perpetrators were, in the survey, indicated to be based in and the proceeds of identity
theft go to countries mainly outside of the EU, although a few EU Member States were mentioned by the respondents. These were Romania, Spain, UK, “Eastern Europe”, France, Italy and Poland.

In addition to the loss of money, identity theft can have non-financial consequences for victims. This can include the time and cost associated with cleaning up identity and may have tort implications in some cases. In addition, identity theft may have non-financial effects including psychological and social distress as well as trust implications and limitations of the fundamental rights of data protection and privacy. Furthermore, there are costs to the wider public including enforcement costs and costs associated with crimes that were facilitated by identity-related crimes (e.g. money laundering, illegal immigration etc.). Ultimately, these effects will impact on the extent to which the European area of justice, freedom and security can be realised.

8.2 Definitional Issues and Existing National Legislation

At present, only some EU Member States have enacted specific 'identity-related crime' or 'identity theft' legislation. According to a “Comparative study on legislative and non-legislative measures to combat identity theft and identity related crime” (the 2011 “RAND report”) these are Estonia, France and Slovenia. More recently, according to the present assignment Poland introduced specific provisions in 2011. In the survey we asked for opinions on how effective legislation is in relation to the prosecution of identity theft and identity-related crime (e.g. whether all cases of identity theft and identity-related crime currently covered or there are gaps). A relatively low proportion of the respondents consider existing national legislation to be effective in combating identity theft.

7.2.1 National Legislation and Measures

In many countries, identity theft is tackled mainly through legislation on fraud. Examples of where this is the case include Belgium, Czech Republic, Bulgaria, Germany and the UK. The absence of specific legislation on identity theft does not mean that identity theft is not criminalised in the Member States whose laws do not refer to the identity-related element of the act concerned. Most of the Member States where this is so instead use legal provisions on fraud or forgery and thus do not commonly refer to identity ‘theft’ but rather to ‘fraud’. Furthermore, the mere ‘theft’ of an identity is not always considered a crime but rather it is the use made of the identity acquired illegitimately that takes the conduct into the criminal area. In this way, identity theft is considered as a preparatory act for committing another, independently criminalised offense and not as an act that is criminalised in its own right.

In a written survey with the Member States, to which 18 countries replied, three countries (Czech Republic, Italy and Ireland) confirmed that primary victims are covered in national legislation before a secondary crime has committed. This said, the legislative situation in other Member States is not clear-cut, and there are opportunities for primary victims to obtain redress in certain cases also in other Member States. In many
Summary & Overall Conclusions

countries, primary victims are covered once a secondary crime has been committed by means of the stolen identity information.

Currently in the EU there is neither a common terminology used to describe the phenomenon of identity theft (Member States use ‘Identity Theft’, ‘Identity Fraud’ and ‘Identity-related Crime’) nor a common legal definition of it. The extent to which and in what way this general phenomenon is recognised and criminalised in Member States is determined by national laws and the approach taken by the different national legal systems varies considerably.

7.2.2 Scope for EU Action

The absence of a common definition is a complication in developing a strategy at an EU level to combat identity theft. Most experts consulted as part of the study thought that it would be helpful to have a common definition. However, they suggested that it would be very difficult to agree on one and suggested that it should perhaps remain a guideline rather than a legally binding text. Others argued for making a common definition as comprehensive as possible and as ‘operational’ as possible. It was argued that provisions for ‘dishonest intent’ would have to be included in any common definition as a requirement for criminal conduct in this area.

Any EU-wide legal framework on identity theft should achieve not only a harmonised and consistent framework but one that creates scope for practical measures to counter the phenomenon. Two broad approaches are possible to developing a common EU definition – a ‘fully-functional’ common EU definition of identity-related crime or a more flexible definition focusing on key principles.

The advantage of the first “fully-functional” approach is that it would: clarify the exact nature of the conduct that needs to be criminalised; make clear that the crime is one of conduct rather than one defined in terms of the result of the activity, which in a multifaceted and rapidly developing area risks serious limitations and anomalies; and enable more precise gathering of statistical data and improved monitoring of progress in combating identity-related crime.

The factors in favour of a less specific approach include leaving the Member States free to define criminal conduct with respect to identity theft in the way most consistent with, and appropriate to, their own legal systems. A suggested working definition of identity theft is provided in the report.

8.3 Policy Options and Impact Assessment

The rationale for EU intervention is that identity theft and identity-related crime is affecting a significant proportion of the EU’s population, as well as businesses and public institutions, and that action at an EU level could help to tackle the problem. As noted earlier, cautious estimates suggest that a range between 2 million and 8 million individuals could be affected per annum and that costs can be estimated at 20 billion euro per annum. Secondly, the identity theft has transnational aspects and other
features that mean that effective action to tackle the problem requires intervention at an EU level.

8.3.1 Policy Objectives

EU policy objectives are summarised below:

<table>
<thead>
<tr>
<th>General objectives</th>
<th>Specific objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>To combat identity theft and identity related crime</td>
<td>• To reduce identity theft and related crime.</td>
</tr>
<tr>
<td>More generally, to promote security, combat crime and protect victims’ rights</td>
<td>• To improve the capacity to prevent and tackle identity theft and related crime both in the public and private sectors, including in relation to cross-border aspects of the problem, at national and EU level.</td>
</tr>
<tr>
<td></td>
<td>• To ensure that primary and secondary victims of identity-related crime obtain support and redress.</td>
</tr>
<tr>
<td></td>
<td>• More generally, to safeguard fundamental rights, including in particular:</td>
</tr>
<tr>
<td></td>
<td>- Right to liberty and security (Art. 6);</td>
</tr>
<tr>
<td></td>
<td>- Respect for private and family life (Art. 7) and protection of personal data (Art. 8);</td>
</tr>
<tr>
<td></td>
<td>- Right to property (Art. 17);</td>
</tr>
<tr>
<td></td>
<td>- To protect consumers (Art. 38), whose identity information may be acquired and abused in relation to online shopping, as well as shopping in the offline world and thus have a negative impact on consumer protection. This is also a fundamental right.</td>
</tr>
<tr>
<td></td>
<td>- Right to an effective remedy and to a fair trial (Art. 47)</td>
</tr>
<tr>
<td></td>
<td>• To protect businesses, in particular SMEs which tend to be more vulnerable to identity theft and its consequences than larger firms.</td>
</tr>
<tr>
<td></td>
<td>• To improve the knowledge base regarding identity theft and related crime.</td>
</tr>
<tr>
<td></td>
<td>• To prevent the risk of forum shopping in relation to identity theft and related crime in the EU.</td>
</tr>
</tbody>
</table>

Work is currently on-going at the EU level both in terms of preventative measures (e.g. concerning the security of online systems) and in terms of aggravated penalties if someone’s identity is used and creates damage to the owner in an online environment. It is important that any new initiative builds on these and other initiatives.

8.3.2 Policy Options

There are a number of policy options ranging from maintaining the status quo to legislative intervention to criminalise identity theft across the EU:

**Policy Option 1 – Status quo:** this option would be relevant if it is determined that the problem is not of such a nature to justify an initiative at the EU level to help combat identity theft. It might also be argued that the nature of the problem is such that EU
intervention is unlikely to be effective. The feedback obtained from the research suggests that most stakeholders are not content with a status quo situation. The CSES survey results show that the majority of the respondents (86.7%) think that there is a need for EU action to tackle identity theft, especially given the transnational nature of the problem and its manifestations. Furthermore, the expert workshops and other consultations also suggest that there is a need for EU action.

**Policy Option 2 – Non legislative action:** could involve the establishment of a platform for victims and specialists to share experience and knowledge (Sub-option 2.1); information exchange and awareness raising targeting law enforcement authorities and the judiciary (Sub-option 2.2); and a Commission Recommendation on a common definition and various other measures to reduce the current fragmentation of approaches (Sub-option 2.3). Feedback from the research suggests that Policy Option 2.2 has widespread support but is not, in itself, a sufficient response to the growing problem of identity theft. Policy Option 2.1 is the least favoured sub-option amongst those we consulted. With regard to sub-option 2.3, the adoption of a common definition of identity theft is seen as essential if Member States are to work more closely together, and with the Commission, to tackle the problem of identity theft.

**Policy Option 3 – Legislative intervention:** could involve two sub-options. Firstly, adoption of a Directive on identity theft, focusing on primary victims - minimalist approach (sub-option 3.1); and secondly, adoption of a Directive on identity theft and related crime, i.e. including both primary and secondary victims - maximalist approach (policy option 3.2). The adoption of a common definition of identity theft is seen as essential if Member States are to work more closely together, and with the Commission, to tackle the problem of identity theft.

Combinations of policy options have also been assessed, including two combinations of the non-legislative options, as well one option combining the three non-legislative policy options and the legislative policy option 3.1.

**8.3.3 Assessment of Impacts**

As a way of combining different aspects of the assessment, the following table provides a high level summary of the impacts that the research suggests are likely to come about (vertical axis) in relation to different policy options (horizontal axis) using the ‘high level’ criteria set out as part of the intervention logic in Section 6. The status quo is not included as it is rated as neutral.
**Summary & Overall Conclusions**

**Summary of Key Impacts**

<table>
<thead>
<tr>
<th>Impact/Policy Options</th>
<th>2.1</th>
<th>2.2</th>
<th>2.3</th>
<th>2.4</th>
<th>2.5</th>
<th>3.1</th>
<th>3.2</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relevance</td>
<td>●</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>Effectiveness</td>
<td>●</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>Efficiency</td>
<td>●</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>Impact and added value</td>
<td>●</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>Feasibility</td>
<td>★★★★</td>
<td>★★★</td>
<td>★★★</td>
<td>★★★</td>
<td>★★★</td>
<td>★★★</td>
<td>★★★</td>
<td>★★★</td>
</tr>
</tbody>
</table>

Key: ● = low score; ★★★★★ = high score

Overall, according to our assessment, Policy Option 4 is likely to have the biggest impact on identity theft as it would provide a comprehensive framework, addressing the current legislative gap in relation identity theft for primary victims (Policy Option 3.1), and with the legal means to enforce penalties, as well as introduce non-legislative measures in the form of an online platform and a network of contact points. Whether such a measure would be an effective deterrent to the perpetrators of identity theft beyond the modest impacts we have estimated is impossible to say but it would make it easier to tackle the consequences.

The main disadvantage of Policy Option 4 is that it would be more difficult to implement as it presupposes agreement between EU Member States on the need for action at an EU level, on adopting a common identity theft and the other provisions that a Directive would introduce. Policy Option 2 would be easier to implement but would not have the same impact on the problem.

**Based on our research, a step by step approach is preferred by many actors.** Non-legislative action in the form that has been described above would be welcome including actions to share information, to help collect information and to oversee the development of an EU strategy to combat identity theft. In addition to these measures, a need for a Directive including a common definition of identity theft as a framework for further initiatives to combat identity theft in the future, including possible criminalisation is seen as useful by many of those consulted in the framework of the present study. Such an approach would demonstrate that the Commission is responding to the need for action to tackle the growing problem of identity theft with measures that are practical and add value to what Member States are already doing.