FIDIS

Future of Identity in the Information Society

Title:	"D12.7: Identity-related Crime in Europe – Big Problem or Big Hype?"
Author:	WP12
Editors:	Nicole van der Meulen (TILT, Netherlands) Bert-Jaap Koops (TILT, Netherlands)
Reviewers:	David-Olivier Jaquet-Chiffelle (VIP, Switzerland) Peter Sommer (LSE, UK)
Identifier:	D12.7
Type:	[Report]
Version:	1.0
Date:	09 June 2008
Status:	[Final]
Class:	[Public]
File:	fidis-wp12-del12.7-identity-crime-in-Europe.doc

Summary

In the United States, identity theft is portrayed as a big problem, although the actual size of the problem is contested. Following the US situation, public attention for identity theft in Europe is rising, but its prevalence is unknown. This report provides a first indication of the prevalence of identity theft in Europe, on which subsequent studies can build. For Belgium, France, Germany, and the United Kingdom, as well as the US, it sketches – as far as data are available – the prevalence of identity-related crime, vulnerabilities in financial and identification infrastructures, and legal, technical, and organizational countermeasures. It provides recommendations for policy makers not to focus only on generally accepted definitions or collecting prevalence data, but to conduct in-depth studies of the strengths and weaknesses of European financial and identification infrastructures in the information society.

The FIDIS NoE receives research funding from the Community's Sixth Framework Program

Copyright Notice

Members of the FIDIS consortium

1. Goethe University Frankfurt	Germany
2. Joint Research Centre (JRC)	Spain
3. Vrije Universiteit Brussel	Belgium
4. Unabhängiges Landeszentrum für Datenschutz	Germany
5. Institut Europeen D'Administration Des Affaires (INSEAD)	France
6. University of Reading	United Kingdom
7. Katholieke Universiteit Leuven	Belgium
8. Tilburg University	Netherlands
9. Karlstads University	Sweden
10. Technische Universität Berlin	Germany
11. Technische Universität Dresden	Germany
12. Albert-Ludwig-University Freiburg	Germany
13. Masarykova universita v Brne	Czech Republic
14. VaF Bratislava	Slovakia
15. London School of Economics and Political Science	United Kingdom
16. Budapest University of Technology and Economics (ISTRI)	Hungary
17. IBM Research GmbH	Switzerland
18. Institut de recherche criminelle de la Gendarmerie Nationale	France
19. Netherlands Forensic Institute	Netherlands
20. Virtual Identity and Privacy Research Center	Switzerland
21. Europäisches Microsoft Innovations Center GmbH	Germany
22. Institute of Communication and Computer Systems (ICCS)	Greece
23. AXSionics AG	Switzerland
24. SIRRIX AG Security Technologies	Germany

Versions

Version	*Date*	*Description (Editor)*
0.0	02.07.2007	• template circulated (BJK)
0.1	18.04.2008	• first integrated version (BJK)
0.2	09.05.2008	• second integrated version for internal review (NvdM)
1.0	09.06.2008	• final version (NvdM, BJK)

Foreword

FIDIS partners from various disciplines have contributed as authors to this document. The following list names the contributors for the chapters of this document.

Chapter	*Contributor(s)*
Executive Summary	Bert-Jaap Koops (TILT)
1 Introduction	Nicole van der Meulen, Bert-Jaap Koops (TILT)
2 Belgium	Els Kindt (ICRI)
3 France	Fanny Coudert (ICRI)
4 Germany	Maren Raguse (ICPP)
5 United Kingdom	Nicole van der Meulen (TILT)
6 United States	Nicole van der Meulen (TILT)
7 Conclusion	Bert-Jaap Koops, Nicole van der Meulen (TILT)

Table of Contents

Executive Summary

Identity-related crime can be defined as all punishable activities that have identity as a target or a principal tool. In the FIDIS typology, identity-related crime is a container concept for different forms of crime, including identity fraud and, the most conspicuous, identity theft: using the identity of another existing person, without her consent, for a fraudulent purpose.

In the United States, identity theft has become a household word, and media continue to tell fear-igniting stories of stolen identities. The actual size of the problem, however, is contested, so that identity theft might be a hype rather than a big problem in real life in the US. In recent years, the problem – or the hype – and the subsequent need for policies and countermeasures have spread from the US to other areas, including Europe. The real extent of the problem in Europe is unknown. Rather than relying on (contested) US data and concerns – which may or may not be quite specific for the US situation – a description of actual European prevalence of identity crimes will help put our concerns about identity theft in perspective.

This report tries to help provide such a picture by shedding light on the situation in Belgium, France, Germany, and the United Kingdom; these countries have been chosen as EU Member States that have a policy debate about identity-related crime, so that a certain amount of reports and data are available. In each country chapter, a picture of the prevalence of identity theft and other forms of identity-related crime is sketched, as well as information on vulnerabilities and countermeasures. Altogether, this report provides a first indication of the prevalence of identity theft in Europe, on which subsequent studies can build.

The resulting picture is, unfortunately, only a piecemeal one: studies appear scarce, and most authors point out how the lack of a separate criminal provision makes it more complicated to gather information on the problem, since crimes are not being specifically reported or registered as identity-related crime. Moreover, uncertainty and unclarity about definitions are dominating themes in many discussions with regard to identity theft. The unclarity about definitions and about the actual prevalence of identity theft prevent policy makers, or so they claim, to take action.

Nevertheless, the contours of our picture of the European prevalence of identity-related crime shimmer through the available data and reports. Document fraud is an on-going concern, with tens of thousands of cases yearly in countries like Belgium and France. The traditional forms of document forgery have been supplemented more recently with look-alike fraud, which is a major concern in several countries.

However, in the past few years, a shift is occurring from document and look-alike fraud to online forms of fraud, in particular financial identity fraud or identity theft. Phishing – which traditionally relies on luring ICT users by deceptive email messages to false websites – seems to be increasingly replaced by covert forms of fraud, in particular by botnets that assemble identity and personal data from infected computers.

Altogether, identity-related crime, particularly document forgery, look-alike fraud, and computer-related financial identity theft, are significant forms of crime that are on the rise. There is insufficient empirical evidence to call it a big problem yet, but the upward trend warrant taking expeditious measures to prevent it becoming a big problem in the first place.

Like the US, European countries are indeed taking countermeasures to combat identity-related crimes. This part of the picture is fairly clear and largely similar for the European countries studied. Rather surprisingly in view of regulatory traditions, in Europe, legal measures are

much less prominent than in the United States. Criminal law has not been adapted to accommodate identity crimes specifically; to a very large extent, existing provisions are an adequate basis for prosecuting identity-related crime. Apart from criminal law, other legal areas, like data-protection law and tort law, can also be used.

Other legislative measures taken in the US, like free credit reports, seem rather specific for the US situation. Some measures, for example mandatory truncation of credit card numbers on receipts, may nevertheless be valuable in Europe as well. Particularly laws requiring security breach notification have recently also become an issue in Europe. Such a system requires organizations to provide their customers with notification whenever they have lost personal information. This is a promising measure, although the danger of individuals becoming immune to frequent notifications must be taken into account.

Measures like those imposed in the US by legislation are often taken by the financial sector itself, or by public-private partnerships, in Europe. Financial institutions are acutely aware of the threat of identity theft, and they take the lead in enhanced technical and organizational security measures. Unlike in the US, these do not necessarily have to be backed up by legislation. A wide panorama of measures is visible, consisting of awareness raising campaigns, complaint centers, and innovative technical measures like virtual dynamic cards or enhanced transaction authentication numbers. Some potential solutions, however, are opposed by merchants and banks for economic reasons, suggesting that market failure – one of the reasons for the US to impose legal obligations – may not altogether be absent in Europe.

Welcome as all these countermeasures are, there is a snag. One countermeasure consistently showing up is to introduce general-purpose electronic identity cards and numbers, often backed up by biometrics, aimed at preventing document or look-alike fraud. The downside of such measures is that they introduce considerable vulnerabilities: as the resulting identification infrastructure comes to rely heavily on the unique eID method, the risk of identity theft actually rises, and the burden of proving being a victim of identity theft becomes heavier as the system is supposedly more secure. Thus, general-purpose eID cards and numbers to curb document fraud are a two-edged sword, and governments need to carefully consider and monitor emerging side-effects.

Perhaps the most important lesson of this report's survey is that countermeasures to combat identity-related crime are not always targeted at relevant vulnerabilities in the identification infrastructures. Europe has wisely chosen not to follow the United States too closely in choosing countermeasures, since identity theft in the US most likely stems from US-specific vulnerabilities in the financial system and market orientation, with its epidemic data brokers and lack of private-sector verification. However, a closer look is needed at vulnerabilities in the European situation itself. The current policy debate sometimes focuses still too much on document fraud and too little on online financial identity theft, and a comprehensive plan of attack to combat phishing by botnets rather than by fake websites has yet to be developed.

Therefore, rather than continue to harp on about generally accepted definitions, lack of data, and whether or not to start registering identity-related crime before countermeasures can be taken, a better approach to address the threat of identity-related crime may well be to start conducting more in-depth studies of the strengths and weaknesses of European financial and identification infrastructures in the information society. Now that identity theft is past the stage of big hype in the US, there is yet time to prevent it becoming a big problem in Europe.

1 Introduction

Identity-related crime can be defined as all punishable activities that have identity as a target or a principal tool.[1] In the FIDIS network, a typology of identity-related crime has been developed.[2] It is a container concept for different forms of crime: identity fraud, which includes identity theft[3] and unlawful identity delegation, exchange, or creation, but also unlawful identity obstruction and unlawful identity restoration. By far the most conspicuous of these is identity theft: using the identity of another existing person, without her consent, for some criminal – usually fraudulent – purpose.

Identity theft has become a household word over the past few years. This may have something to do with its thriller appeal, based on representations in movies of scary identity takeovers,[4] but more likely it is due to the fact that identity theft is now often called one of the fastest rising crimes in the world. In particular, it is a major concern in the United States. Media headlines continuously provide the public with the most fear-igniting stories, and the problem continues to take a rather prominent place on the political agenda.

Discussions about the prevalence of identity theft, however, have cast doubt on the actual size of the problem, creating the possibility that identity theft carries elements of a hype rather than a big problem in real life. Sources, from studies to complaint databases, provide different and at times conflicting results. This is problematic, particularly since figures from the United States – where most prevalance data are available – are often quoted by other countries to indicate the increasing threat of the crime, whereas the US data are particularly controversial as they largely stem from complaint centers. Chris Jay Hoofnagle, for example, writes "we are asking the wrong people about the crime. The surveys seek to obtain information about identity theft from its victims — individuals who have the most limited view of the problem. Victims often do not know how their personal data were stolen or who stole the information."[5] Hoofnagle refers to previous survey studies conducted on citizens and also the data obtained by the Federal Trade Commission which exclusively relies on consumer complaints. Hoofnagle therefore proposes a solution to the problems associated with obtaining reliable and insightful data. He suggests financial institutions ought to publicize the prevalence data they maintain on identity theft in order to help create an accurate picture of the size of the identity theft problem. The data provided by financial institutions could subsequently be a significant aid in the determination of the actual size of the problem and the potential countermeasures.

---

1 Koops, Bert-Jaap & Ronald Leenes (2006), 'ID Theft, ID Fraud and/or ID-related Crime. Definitions matter', *Datenschutz und Datensicherheit* 2006 (9), p. 553-556.

2 Leenes, R. (ed.) (2006), *D5.2b: ID-related Crime: Towards a Common Ground for Interdisciplinary Research*, FIDIS deliverable, available at http://www.fidis.net/; Koops, Bert-Jaap, Ronald Leenes, Martin Meints, Nicole van der Meulen & David-Olivier Jaquet-Chiffelle (2008), 'A Typology of Identity-related Crime: Conceptual, Technical, and Legal Issues', *Information, Communication & Society* (forthcoming).

3 It would be more correct to write *identity 'theft'* to indicate that the identity is not really stolen but rather abused, because normally the victim still retains her identity. In this report, however, we will conform to the regular practice and talk about *identity theft.*

4 Pintér, Róbert (ed.) (2007), *D5.2c: Identity related crime in the world of films*, FIDIS deliverable, available at http://www.fidis.net/.

5 Hoofnagle, C.J. (2007), "Identity Theft: Making the Known Unknowns Known", *21 Harvard Journal of Law & Technology* (1), p. 99.

In recent years, the problem – or the hype – and the subsequent need for policies and countermeasures have spread beyond the boundaries of the United States. Within the European Union, certain Member States have demonstrated similar problems. Notably the United Kingdom has produced figures and stories about the current danger of identity theft in its territory. The situation in other Member States, however, is rather vague, due to a lack of research and a growing uncertainty about the problem.

It is therefore urgently needed to get a clearer picture of the state of affairs concerning identity-related crime, in particular of identity theft, to draw more definite conclusions that can help to move forward the policy discussion and the taking of countermeasures. Rather than relying on (contested) US data and concerns – which may or may not be quite specific for the US situation – a description of actual European prevalence of identity crimes will help put our concerns about identity theft in perspective.

This report tries to help provide such a picture by shedding light on the situation in various EU Member States. In each country chapter, authors aim to paint an insightful picture of the situation based on available studies and national information on developments with regard to identity theft and other forms of identity-related crime. The chapters go beyond a discussion of mere prevalence data and also include information on vulnerabilities present in society and countermeasures available. The added value of these sections is significant. The analysis of vulnerabilities could provide crucial information with regard to the examination of which opportunities exist for perpetrators to commit identity-related crime within the different countries. The unveiling of opportunities is important in order to observe whether identity-related crime could become a big problem within certain countries and will allow countermeasures to be introduced specifically based on societal vulnerabilities. The discussion of countermeasures also indicates what has already been done against the problem, or which legal countermeasures apply, and what, as a result, should still be introduced in order to combat the issue. To find the gaps, one first needs to have an adequate overview of what already exists. Although figures on prevalence of identity-related crime appear scarce, the picture at least gives a first indication of the prevalence of identity theft in Europe, on which subsequent studies can build.

The following Member States are included in this report: Belgium, France, Germany, and the United Kingdom. We have chosen these not only because they are key countries in the FIDIS network that provided the infrastructure to write this report, but particularly because these countries have a policy debate about identity-related crime, so that a certain amount of reports and data are available.[6] In addition to the European countries, for comparative purposes, a chapter on developments, prevalence data and trends in the United States is included.

[6] In the newer EU Member States, identity-related crime hardly seems a public issue. For example, a preliminary study of the Czech Republic that was conducted for this report, revealed that no data or reports are available at all to indicate the prevalence of identity-related crime. There is no complaint center for victims, and identity-related crimes – if they occur – are not registered as such since the Czech criminal law does not use this concept. Currently, identity theft is not perceived as a problem in the Czech Republic; time will show whether this changes in the future, as online banking (currently at about 10% of bank users) and credit card use (with 2.4 million card holders and an increase rate of 12% in 2007) are on the rise.

2 Belgium

2.1 Concepts

The debate about identity-related crime

Since a couple of years, attention for identity-related crime is increasing in Belgium, and a debate about the use and abuse of identity (documents and data) and related crime is taking place. The debate was initially mainly limited to problems of document fraud, such as fraud with ID cards and especially with passports and travel documents. Blank documents (especially passports) were stolen and later illegally used,[7] identity documents were counterfeited,[8] existing identity documents were used by someone other than the owner to whom the document was issued (look-alike fraud)[9] or travel documents (such as visa[10]) were obtained in a fraudulent way. The discussion, however, has broadened. The debate now also includes problems with online authentication and the misuse of identity (data) and is intensified in the light of some recent cases of online credit card and identity fraud and theft.[11]

Although identity-related crime has always taken place, it remained nevertheless rather limited as compared with other countries, such as the United States and the United Kingdom. This may be partly explained by the fact that citizens in Belgium are since long obliged to carry identity cards. The identity card is the evidence of the registration in the population register kept by the government and can be used for identification purposes. The information on the identity card is an extract of the information kept in the population registers and the central National Register. In case of doubt, the identity of Belgian citizens could hence be easily verified.[12] When an identity document is stolen or lost, the citizen can, after filing a declaration of the theft or loss with the local police, obtain a new identity document without too many problems. The easiness to obtain a new identity document after an incident of theft could therefore also be a weakness. In order to file a declaration of theft or loss, the individual needs to submit a recent picture and any document that could prove her identity, such as a driver's license, but also other documents are accepted, such as evidence of registration in a health insurance service. After such a declaration, the procedure for the re-issuance of a new identity document starts automatically after fifteen days. The individual may also choose to

---

7 The theft of blank identity and passport documents has decreased since these blank documents are kept centralized and no longer in the local city halls. For the prevalence, see *below* and at footnote 28 and surrounding text.

8 Because of the increased security measures against counterfeit (such as holograms, color prints, etc), this type of identity fraud has decreased to some extent, although it remains difficult to detect a general trend (see also *below* and at footnote 28 and surrounding text).

9 See interview with J. Denolf of the Federal Police in X., 'Look-alike nieuwste documentenfraude', *De Standaard Online*, 18 September 2003, available at http://www.standaard.be/Artikel/Detail.aspx?artikelId=DST18092003_015&word=+look+alike+fraude#.

10 See, for example, the Recommendations of 4 February 2003 of the Commission for the Interior and Administrative Matters of the Senate, relating to trafficking in humans and visa fraud, which state that a better control on visa applications should be exercised and accurate procedures for the civil population registers re-established, for example in the Democratic Republic of Congo: *Proc*. Senate 2002-2003, 4 February 2003, n° 2-1018/3, available at http://www.senate.be/www/?MIval=/publications/viewPubDoc&TID=33620429& LANG=nl.

11 See *below* at footnote 78.

12 See also *below* about the identification procedures. The situations where individuals are obliged to show or submit their identity cards are limited. This does however not prevent individuals from voluntarily showing or submitting their identity card upon request. Refusal to do so could create suspicion.

immediately request a new identity document, in which case the previous (lost or stolen) identity document becomes immediately invalid. Perpetrators may abuse this system to obtain a new identity document to commit fraud.

The focus of the debate however is no longer only on document theft or fraud, but also on identity-related theft and fraud. These crimes are accelerating because of the increasing use of electronic communication services, in particular over the Internet, where the verification and authentication of identity is less obvious than in an off line environment. In addition, these new communication channels and technologies are sometimes misused to fraudulently obtain confidential information about individuals, such as personal and identity-related data. With this information, criminals attempt to gain access to bank accounts or to engage in contracts in the name of someone else.[13]

When the electronic version of the existing mandatory identity card for citizens was introduced in Belgium, it was highlighted that the eID card with its enhanced authentication functionalities offers the advantage that it can be used as a tool for combating fraud in an on-line environment.[14] The limited distribution of eID card readers and the rather limited number of applications which have been developed so far to allow the use of the eID, however, have resulted in a rather limited absorption at present of the benefits that the Belgian eID card could offer.[15]

Framework Note on Integrated Security

In 2004, the federal government adopted in a Framework Note on Integrated Security (hereinafter 'Framework Note') in which identity theft was identified, in the context of computer crime, as one of the priorities in crime prevention and combat. The Framework Note stressed that an integrated approach is needed which requires the cooperation between several services with attention for the victims. The Framework Note was prepared by the Service for Criminal Policy (*'Dienst voor het Strafrechtelijk Beleid')* which is part of the Federal Department of Justice. The Service for Criminal Policy advises the Minister of Justice.[16] The Service has been established in order to collect useful information, for example about the evolution of a specific crime, in order to be able to analyze and research the roots of the crime and to propose a policy to combat such crime. The Framework Note advocates taking action to combat identity-related crime not only on the regulatory level, but also on the level of prevention and repression. The figures which the Service presents or relies on, however, are not up to date. The figures of 2004 are still not finalized. One of the reasons is that the categorization of the central crime register is used. This categorization is based on a division of crimes in seven categories, which does on the one hand not allow one to draw detailed conclusions about the prevalence of identity-related crimes and on the other hand is too detailed (in total more than 2000 lines).[17]

---

[13] See in general, K. Draps, *Identiteitsfraude. Een routineactiviteitenbenadering*, Leuvense Universiteitsbibliotheek, Leuven, 2007, 103 p.

[14] For misuse of identity and the use of the electronic eID as a possible solution, see for example, Y. Delepeleire, 'Veilig chatten met eID', *De Standaard*, 15 September 2005, 10.

[15] See also D. De Cock, Ch. Wolf & B. Preneel, *The Belgian Electronic Identity Card, (Overview)*, available at http://www.cosic.esat.kuleuven.be/publications/article-769.pdf.

[16] For the home page, see http://www.dsb-spc.be/Joomla/index.php?lang=nl.

[17] See Service for Criminal Policy at http://www.juridat.be/statistique_dsb/inhoud/nl_index.htm . A conference was held on this topic on 6 and 7 December 2007 entitled 'De cijfers van de misdaad in debat' [Debating crime figures]. Information is available at http://www.quetelet.net/colloque%20.

The Framework Note is soon to be replaced by a new framework note for integrated security for the period of 2008-2011.

Definition of identity theft/fraud?

There is no specific provision in the Penal Code which punishes identity fraud or identity theft as such, or a legal definition of identity-related crime in Belgium. In March 2005, the Minister of the Interior was questioned in the Senate about figures on and trends in identity fraud/theft.[18] At that time, the Minister replied that identity fraud and theft can be defined as '*each kind of crime that consists in the fraudulent obtaining and using of the identity of someone else with the intent to commit fraud or other criminal activities, usually for economic gain*'. The Minister furthermore referred to four kinds of activities in which identity fraud and theft is involved: (1) phishing, (2) theft of web mail accounts or user identity, (3) hacking of computer systems and (4) the use of spyware for obtaining personal and banking data. It was impossible for both the Federal Department of Justice and the Federal Department of the Interior to provide any indication on the cost of identity fraud or identity theft because they had not conducted any in detail investigation of the issue.[19]

In June 2005, the Federal Forensic Police (Directorate economic and financial crime) ('*Directie economische en financiële criminaliteit*') organized a colloquium in Brussels entitled 'Identity fraud. Crime of the future ?'[20] There, identity fraud and identity theft were analyzed and discussed by national and international experts. The objectives of that colloquium included raising awareness, knowledge and alertness for identity-related crime. Identity-related crime was analyzed from different angles, including from the perspective of companies and the consequences of identity crime for their economic activities. Because there is no legal definition of identity crime or theft, each speaker made an attempt to give a definition. Some described identity theft as '*the fraudulent - whether or not short-lived - use of any identity data that belongs to another person*' and stressed that there are several ways such crime can appear (for example, phishing, key logging, account take, etc).[21] Another definition of identity theft that was used in order to assess whether the existing incriminations of the Belgian Penal code were sufficient was '*the 'theft' of someone else's personal information for later fraudulent use for committing various crimes*'.[22] These definitions fall under unlawful identity change (identity fraud) and identity theft in the categorisation of identity-related crime in the FIDIS typology.[23].

---

[18] *Questions and Answers* Senate 2004-2005, 21 March 2005, 3-45 (Question N° 3-2371 of Ms. Hermans), available at http://www.senate.be/www/?MIval=/publications/viewPubDoc&TID=50344709&LANG=nl

[19] Another reason why there are few figures about identity crime in companies, for example, is that the crime as such is not always recognized or, if detected, for commercial reasons, not reported.

[20] The colloquium took place in Brussels on 9 June 2005 in cooperation with the National Bank of Belgium and Politeia and was well attended. The contributions of the national and international speakers have been published in J. Denolf (ed.), *Identiteitsfraude. Misdrijf van de toekomst? Fraude d'identité. Le crime du future?* Politeia, Brussels, 2005, 116 p.

[21] M. Vervaenen & S. De Lil, 'Identiteitsdiefstal. Risico's voor ondernemingen en de politionele reactie' in J. Denolf (ed.), *o.c.*, (17), 19 - 24.

[22] D. Reynders, M. Taeymans & W. Cruysberghs, 'Identiteit en diefstal van identiteit. Een verkennende juridische duiding', in J. Denolf (ed.), *o.c.*, (31), 40.

[23] See Koops, Bert-Jaap, Ronald Leenes, Martin Meints, Nicole van der Meulen & David-Olivier Jaquet-Chiffelle (2008), 'A Typology of Identity-related Crime: Conceptual, Technical, and Legal Issues', *Information, Communication & Society* (forthcoming).

2.2 Prevalence

Computer crime reporting figures of the federal police (Federal Computer Crime Unit)

According to the annual report of the Federal Forensic Police (see also section 2.2.1), a record number of cases of computer crime was reported in 2006 to their central complaint site, in total 28,434 cases.[24] 23,883 cases concerned the reporting of 'Nigerian' fraud[25] and 2,422 cases concerned phishing. These two activities are increasing very fast, as reported.

	2002	**2003**	**2004**	**2005**	**2006**
Total, of which	2,360	7,739	12,002	17,490	28,434
ICT – crime	3	6	11	8	15
- Hacking	0	0	6	5	11
'Nigerian' fraud	1,640	6,885	7,760	11,181	23,883
Phishing	0	0	1,251	1,386	2,422

Table 2.1. Number of reported computer crime cases[26]

The Federal Police did not investigate all reported cases, but only a selection if enough details were submitted. The Federal Police also received an increasing number of requests to identify e-mail addresses (1320), IP addresses (37), pseudonyms, URLs, advertisements and mobile phone numbers, in total 1378 requests for 2006.[27] Such information is in some situations also relevant in investigations of identity related crime.

Document fraud reported by the Federal Police

The Fifth activity report of the Federal Forensic Police also reports on document fraud. Table 2.2 mentions the number of false identity cards (IK), passports (PP) and residence permits (VD) from 2001 until 2006 according to the type of fraud. [28]

As stated before, document fraud is in general decreasing (especially theft of blank documents (except residence permits), counterfeit and forgery). Because the figures are not showing trends in a consistent way, it remains difficult to draw definite conclusions from these figures.

---

[24] Federal Police. Directorate economic and financial crime, *Fifth activity report 2006*, p. 72. The number of 28,434 concern cases in which a crime was found or useful information relating to a crime, available at http://www.polfed-fedpol.be/pub/jaarverslag/pub_jaarverslag2006_nl.php.

[25] 'Nigerian' fraud is a practice by which criminals send e-mail messages to people, requesting their help to transfer (large) money sums; the victims are promised a percentage of the profit if they first send a sum of money. The victims never hear anything back, and lose the money. It also happens that the victims are requested to provide their banking account, which is thereafter plundered.

[26] Federal Police. Directorate economic and financial crime, *Fifth activity report*, 2006, 72–74.

[27] *Ibid*., 69.

[28] *Ibid*., 85.

	Counterfeit			Forgery			Theft of blank documents			Look alike fraud			Intellectual fraud		
	IK	PP	VD	IK	PP	VD	IK	PP	VD	IK	PP	VD	IK	PP	VD
2001	353	490	865	87	1.902	70	123	455	210	53	385	104	34	166	47
2002	354	595	902	40	1.067	61	68	152	118	38	148	42	30	117	39
2003	762	628	652	69	1.009	75	51	77	284	139	242	82	34	190	48
2004	631	2.894	814	70	1.293	74	65	268	278	430	459	92	58	258	109
2005	496	1.224	806	52	1.098	118	19	158	773	321	313	104	39	236	77
2006	391	485	500	92	1.016	92	32	104	217	111	171	40	60	223	112
TOTAAL 30.726	2.987	6.316	4.539	410	7.385	490	358	1.214	1.880	1.092	1.718	464	251	1.190	432
%	9,7	20,5	14,7	1,3	24	1,6	1,2	4	6,1	3,6	5,6	1,5	0,8	3,9	1,4

Table 2.2. Fraud of documents in numbers

Figures by the Banking, Finance and Insurance Commission

In connection with a recent case of fraud, the Banking, Finance and Insurance Commission (*Commissie voor het bank-, financie- en assurantiewezen (CBFA*)), which supervises the activities of banks and insurance companies, stated in the press that there had been only 51 or 52 successful attempts of Internet banking fraud cases since 2005, causing a total financial loss of almost 800,000 euro. The Commission said that the cited number of cases is in its opinion rather low, especially in view of the 500,000 daily Internet banking transactions.[29]

Figures about card use

The use of payment and credit cards also increases considerably. Below are figures about the amounts involved in both the online and offline use of various cards in Belgium. Table 2.3 shows a clear increase over the recent years.

Debit cards			Credit cards		Company cards	Prepaid cards
Payments		Cash withdrawal	Payments	Cash withdrawal	Payments	Payments
2001-II	11.350	10.834	3.338	708	813.	154
2002-I	11.981	11.478	2.951	713	881.	366
2002-II	13.027	11.550	3.115	842	916.	303
2003-I	13.051	13.455	3.381	792	.	280
2003-II	14.056	13.570	3.938	783	.	271
2004-I	14.286	13.427	3.143	712	.	272
2004-II	15.477	13.527	3.327	786		257
2005-I	15.691	13.393	3.705	798		250
2005-II	17.125	13.573	3.593	896		236

Table 2.3. Amount of operations (online and offline) (in million of euros) per type of card[30]

[29] *De Standaard Online*, 6 October 2007.

[30] Source Belgostat. National Bank of Belgium, *Payment cards. Amount of the transactions per type of card (per million euro's)*, Eurostat, available at http://www.nbb.be/belgostat/DataAccesLinker?Lang=N&Dom=4105&Table=56&Order=ASC.

Because the use of chip and pincode is now applied to all credit cards, the fraud with these cards would have dropped with 30%, according to Banksys.[31]

2.3 Vulnerabilities

2.3.1 Identification Processes

As stated before, Belgians have an obligation to carry their identity card, and this as of the age of fifteen. A Royal Decree of 1985 specifies in which cases the identity card has to be shown or submitted: (i) upon request of the police, (ii) when filing a notification (‘*aangifte’),* (iii) upon each request for certificates (‘*getuigschriften’),* and (iv) in general, each time the holder has to submit evidence of his/her identity, and (v) to the bailiff who shall serve a writ (of summons) or to persons who shall serve a copy thereof. [32] The Belgian Privacy Commission has stressed that in all other cases an individual can in principle only be obliged to show or submit his/her identity card if this is necessary for the execution of a legal obligation.[33]

Several legal provisions explicitly refer to the necessity to submit the identity card. In the context of actions against money laundering, credit card companies, leasing companies and a large group of other financial institutions are by law obliged to request their clients, under particular circumstances, to submit their identity cards for proper identification and to keep a photocopy. This requirement is also applicable to a large group of other professionals, including notary publics, who shall also duly identify the individuals who appear before them by checking their identity on the identity card.[34]

Operators of electronic communication networks and services are in principle also obliged to be able to identify their customers.[35] For that purpose, they request from their customers a copy of their identity card, for example when applying for an Internet connection. A similar practice is applied by utility companies.

These legal provisions which require the aforementioned companies and public servants to verify the identity should have the benefit of making it more difficult for criminals to act in or to abuse someone else’s name when applying for these services. On the other hand, individuals get used to submitting their identity card to obtain services in the private sector and may become willing to provide their identity details voluntarily for other services, even in case this may not be necessary. Criminals will take advantage of this attitude. Opponents of the eID card will even argue that it becomes easier to copy the personal data of the identity card with (unauthorized) smart card readers.

2.3.2 The use of a central unique personal identification number

The personal identification data of citizens in Belgium are centralized in a national database, the National Register (‘*Rijksregister’*). The central registering, the memorizing and the communication of personal data about the identification of persons started in 1968. Local municipalities could adhere voluntarily and on contractual basis to the system. The practice

---

[31] Federal Police. Directorate economic and financial crime, *o.c.,* 83.
[32] Article 1 of the Royal Decree of 29 July 1985.
[33] Commission for the Protection of Privacy, *Opinion 08/2003,* 27 February 2003, 5.
[34] See Act of 11 January 1993 for the prevention of the financial system for purposes of money laundering and the financing of terrorism (as modified several times), *Belgisch Staatsblad* [Belgian Official Journal], 9 February 1993, also available at http://www.cbfa.be/nl/hk/wg/pdf/law_11-01-1993.pdf
[35] See Article 127 §1 2° of the Act on electronic communication of 13 June 2005.

has obtained a legal framework through the Act of 8 August 1983 for the organization of the National Register of natural persons which confirmed the practice post factum.[36]

All persons who are registered in the National Register are identified by the government for administrative purposes with a central unique personal identification number, called the National Register Number (*'Rijksregisternummer'*). The National Register Number is intended to be a unique identifier which links persons to personal information relating to them and kept by governmental services. It contains references to date of birth. This National Register number is also mentioned on the eID and in the certificates of the eID. Access to the National Register and the use and processing of the National Register number however is restricted and requires authorization. These strict rules on the use of the National Register number have as a side-effect that for persons not authorized to use the number, it is more difficult to verify the correctness of identity-related data. Companies and persons who are merchants or exercise a liberal profession are also identified by the government by a unique personal identification number, the so-called Company Number (*'Ondernemingsnummer'*).

These unique personal identification numbers conferred by the government allow the government and an increasing number of parties authorized to access and use the number to identify natural persons (and companies) in a reliable way (for example by avoiding errors because of similar names, etc). The number also permits the users to update and access the personal information of citizens in an efficient way. The number further facilitates the exchange of personal information amongst several departments of the government. Arguments against the use of the unique personal identification numbers are the risks of linking personal information processed in distinct databases which could lead to major risks for the privacy of citizens.[37]

The unique personal identification numbers however could also be abused by criminals. This risk is increased by the fact that the National Register Number is also mentioned on the eID, and because the identity and the signature certificates on the eID become visible if the eID is used for electronically signing or identifying in private transactions.[38] The government is to some extent aware of this risk and is for this reason considering the creation and deployment of different unique identification numbers for other privacy-sensitive information kept by the government, on the Be-Health platform for example.[39]

---

[36] See D. De Bot, *Privacybescherming bij e-government in België*, Vanden Broele, Brugge, 2005, n°249.

[37] See also *ibid*., n° 128 et seq.

[38] See J. Dumortier, 'eID en de paradoks van het Rijksregisternummer', *Trends Business ICT*, March 2005. For a clear position on the (il)legality of the number on the certificates , see D. De Bot, *o.c.*, n° 1198. Compare the opinion of Jan Grijpink about the negative effects of the storage of biometric characteristics in passports: J. Grijpink, 'Identiteitsfraude en overheid', *Identiteitsfraude: Lessen uit het buitenland. Justitiële verkenningen 32*, (J.E.J. Prins & N.S. van der Meulen (eds.)), 2006 (37), 51.

[39] See also P. Van Velthoven, 'De nieuwe Belgische identiteitskaart. Meer kansen op een betere identificatie voor de openbare besturen', in J. Denolf (ed.), *o.c.*, (93), 97.

2.4 Countermeasures

2.4.1 Legal countermeasures

2.4.1.1 Criminal law

Belgium has in principle no specific legal provision which criminalizes identity fraud/theft as such, understood as 'fraud or another unlawful activity committed with identity as a target or tool for illegal activities'.[40] Article 231 of the Penal Code (see *below*), however, can be seen as an article which comes close to a provision criminalizing identity fraud, understood as 'unlawful identity creation' and, in some cases, 'identity theft' (both in the category of 'unlawful identity change').[41] Furthermore, several other provisions in (mainly) the Penal Code punish activities related to identity theft/fraud. Legal provisions which criminalize activities related to identity fraud/theft are the following.

i) Adoption of a false name ('valse naamdracht' or 'aanmatiging van naam') (Article 231 Penal Code)

In the Belgian Penal Code, article 231 penalizes 'adopting in public a name which does not belong to oneself' (*'valse naamdracht' or 'aanmatiging van naam').* The article was introduced with the adoption of the Penal Code by Act in 1867 and is part of Title III 'Criminal offences against the Public Trust' and in particular of a Chapter which penalizes the unlawful adoption of functions, titles, or names. The purpose of the legislator was to abolish uncertainty with regard to someone's identity. The article is related to public order (*'openbare orde').* Three elements have to be combined: (1) the adoption of a name, (2) in public, and (3) the name should not belong to oneself. In addition, one shall do this 'knowingly' (*'wetens en willens').*

Some authors state that the first element which requires for the individual to 'adopt a name' (*'aanmatiging van een naam')* only refers to the family name,[42] but this is unclear. The Supreme Court has stated that it is sufficient that someone uses a nickname which is not on his certificate of birth[43] or that someone wants somebody else to believe that the false name is his own name.[44] It is hence irrelevant for this criminal offence whether the name is the name of someone else or not, but rather essential that it is not the name as mentioned on the birth certificate.

There is also some confusion with regard to the second requirement of adopting a name 'in public'. The use of a false name for registration in a hotel register has been considered to fall under this qualification, even though such hotel registers are in principle not public documents. Therefore, some hold that it is sufficient that there is a certain degree of publicity whereby the adoption of the name is visible.

---

[40] Koops, Bert-Jaap & Ronald Leenes (2006), 'ID Theft, ID Fraud and/or ID-related Crime. Definitions matter', *Datenschutz und Datensicherheit* 2006 (9), p. 553-556. For the concepts, see Koops, Bert-Jaap, Ronald Leenes, Martin Meints, Nicole van der Meulen & David-Olivier Jaquet-Chiffelle (2008), 'A Typology of Identity-related Crime: Conceptual, Technical, and Legal Issues', *Information, Communication & Society* (forthcoming), and footnote 45 *below*.

[41] See footnote 45 *below*.

[42] D. Reynders, M. Taeymans & W. Cruysberghs, 'Identiteit en diefstal van identiteit. Een verkennende juridische duiding', in J. Denolf (ed.), *o.c.*, (31), 43.

[43] Supreme Court (*'Hof van Cassatie'*), 17 April 1905, *Pas.*, 1905, I, 196.

[44] Supreme Court (*'Hof van Cassatie'),* 6 February 1967, *Pas.*, 1967, I, 687.

The third requirement is that the name should not belong to oneself. As stated before, it is not required that the name should belong to someone else. The use of a pure fictitious name is sufficient. It is not required that third persons are involved or incur negative consequences. It is not required for this offence that one has the intention to hide his identity; merely using a false name is satisfactory.

Article 231 of the Penal Code covers in fact a rather broad area of use of a false name. The article refers to some extent to the category of acts of unlawful identity change as described and defined in the FIDIS typology.[45] It is not exactly the same, because for the application of article 231, the mere change of identity in public is sufficient and does not require other crimes or unlawful activities committed with this new identity. The use by someone of a (family) name other than the one mentioned on the birth certificate in chat rooms on the Internet, for signing comments in an electronic visitor's register of a website or even in an e-mail address, would in principle be sufficient for criminal liability. The principle that criminal provisions should not be interpreted in an analogous way does not seem to prevent the application of this article to cases in an online environment.[46] Article 231 Penal Code seems to have been invoked in prosecutions in 2000 1400 times, increased to 2100 cases in 2004.[47]

ii) Theft ('diefstal') (Article 461 Penal Code)

Article 461 of the Penal Code states that someone commits theft if 'he takes away a thing which does not belong to him'. Such theft has to be done with malicious intent. The theft of someone else's identity as such encounters problems under this article. First of all, theft is traditionally understood as the taking away of a material thing. Unless the identity papers also have been stolen, there is a problem with the theft of 'identity' in the sense of the identity of someone else as attributed in the certificate of birth, and further built up by that person over time by registration in the social security registers, other governmental agencies, banks, etc. Courts, however, have been creative in the interpretation of theft, and have for example in the case of hacking of a computer (before the Act of 28 November 2000) accepted the theft of electricity.[48] Whether courts would have the same attitude towards the theft of identity, is uncertain.

iii) Forgery of documents, informatics and telegrams and use thereof ('Valsheid in geschriften, in informatica en in telegrammen') (Article 193 et seq. Penal Code)

---

[45] In the conceptual categorisation of identity-related crime in Koops et al. 2008, a distinction is made between lawful and unlawful identity change. According to the authors, unlawful identity change typically contains an element of fraud, and therefore, unlawful identity change is called 'identity fraud', defined as 'fraud or another unlawful activity committed with identity as target or principal tool'. Article 231 Penal Code, however, does not require this (additional) element of fraud. Under article 231 Penal Code, the mere change of identity by adopting a (family) name which is not the name registered in the birth certificate, is in principle always unlawful.

[46] But see D. Reynders, M. Taeymans & W. Cruysberghs, 'Identiteit en diefstal van identiteit. Een verkennende juridische duiding', in J. Denolf (ed.), *o.c.*, (31), 45.

[47] U. de Vries, H. Tichelaar e. a., *Identiteitsfraude: een afbakening. Een internationale begripsvergelijking en analyse van nationale strafbepalingen*, 20 July 2007, 164, available at http://www.wodc.nl/images/1496_%20volledige_tekst_tcm44-86343.pdf.

[48] Court of first instance Brussels, 8 November 1990 (Bistel case), *Computerrecht* 1991, 31. See also E. Kindt & E. Szafran, 'Informaticacriminaliteit: Nullum crimen, nulla poena sine lege', Note under Court of first instance Gent, 11 December 2000, *Computerrecht* 2001, 84. In this case, the court even classified (by analogy) the abuse of a password as 'the use of false keys'.

Someone commits a crime if he changes with fraudulent intent or with the intent to harm the truth in documents specified in the Penal Code or if he makes use thereof (Article 193 through 212 Penal Code). These articles specify four categories of documents:[49] (a) authentic and public documents,[50] commercial or bank documents and private documents,[51] (b) travel documents, permits to be armed, labour booklets, travel orders and certificates, (c) informatics systems, and (d) telegrams. The documents (or systems) which are protected are documents (or systems) which confirm a specific act or fact and which are relevant for the public trust. Forgery in informatics was added to this list (article 210*bis* Penal Code) by the Act of 28 November 2000 on computer crime.[52] Article 210*bis* criminalizes fraud in legally relevant data stored in an informatics system by entering, changing, deleting or modifying by any other technological means the use of such data. Log books and data of e-mail messages could qualify as such legally relevant data.[53]

iv) Abuse of confidence and misappropriation ('Misbruik van vertrouwen en verduistering') (Article 491 through 495bis Penal Code; Article 240 Penal Code))

The provisions of the Penal Code with regard to the misappropriation or embezzlement with fraudulent intent of handed over (for return) 'goods, money, commercial goods, notes, receipts, writings of whatever kind, which contain or create an obligation' with possible detrimental consequences may in specific circumstances also be relevant for identity fraud (see articles 491 through 495*bis* Penal Code). In addition, a similar crime of misappropriation exists for persons acting in a capacity as public official.

Because the misappropriation requires in principle a material good (and not immaterial goods such as 'identity'), the application of these criminal provisions to identity fraud cases will be limited to those cases in which an identity document has been handed over (for example, the temporary handing over of an identity card as caution for the rental of a bike) and misappropriated (for example, when the identity document is not returned or photocopied). It might however also apply to cases in which for example the data of credit cards are misused when the card is temporarily handed over, for example, for payment in a restaurant.

v) Fraud ('Oplichting en bedriegerij') (Article 496 through 504 Penal Code)

Identity-related crimes involve the gathering of identity data of others or creating new identity data and, in a second stage, the using of these data in some unlawful way.[54] If the intent is to obtain the handing over of money, goods, obligations, receipts or debt releases belonging to others, in a fraudulent way, including by the use of false names or functions, or by the use of deceitful tricks ('*listige kunstgrepen'*), one commits fraud ('*oplichting en bedriegerij'*).[55]

---

[49] For these categories, the constitutional elements of the crime are the same but the penalties different. Moreover, these articles have a general application field, and yield in case there exist more specific penal provisions on a specific type of document fraud.

[50] Fraud in authentic and public documents is only applicable to public officials or officers who act in the execution of their function.

[51] Fraud in private documents is much broader: it is sufficient that the document is fit for use as evidence: see Supreme Court ('*Hof van Cassatie'*), 27 April 1982, *Arr. Cass.*, 1981-82, 1033.

[52] See *below*, at footnote 56.

[53] Since e-mail messages are processed and stored by informatics systems, can be used as evidence and are often (with reason or not) perceived by the public as containing the truth, it is likely that courts could bring forgery of e-mail documents and messages (for example, by changing the name of the sender/recipient) under these provisions.

[54] See B-J. Koops (ed.), *o.c.*, 18.

[55] See article 491 § 1 Penal Code.

Phishing may fall under this article if the mails and other tricks are material for obtaining money or goods (e.g., the phishing of the username and password for obtaining access to an online banking account).

vi) Fraud in informatics ('Informaticabedrog') (Article 504quater Penal Code)

By Act of 28 November 2000, several computer crimes have been defined and introduced in the Penal Code.[56] Article 504*quater* of the Penal Code criminalizes the act (and the attempt) of obtaining an illicit economic advantage for oneself or for a third party by inputting data in a computer system, changing such data, deleting or changing the normal use of such data by any other technological means with fraudulent intent.

Legal provisions relating to offences against the confidentiality, integrity and availability of computer data and systems

vii) Computer hacking ('Hacking') (Article 550bis Penal Code) and sabotage of data and informatics ('Data- en informatica sabotage') (Article 550ter Penal Code)

If one accesses a computer system or part thereof without authorization, from the outside (external hacking, in which case it is sufficient to know that one accesses the system) or from the inside by someone who exceeds his authorization (internal hacking, in which case fraudulent intent or the intent to harm is required), he commits the crime of computer hacking (Article 550bis Penal Code).[57] If one deletes or damages data in a computer system, with the intent to obtain illicit gain or with malicious intent, he is committing data sabotage (Article 550ter Penal Code). Producing, possessing, selling, obtaining, importing or distributing tools, including software tools, which facilitate such crimes is also punishable.

The crime of hacking will occur in many cases of online identity-related crime. In a criminal case before a Belgian court, where someone (with the intention to show a bank the weak or absent security measures of its Internet banking system) had hacked the beneficiaries' list of an internet banking user and changed one beneficiary on this list (with the message 'Hacked Bacob is aware of the problem'), article 550*bis* Penal Code was applied.[58]

Legal provisions relating to the secrecy of communications

viii) Wiretapping of private communications (Article 259bis and 314bis Penal Code)

By Act of 30 June 1994 penalizing wiretapping, penalties are provided for the crime of interception of a private communication between other parties during the transfer thereof and the use of such interception, by public officials or civil servants in the execution of their functions, in cases not foreseen by law (Article 259*bis* Penal Code).[59] A similar provision sanctions interception and use thereof by other persons (Article 314*bis* Penal Code).

The interception of communication over the Internet (such as the communication with a web server) for purposes of identity-related crimes, such as obtaining usernames and passwords, and the use of the information obtained in such way, is hence penalized.

---

[56] The provisions of the Computer Crime Act have been updated by Act of 15 May 2006, *Belgian State Gazette* 12 September 2006 (2nd ed.).

[57] A similar criminalisation for hacking exists for persons gaining or maintaining on purpose access to the Cross Road database and sabotage of the data in this database.

[58] Court of first instance of Hasselt, 21 January 2004, *Computerrecht* 2004, 21 (online version), with note of H. Graux.

[59] Act of 30 June 1994 for the protection of private life against listening in, taking knowledge, and opening of private communication and telecommunication, as modified by Act of 15 May 2006.

ix) Secrecy of the existence and details of a communication (Article 124 Electronic Communications Act)

The existence of an electronic communication amongst third persons, including the identification of the persons involved and other related data, shall remain secret, and the taking knowledge thereof or the intentional use or revealing of such information is a crime (Article 124 Electronic Communications Act).[60]

This article (in its previous version of article 109terD) has been applied by the courts in the case ReDaTtack where someone had, through the use of an e-mail account of someone else, downloaded details of payment transactions of clients of Internet banking services of a large bank and had sent this information to the press.[61] Usernames, passwords and pin codes which were obtained by the hacker, were in the decision qualified as 'data relating to the communication'.

Conclusion '*Nullum crimen sine lege'* ('No crime without legal provision') is one of the basic principles of penal law. This principle could be invoked by criminals because there is in Belgium no specific legal provision which criminalizes identity theft/fraud as such. However, perpetrators of identity-related crime will in many cases be punishable under one of the legal provisions discussed above. Authors who have analysed identity-related crimes under the aforementioned articles have concluded that, despite the lack of a specific legal provision which criminalizes identity theft as such, identity-related crimes can be tackled.[62] We concur only partly with this finding: each relevant article of the Penal Code has specific requirements which may not always be fulfilled. 'Theft' in article 461 of the Penal code, for example, requires the taking away of an object. Interpretation by analogy is not accepted. In addition, not all aspects of an identity-related crime may always be covered. If for example article 231 of the Penal Code is applied, the aspect of 'theft' will not be taken into account. The aforementioned provisions of the Penal Code therefore have their limitations if used to prosecute identity theft/fraud cases.[63]

In addition, victims need to be recognized and their position improved by for example having the possibility to file a complaint, which might be more difficult if there is no evidently appropriate article for the identity-related crime committed in the Penal Code. Nevertheless, the establishment of a central complaint database (which later became the ECops site in 2007) has been a start for this purpose.[64]

2.4.1.2 Data Protection Law

Other legal countermeasures can be found in the Law of 8 December 1992 on the protection of private life and the processing of personal data (hereinafter the 'Data Protection Act') which imposes specific obligations upon the controller and the processor of personal data.

---

[60] This provision was before incorporated in article 109ter D of the Act of 21 March 1991.

[61] Court of first instance Gent, 11 December 2000, *Computerrecht* 2001, 84, with note E. Kindt & E. Szafran, 'Informaticacriminaliteit: Nullum crimen, nulla poena sine lege'. The authors of the note criticize the broad interpretation of the term 'data about the telecommunication' as applied in this decision.

[62] D. Reynders, M. Taeymans & W. Cruysberghs, 'Identiteit en diefstal van identiteit. Een verkennende juridische duiding', in J. Denolf (ed.), *o.c.*, (31), 60.

[63] D. Reynders, M. Taeymans & W. Cruysberghs, *ibid*., 59, acknowledge this limitation of the existing penal provisions

[64] See footnote 74 *below.*

Under this Act, they should take appropriate technical and organizational measures for the protection of the personal data, in particular against accidental or illicit deletion, accidental loss, modification, access to and any other unauthorized processing of the data (Article 16 §4). Controllers are also obliged to restrict access to the personal data. Personnel which need personal data for the execution of their tasks shall only be authorized to access data which are needed for their tasks or which are needed for the necessities of the department (Article 16 §2 2°). The controller shall also inform its personnel about the relevant provisions of the Data Protection Act. If the controller engages a processor of the personal data, the liability of the processor shall be agreed in writing (Article 16 §1 3°).

If the identity-related crime is due to breach of one of these provisions, victims may invoke the Data Protection Act.

For breach of most of the obligations imposed on the controller and processor by the Data Protection Act, criminal sanctions apply (Chapter 8).Victims can also claim damages from the controller (Article 15bis). The Data Protection Act states that the controller is liable for the damages which are caused by breach of any of the provisions of the Data Protection Act, unless the controller is able to prove that he is not responsible for the fact(s) which caused the damages (Article 15bis paras. 2 and 3).

The Data Protection Act, and in particular the provisions briefly mentioned above, may prove to be an efficient countermeasure against identity-related crime in particular circumstances. For example, if a controller does not apply adequate security measures upon the transfer of personal data to a third party, online or offline, and the personal data are lost or illegally acquired by others, the controller may be (criminal and civil) liable under the Data Protection Act. Controllers should be made better aware of the responsibility and liability they have for the processing of personal data, and the possible consequences, including identity-related crime which may result from neglecting state of the art security measures.[65] In particular circumstances, the legal provisions may not have the envisaged effect. Controllers often do take adequate and state-of-the-art security measures, but hackers typically try to break state-of-the-art security measures, for example, of an online bank. In other cases, the users may also be negligent, by using copied or not up-to-date software (where detected 'holes' are not sufficiently remedied) or by posting their username and password in places where these can be read.

Reference measures for the Protection of each Processing of Personal Data

The so-called Reference measures for the Protection of each Processing of Personal Data (*'Referentiemaatregelen voor de beveiliging van elke verwerking van persoonsgegevens')* are also important in the fight against identity-related crime.[66] These Reference measures deserve to be briefly mentioned although they are not specifically issued for identity fraud, because they provide generally applicable guidelines for the protection of the processing of personal data. The measures were issued by the Belgian Data Processing Authority (*Commissie voor de Bescherming van de Persoonlijke Levenssfeer*) some years ago in order to clarify and

[65] For example, in case a controller sends (automated) files with personal data, such as the name and date of birth, of 25 million persons, even offline, stored on a cd-rom or other portable carrier, and does not take adequate security measures for a safe transfer, the controller could be liable in Belgium under the Data Protection Act.

[66] Reference measures for the Protection of each Processing of Personal Data (*Referentiemaatregelen voor de beveiliging van elke verwerking van persoonsgegevens)*, available at http://privacy.fgov.be/nl/static/pdf/referenciemaatregelen-vs-01.pdf (visited 16 November 2007).

specify the measures which could or should be taken in furtherance of article 16§4 Data Protection Act. The measures give ten action domains in which controllers and processors of personal data shall take specific action in order to secure the personal data. These actions shall be adapted in relation to the specific context, including the nature of the data and the kind of organization of the controller. The measures state, for example, that a security consultant (section 2) shall be nominated and that there should be a plan for the governance of security incidents (section 9).

2.4.2 Technical and organizational countermeasures

Technical countermeasures

The Belgian eID card

The government has decided to introduce the eID card for all Belgian citizens aged twelve years and older.[67] The government advocates the use of the Belgian eID card as a tool for a safer Internet use. The eID card should enable the government, citizens and companies to exchange information over the Internet in a secured way. Many companies are in the process of developing software applications for the use of the card. The Minister for Computerization, Mr. Vanvelthoven, has announced that all sites which will use the eID card for authentication purposes will focus on fraud control. The Minister intends to prevent phishing attempts in which criminals want to obtain personal (and credit) data from persons. Without such extra control, 'all developments relating to e-government become endangered'.[68] The development and the introduction of the eID card for all Belgian citizens and the control over its use are therefore very important in the context of identity-related crime.

The introduction of biometric passports and travel documents

Belgium will introduce biometric passports in furtherance of European Regulation 2252/2004. This Regulation explicitly states that specific biometric identifiers shall be used to verify whether the holder of the passport is the owner of the travel document The biometrics are introduced as a technical means to counter lookalike fraud.[69]

Organizational countermeasures

Application of ISO standards

The government states that the security of its IT infrastructure is one of its key objectives. All government projects which imply the use of IT infrastructures need to comply with ISO 17799 standard relating to security.[70] The security measures need to prevent inter alia 'hacking' and 'fraud with personal identity information'.[71]

The Consultation Platform for Information Security

---

[67] See also E. Kindt, 'Algemene invoering van de elektronische identiteitskaart in België', *Computerrecht* 2005, 238. See also *above* in section 2.4.1 on legal countermeasures.

[68] X., 'Vanvelthoven waarschuwt voor phishing', *De Standaard Online*, 10 May 2004.

[69] About biometrics in ID documents, see also Meints, M. and Hansen, M. (eds.), *D3.6. Study on ID Documents*, Fidis, 2006, 160 p.

[70] See also D. De Bot, *o.c.*, n° 54 et seq.

[71] See also FOD Economie, *Beveiliging van informatiesystemen en –netwerken*, available at http://mineco.fgov.be/information_society/networks_security/home_nl.htm.

In order to cope with IT security in general, such as spam, spyware, viruses, botnets and theft of personal data, the federal government has taken in 2005 upon initiative of Minister for computerization, Peter Vanvelthoven, the initiative to (re)establish a national 'Consultation Platform for Information Security' ('O*verlegplatform voor Informatieveiligheid*) (hereinafter the 'Platform', also named by some the 'Belgian Network for Information Security (BeNIS)).[72] Many government institutions which have an important expertise with regard to a particular aspect of IT security participate in the Platform. They meet regularly and the Platform coordinates actions by the various institutions.

Belgium also participates in the European Network and Information Security Agency (ENISA) where it obtains expert advice on matters of network and information infrastructure security.[73]

ECops : A Central Complaint Database

In order to facilitate the overview of the Federal Police of all types of identity-related crime to allow appropriate action, citizens are encouraged to report computer-related crimes. At the initiative of the Minister for Economy, the Federal Department for Economy and the Federal Computer Crime Unit of the federal police have worked together in order to establish a unique central website for the filing of complaints relating to fraudulent activities on the Internet. The website is named eCops ('Electronic Complaints Processing System') and is operational since 2007. ECops is available at http://www.ecops.be/.[74] The goal is to facilitate the filing of complaints of citizens if they encounter problems when surfing on the Internet, receiving mails or doing e-commerce transactions and do not know where to report the problem. The claims are automatically transferred by eCops to the competent authority for further investigation. In particular, if the claim relates to an unfair trade practice on the Internet, such as incorrect price announcements or the sending of unsolicited advertisement, the claim will automatically be forwarded to the Federal Department of Economy; if the claim relates to illegal content, a criminal offence or computer crime, the claim will be forwarded to the Federal Computer Crime Unit of the Federal Police. One of the objectives of eCops for the government and the Federal Police is to identify at an early stage new illicit practices on the Internet in order to combat them. This should in turn result in an increased confidence of citizens on the Internet.

Other central processing of complaints

The Federal Department of Economy also sends claims relating to phishing, which it receives from citizens, to a central database, Consumer Sentinel, which collects complaints relating to transnational consumer problems from over 17 countries.[75]

Press coverage

---

[72] .be België, *Federale overheid slaat handen in elkaar voor veiliger internet*, 30 September 2005, available at http://www.belgium.be/eportal/application?pageid=contentPage&languageParameter=nl&docId=40063

[73] See http://enisa.europa.eu/.

[74] See FOD Economie, K.M.O., Middenstand en Energie, 'eCops: een enig loket om bedrieglijke praktijken op het internet aan te geven', available at http://mineco.fgov.be/protection_consumer/complaints/complaints_nl_010.htm (visited on 15 November 2007). ECops will replace the central complaint site mentioned *above* in section 2.2.

[75] For the portal of ConsumerSentinel, see http://www.consumer.gov/sentinel/trends.htm.

With regular intervals, the theme of bank card fraud and Internet fraud in general, sometimes with mention of particular trends such as phishing, is covered in the Belgian press.[76] Such coverage is often made in the form of a warning of a governmental body, such as the Cell Consumer fraud of the Federal Department of Economy[77] or of a particular fraud case.[78]

Public awareness campaigns

The federal government informs the public at regular times on its federal web portal .be Belgium about the risks of the Internet.[79]

Unisys awareness study 2007

The awareness of consumers in Belgium about identity fraud has been measured by industry, in particular Unisys, a leading worldwide supplier of information (security) services. Unisys regularly publishes its 'Unisys Security Index' which reveals consumer perceptions about financial and personal security. The index is based upon surveys of over 13,000 people in 14 countries, including Belgium (where 1,022 persons were questioned). In October 2007, the Belgian Unisys Security Index stands at 131/300 (where 300 is the highest level of perceived anxiety).[80] Belgium seems to be at an average level for Europeans.[81] From the survey, it appears that especially online security and fraud is a source of concern. 34 % of Belgians are 'extremely concerned' and 24% 'very concerned' about credit/debit card fraud.[82] Furthermore, a majority of Belgians is seriously concerned about unauthorized access to or misuse of personal information (identity theft): 29% are 'extremely concerned' and 28% of Belgians are 'very concerned'.[83] 31% are somewhat concerned, so that altogether 88% of Belgians is concerned about fraud with financial and personal information.

---

[76] See e.g., I. Van Daele, 'Uw pc is een open portemonnee', *Knack*, 25 July 2007, 28-33.

[77] See e.g., X., 'Economische Zaken waarschuwt voor "phishing" op internet', *De Standaard Online*, 5 February 2004. The Cell Consumer fraud of the Federal Department of Economy warned in that case for e-mail requests to visitors of eBay, in which presumely 'eBay' would ask numbers of credit cards, of bank accounts and passwords for these bank accounts, to be filled out on a page linked with a fraudulent site (but appearance of the official eBay site).

[78] A case reported in the press related to the hacking of Belgian bank accounts of two major banks, KBC and Dexia which were use for internet banking. See for example X, 'Russische mafia kraakt Belgisch internetbankieren', *De Standaard Online,* 6 October 2007.

[79] See 'Privacy en Informatieveiligheid' on the webportal .be Belgium, the portal of Fedict of the federal government, available at http://www.belgium.be/eportal/application?origin=searchResults.jsp&event=bea.portal.framework.internal.refresh&pageid=indexPage&navId=45238 (visited on 13 November 2007). See also Portal about information security applied by the government, available at *http://www.xs4all.nl/~rvy/ib-overheid.html*

[80] Unisys, *Unisys Security Survey and Index – Belgium, 6 September 2007*, 15 p, available at http://www.unisys.com/eprise/main/admin/corporate/doc/services/security_index/BL07-0075_Belgium_final.pdf. See also the press release: Unisys, *Key Growth Economies Most Worried About Security Threats, Unisys Global Survey Reveals*, 30 October 2007, available at http://www.businesswire.com/portal/site/google/index.jsp?ndmViewId=news_view&newsId=20071030005080&newsLang=en.

[81] The overall Unisys Security Index scores by country are as follows: Brazil (188), Hong Kong (179), Malaysia (174), Singapore (172), Germany (160), U.S. (151), Australia (144), U.K. (138), Belgium (131), Spain (115), New Zealand (108), Netherlands (98), Italy (90) and France (83).

[82] Unisys, *o.c.* at footnote 80, 7.

[83] Unisys, o.*c.* at footnote 80, 10 (chart 13).

2.4.3 Credit reporting

By Act of 10 August 2001, the central database kept by the National Bank of Belgium with the registration of defaults under credit agreements with consumers and mortgage loans has been reorganized in the Central Database for the registration of Credit agreements to Individuals (*'Centrale voor Kredieten aan Particulieren')* and regulated by law.[84] In the database, the credit agreements concluded by individuals are registered, including any defaults of payment. The database shall be consulted by credit institutions before granting a new credit agreement.

The individuals are registered through an unique National Register number, their name, gender, date of birth as mentioned in their identity document and domicile or place of stay.[85] This should prevent that persons are incorrectly listed (e.g., because of similar names). The credit information shall only be communicated to the persons identified in article 8 of the Act and shall only be used for the conclusion and the management of credit agreements. Although access to the central database is limited, the Privacy Commission stated in its opinion relating to the draft law that the conditions for communicating the information are very general and that abuse remains possible.[86]

2.5 Conclusion

Identity-related crime has always been present in Belgium. The traditional identity-related crime concerns mainly documents, such as the theft, forgery and the use of false identity documents (as in lookalike fraud), especially for travel and immigration purposes.

Although this identity-related crime still takes place, and technical measures are introduced, such as biometric passports which should combat lookalike fraud, the focus of attention in the press and of the public is the last few years shifting towards online identity-related crime, such as phishing and online credit fraud. Governmental authorities seem to be willing to take the concerns provoked by this new kind of crime into account. The government has already decided to introduce the eID card for all Belgian citizens, which should allow inter alia secure identification and authentication online. Several other initiatives are taken on federal governmental level, both by the Department of Economy and the Federal Police, for example a single website for the notification by the public of online fraud and unfair trade practices. These initiatives lead to the collection of more data, which allow in turn further investigation and research on the need for a distinct criminal provision of identity theft/fraud. The reporting by citizens also shows inter alia that the awareness campaigns are useful. Such campaigns are regularly made in order to make the public aware of the risks of providing personal and financial data through online channels.

Until now, the reported cases of online identity-related fraud have been rather limited in number, persons involved and amount lost. However, nothing indicates that online identity-

---

[84] Act of 10 August 2001 on the Central Database for Credit Agreements to Individuals, *Belgisch Staatsblad* [Belgian Official Journal] 25 September 2001, 32027, also available at http://www.bnb.be/NR/rdonlyres/AFA66A94-E8C7-4B38-BC22-1BA88F091136/0/Loidu10aout2001relativealaCCP.pdf .

[85] Article 2 of the Royal Decree of 7 July 2002, *Belgisch Staatsblad* [Belgian Official Journal] 19 July 2002, 32542.

[86] Commission for the Protection of Privacy, Opinion N° 31/2000, 9 November 2000.

related fraud may not become far more important in the coming years. The reported events indicate that there is an increasing trend. Because of the rather high penetration of Internet use with the population in Belgium and the steady increase of e-commerce, the factors which are responsible for identity-related crime are also present for an increase in online identity-related crime.

3 France

3.1 Concepts

Identity-related crime concerns in France mainly focus on document and financial fraud. The former arose from the debate on the introduction of a national electronic identification card. The main arguments advanced by the government for such a card mainly rely on the need to fight document fraud. A secure document and handout procedure are foreseen as an adequate means to combat false identity documents and the use of false identities based on authentic documents.

Concerns with regard to financial fraud and more particularly credit card fraud arise from the fact that 80% of on-line payments are done by credit cards,[87] which are also largely used as identifiers in e-commerce.[88] A report issued by the Observatory for Payment Card Security [*Observatoire de la sécurité des cartes de paiements*] showed that the amount of fraudulent payments by credit card amounted to 252,6 M€ in 2006. Some attention has also been brought to the problem raised by *phishing* as several French banks and their clients have been victims of such practices, which ignited a strong response.

It follows that the debate mainly relates to what FIDIS researchers identified as "unlawful identity takeover", i.e. the "fraud or another unlawful activity where the identity of an existing person is used as a target or principal tool without the person's consent" and, to a lesser extent, unlawful identity delegation or creation.[89]

In view of these threats, public and private actors have tried to give appropriate answers to identity-related crimes, whose concerns have been revived by the rise of the Internet and the spread of new technologies. Legal, technical and organisational measures have been taken by public authorities, financial institutions and online merchants to fight identity fraud and empower citizens to prevent or defend themselves against abuses.

3.2 Prevalence

Few studies have focused on identity fraud as such. Three reports should be mentioned because they provide an overview of the current state of identity-related fraud. The first, the 'Informative Report on the new generation of identity documents and document fraud',[90] presented to the Senate in June 2005, focuses on identification document fraud. The report aimed to comprehend the phenomenon of document fraud in France, to identify its main

---

87 Forum des Droits sur l'Internet, 'Online payments' [*Les paiments sur l'Internet*], 19 May 2005, p. 8.

88 Opinion of the CNIL, Recommendation n°03-034 of 19 June 2003 adopting a recommendation on the storage and use of the credit card number in the field of distance selling [*portant adoption d'une recommandation relative au stockage et à l'utilisation du numéro de carte bancaire dans le secteur de la vente à distance*], available on-line at: http://www.cnil.fr/index.php?id=1357, last accessed on 31 October 2007.

89 Koops, Bert-Jaap & Ronald Leenes (2006), 'ID Theft, ID Fraud and/or ID-related Crime. Definitions matter', *Datenschutz und Datensicherheit* 2006 (9), p. 553-556; Koops, Bert-Jaap, Ronald Leenes, Martin Meints, Nicole van der Meulen & David-Olivier Jaquet-Chiffelle (2008), 'A Typology of Identity-related Crime: Conceptual, Technical, and Legal Issues', *Information, Communication & Society* (forthcoming).

90 Lecerf J.-R., Informative report to the French Senate on a new generation of identity documents and document fraud [*Rapport d'information au Sénat n°439 sur la nouvelle génération de documents d'identité et la fraude documentaire*], 29 June 2005, p.17, available on-line at: http://www.libertysecurity.org/IMG/pdf/Rapport_d_information_sur_la_nouvelle_generation_de_documents_d_identite_et_la_fraude_documentaire.pdf.

origins and to formulate the relevant recommendations in view of making a contribution to the public debate surrounding the introduction of a national electronic identification card. The second report relates to the origins and forms of credit card fraud and is issued on a yearly basis by the Observatory for Payment Card Security. Finally, the third report, issued by the Observatory for Cyber-Consumerism [*Observatoire de la cyber-consommation*], under the resort of the Forum of Rights on Internet, issued in May 2005, assessed the reality of consumers' fears towards on-line payment fraud.

3.2.1 Document fraud

3.2.1.1 Measurement of the phenomenon

The Report "on the new generation of identity documents and document fraud" provides an overview of the current state of document fraud in France on the basis of the available data. This report identifies four types of identity fraud: use of false identity, identity theft, exchange of identity and use of a dead person's identity. The means used to perpetrate such crimes usually include stolen blank identity tokens, counterfeit tokens, forgery, fraudulently obtained identity tokens and fraudulent use of another person' identity token.[91]

This Report notices an important increase in document fraud over the last few years. The use of false identity documents, for example, appears to have increased by 7,71% between 2001 and 2003, as illustrated by Table 3.1.

	2001	2002	Difference	2003	Difference	Difference 2001-2003
False identity documents	9275	10712	+15.49%	9990	-6.74%	+7.71%
False documents related to vehicles	1959	2342	+19.55%	2311	-1.32%	+17.97%
Other administrative documents	2476	3086	+24.52%	3258	+5.68%	+31.58%
Fraud and breach of confidence	154107	140593	-8.77%	145174	+3.26%	-5.80%
Total	167817	156730	-6.61%	160733	+2.55%	-4.22%
Part in the total of offences	4.13%	3.81%		4.04%		

Table 3.1. Document Fraud – Continental France (extract of « état 4001")[92]

[91] Ibid.
[92] Ministry of Internal Affairs, extracted from 'Report on a new generation of identity documents and document fraud', p. 23. The «état 4001» gathers all crimes and offences recorded by police forces.

The figures relative to breaches of the law based on document fraud punished between 1994 and 2003 reveal the same tendency.

Breach of the law	Year	All sanctions for this breach	Sanctions as main breach	Sanctions as sole breach
Fraudulent possession of false administrative documents acknowledging a right, an identity or a quality	1994	108	38	6
	2002	1213	526	126
	2003	1155	460	114
Forged administrative document acknowledging a right, an identity or a quality	1994	2550	885	185
	2002	1456	589	64
	2003	1467	586	57
Provision of imaginary identity which may imply false mentions in criminal records	1994	161	33	6
	2002	350	63	15
	2003	421	97	24
Use of false administrative document acknowledging a right, an identity or a quality	1994	3521	690	220
	2002	2848	550	191
	2003	2691	547	180
Sanctions pronounced for false identity-related crimes	1994	6340	1646	417
	2002	5867	1728	396
	2003	5734	1690	375

Table 3.2. Document Fraud – number of sanctions[93]

However, these figures are merely indicative and the real significance of the phenomenon remains unknown as no public agency has been in charge of collecting any statistical information. The available information is thus fragmented and information sources are dispersed and uncertain. Furthermore, in most of the cases the competent authorities have not developed measuring tools.

The lack of centralisation of the information, the lack of common benchmarks and definitions and the fact that frauds linked to the perpetration of other crimes than identity fraud are not taken into the statistics are identified as one of the main barrier in the fight against document

[93] French Ministry of Justice, extracted from 'Report on a new generation of identity documents and document fraud', p. 24.

fraud. To that effect, the report suggests putting the National Observatory of Delinquency[94] in charge of the elaboration of a permanent evaluation tool of identity fraud.

3.2.1.2 Weaknesses identified

The report identifies several weaknesses of the system not only related to the production and detection of false identification documents but also both located in the handout procedure of authentic documents.

False documents

First of all, problems arising from the production of false documents are mainly present in passports and driving licenses due to the fact that they do not benefit from a centralised procedure of issuance, contrary to the national identification card. In that sense, the report suggests giving legal validity for identification exclusively to documents such as the national identification card and passports. It even raised the question of a possible fusion of both documents.

Moreover, some of the security measures incorporated in identification documents cannot be checked during identity controls because the police lack adequate instruments.

Authentic documents issued on the basis of false documentation

Another problem stressed by the report resides in the fact that it is possible to obtain authentic (i.e., official) identification documents by providing forged (unofficial) documentation. This facilitates the obtaining of a false identity certified by an authentic document.

In view of obtaining an identification card or passport, individuals need to prove that they are entitled to be delivered such document. To that effect, they must produce an authentic document which states their date and place of birth and their filiations, the so-called "*justificatif d'état civil*". These documents are usually delivered by municipalities, in charge of the Civil Registers, or abroad, by Consulates. There is no centralised Civil Register in France.

The report observes that the staff in charge of handling these documents is sometimes insufficiently prepared and do not respect the existing guarantees of the procedure such as the persons whom this document can be handed to (the beneficiary itself, its ascendants, descendants or a third person with a valid mandate). This facilitates the issuance of authentic documents to unauthorized persons. In foreign countries, two main issues are identified as facilitating fraud, namely cases of corruption of civil officers and the lack of quality of Civil Registers (several persons recorded under the same name, outdated registers, etc.). The Ministry of Foreign Affairs has observed an increase in the production of irregular or forged "*justificatifs d'état civil*" issued in foreign countries.

Moreover, the existing databases of requests of identification documents and of reported stolen and lost identification documents are insufficiently used and updated by the Civil Registry officers and the police. Structural problems hinder the work of such officers. For example, digital prints are exclusively stored on paper, which prevents checking the digital print taken against the database when a new document is requested.

---

[94] The National Observatory of Delinquency is an independent administrative body created in 2003 in charge of centralising all delinquency related statistical data, defining a common methodology and benchmarks, in order to make global studies on delinquency.

The report concludes that there is a need to use secure identity tokens (secure eID card), to introduce a more secure handout procedure of identity tokens mainly through the centralisation of procedures and the introduction of biometric identifiers.

3.2.2 Credit card fraud

Since 2003, the Observatory for Payment Card Security,[95] under the resort of the French National Bank, issues an annual activity report which includes a survey of credit card fraud. The survey is based on a specific methodology developed by this Observatory to obtain reliable statistics in the field.[96]

First, a definition of payment cards fraud needed to be provided. The definition adopted covers the use of cards or the data captured on them as well as the activities contributing to the perpetration of fraud. Irrespective of the criminal offences that exist under national law, the Observatory has chosen to adopt a functional definition that links the fraudulent nature of an act to its illicit nature and to the harm possibly caused to the various actors involved in a card transaction. It has decided to exclude all use or attempts to use payment cards by the lawful cardholder that are considered fraudulent solely due to lack of funds.

The Observatory has in addition defined a fraud typology in line with the various approaches outlined in the definition of fraud and closely based on the classification criteria used by the various issuers. This typology distinguishes between:[97]

- the origin of fraud: lost or stolen cards, non-received cards, forged or counterfeit cards, misappropriate card numbers, unallocated card numbers, splitting payments;
- fraud techniques: skimming, opening of a fraudulent account, usurpation of identity, wrongful repudiation, hacking automated machines, hacking automated data systems, card number generation;
- types of payment: face-to-face payment, remote payment, withdrawal;
- losses of the different actors: merchant's bank, acquirer of the transaction, cardholder's bank, issuer of the card, the merchant, cardholder, insurance company and any other operator involved;
- geographical area of issue or use of the card or the data encoded on them.

The statistics are based on a diversified sample, comprising as many respondents as possible, and encompassing the most representative operators on the market. This includes the payment card issuers and merchants represented within the Observatory but also other issuers and merchants.

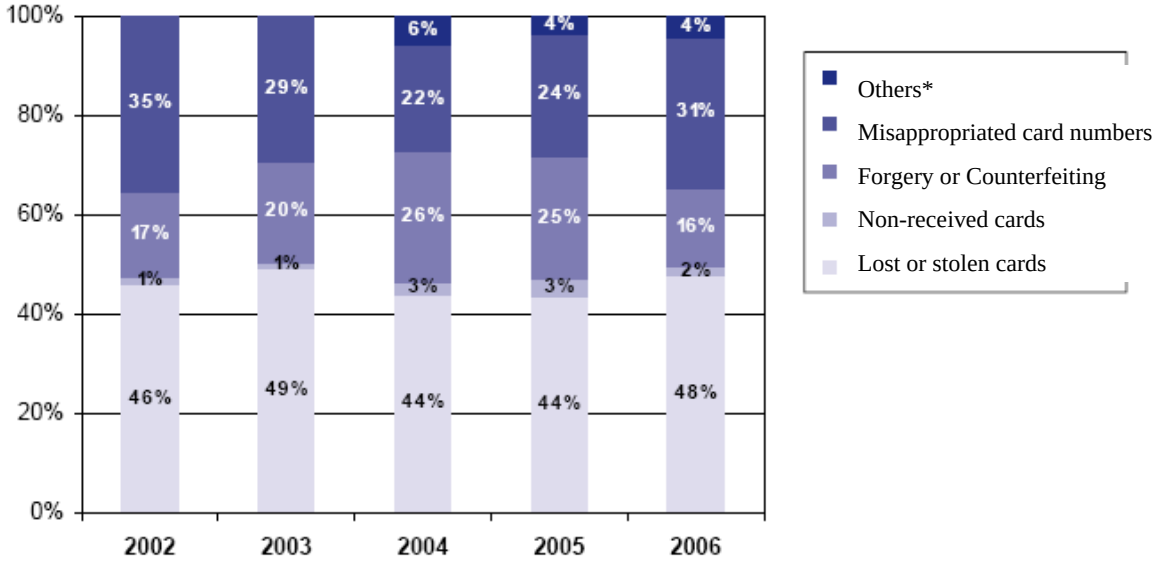
---

[95] The Observatory on payment cards security has been created by the Daily Safety Act n° 2001-1062 of 15 November 2001. It is in charge of promoting the exchange of information and the cooperation between interested stakeholders in the functioning of card payments systems.

[96] The Observatory found it necessary to develop its own methodology for calculating credit card fraud statistics due to the fact that available fraud statistics are not very accurate because dispersed and cover only a fraction of the payment cards issued in France and due to the difficulty of comparing statistics published by different issuers. The following description of the methodology used by this Observatory is extracted from its annual report of 2003, English version, pp. 17-25, available online at: http://www.banque-france.fr/observatoire/rap_act_gb_03.htm.

[97] For more information on the exact meaning of each of the terms and the extent of the category, see Annual Report of 2003, Chapter 3, available online in English at: http://www.banque-france.fr/observatoire/rap_act_gb_03.htm.

The following figure shows the evolution of credit card fraud according to its origins between 2002 and 2006:



Source : Observatoire de la sécurité des cartes de paiement

Figure 3.1. Types of credit card fraud

* The category "other" mainly relates to fraudulent opening of an account or credit file in private credit card companies, very significant for this type of card.

Figure 3.1 shows an increase in credit card fraud, the most important relating to card loss and theft. Counterfeiting is still the reason of 16% of fraudulent national payments. It is worth noticing that the theft of card numbers has increased between 2005 and 2006 after a 3 year-decline.

	All cards		**Bank cards**		**Private cards**	
2006	**Amount (Meuros)**	**Part**	**Amount (Meuros)**	**Part**	**Amount (Meuros)**	**Part**
Lost or stolen cards	52.5	47.9%	50.0	49.8%	2.5	27.5%
Non-received cards	1.8	1.6%	0.7	0.7%	1.1	11.7%
Forged or counterfeit cards	17.4	15.9%	17.1	17.0%	0.3	3.1%
Stolen card numbers	33.5	30.5%	32.7	32.5%	0.8	8.3%
Others	4.4	4.1%	-	-	4.4	49.4%
Total	109.6	100%	100.5	100%	9.1	100%

Table 3.3. Distribution of national fraud according to its origin and the type of card[98]

The Observatory's report observes that there is an increase in cases checked by police related to payment card fraud for the year 2006. In total, 53,755 cases of counterfeiting have been detected, 3496 persons have been arrested, and 1642 persons have received judicial custody.

3.2.3 On-line payment fraud

Finally, the report on On-line Payment issued by the Observatory for Cyber-Consumerism, under the resort of the Forum of Rights on Internet, issued in May 2005, assessed the reality of Internet users' fears.[99] This Report is based on a survey across different actors of on-line payment channels such as consumer organizations, public institutions, technical and financial providers, with the purpose of collecting experiences, practices and fears of Internet users related to e-commerce.

For 32% of Internet users surveyed, (insufficient) security of Internet payments remains an obstacle for online purchases. Three main fears have been identified during the survey: misappropriation of card numbers, automated creation of card numbers and recaptures of cards numbers in daily life. In all cases, Internet users fear inopportune withdrawals on their banking accounts causing them financial damages.

First, with regard to fraudulent interception of card numbers, the report reveals that none has been registered when the payment is made in a secure on-line environment. The reasons seem to rely, on the one hand, on the fact that service providers are allowed in very restrictive cases to store users' credit card information and on the other hand, on the encryption mechanisms used.

Second, automatic generation of credit card numbers cases remain marginal and not exclusive to the on-line environment. Off-line payments also suffered from this type of fraud. In that sense, safeguards such as the use of visual cryptograms or the 3D secure system have been implemented by actors of on-line payment channels (see Section 3.4.2). They managed to keep the risks originating from these practices under control.

Finally, with regard to fraudulently obtaining credit card numbers through off-line payments, the problem resides in the fact that credit card numbers appear on the receipt kept by the merchant. This number is currently necessary, in case of technical problems, to re-enter the transaction realised via the credit card. The solution has consisted in using a visual cryptogram printed in the credit card, which allows the merchant to ensure that the user has the credit card in their possession. Another weakness resides in purchases made by telephone, as the number is given to the merchant by the buyer. Police investigations demonstrated that embezzlers got the numbers through these practices in certain shops such as computers shops or petrol stations. The Observatory recommends a progressive process to delete credit card numbers on all receipts.

The conclusions of the report are reassuring in so far that it appears that multiple technical and organizational measures such as SSL protocol or dynamic generation of credit card number have been implemented in order to protect consumers during on-line credit card payments and that alternative payment solutions have developed simultaneously, for the

[98] Observatory of online payment security, extracted from the Annual report 2006.
[99] Forum des Droits sur l'Internet 2005, *supra* n. 87.

payment of small amounts (see further section 3.4.2). The report also strongly recommends awareness to be raised by public authorities and market actors (banks, online merchants, etc.) with users to fight *phishing* and software which exploits the vulnerabilities of the consumer's computer. The report also reviews micro-payment solutions that allow fast, easy to use payments which ensure relative anonymity for the user and do not imply significant additional costs for the merchant.

3.3 Vulnerabilities in the infrastructure

3.3.1 Identification Processes

3.3.1.1 Off-line identification

As mentioned above, there is a relative freedom in the proof of one's identity. No specific document is given legal value for identification by the law. Article 78-2 of the Code of Penal Procedure allows individuals to prove their identity by any means, i.e. according to a Ministerial circular of 11 December 1985, by any official document including a photograph, i.e. national identification card, passport or driver's license, any other document or through testimony of a third party provided they prove their identity. For foreigners residing in France, the stay/work permit is considered a valid form of identification.

In that sense, article L.131-15 of the Monetary and Financial Code states that individuals should prove their identity by demonstrating an official document which contains their photograph. The document most often used in commercial transactions remains the driver's license,[100] while the national identification card is largely used in relations with public authorities.

This system provides great flexibility. However, as a consequence of some failures in the handout and issuance procedure, a market of false identity documents has developed where the price of a false driver's license is estimated to be around 500 Euros and a false passport around 2,000 euros.[101]

It is worth noting that there is no obligation to formally change the address on official documents such as the identification card or passport. If citizens want these documents to be updated, they have to require a new document and follow the relevant procedure of request, submitting new documents which justify their right to handle this kind of documentation ("justificatif d'état civil", proof of residence, etc.).

3.3.1.2 Online identification

The issue of identification in the on-line environment has mainly arisen in the field of e-government. The French Data Protection Authority, the CNIL [*Commission Nationale de l'Informatique et des Libertés*], advocated for the protection of the anonymity of the user whenever it appears a valid alternative. To that effect, in the opinion on the Electronic Administration Plan,[102] this body defended the implementation of a 'graduate security principle' where anonymity should be the rule whenever authentication is not required for the

[100] Lecerf 2005, *supra* n. 90.
[101] Ibid.
[102] CNIL, Opinion on ADELE programme (electronic administration), 26 February 2004, available online at: http://www.cnil.fr/fileadmin/documents/approfondir/dossier/e-administration/ADELE2004.pdf, last accessed on 31 October 2007.

provision of the public service. Where it is required, authentication means should pass a strict proportionality test: security exigencies should be adapted to each e-process. Even the use of electronic signatures is recommended not to be systematic and, according to the CNIL, should not constitute a condition for the implementation of any e-processes.

Actually, most of the existing e-processes use authentication systems based on identification codes attributed by public agencies and a password chosen by the user. Electronic signatures are not intended to be generalised but only to allow the dematerialisation of services which require a high level of security. They are currently used for VAT e-payment, medical acts with health professional cards,[103] income e-declaration and for certain services provided through Daily Life Cards.[104]

Finally, a project is worth mentioning with a central portal providing access to most public services, www.monservicepublic.fr. The objective is to implement a Single-Sign-on mechanism where the user is automatically recognised by all public services after a unique authentication. This mechanism will simplify the current procedures which require the user to authenticate to every public service, according to the mechanism installed by each public agency. This space will enable the user to store any relevant documents to his relation with the administration. It will enable the citizen to transfer these documents directly to the public authorities which require it. However, this space is strictly personal and can not be accessed by public authorities. It is acknowledged as a safe whose key is handled by the user, who can open it on a case-by-case basis in his relationships with the administration.

3.3.2 The use of a central identification number

Every individual born in the French territory or who becomes a beneficiary of the French Social Security is attributed a registration number (NIR - *numéro national d'inscription au répertoire des personnes physiques*), commonly known as a "social security number". The sole purpose of the Directory, RNIPP (National Directory of Identification of natural persons, *Répertoire National d'Identification des Personnes Physiques*), is to prevent confusion on names (homonymy) and mistakes on the identity of individuals.

The number is largely used by public and private bodies linked to the health sector or finance sector. In other public sectors, the CNIL has always advocated the use of sector-based identifiers. With regard to the identifiers used for authentication functions, the French government expressly opted for adopting sector-based identifiers in accordance with the position of the CNIL.[105] The General Directorate of State Modernisation [*Direction générale*

---

[103] The French health electronic network is based on two different smart cards meant to authenticate beneficiaries (Vitale Card) and professionals (Healthcare professional cards –*Carte professionnelle de la Santé*- the so-called CPS card). The CPS card contains a function of authentication and signature. The Vitale card, held by the patient contains only a function of authentication. After a consultation, the Healthcare professional sends a petition of reimbursement to the Social Security. It uses the CPS to electronically sign such petition. More information is available at: www.sesam-vitale.fr as regards the Vitale card, and at: www.gip-cps.fr as regards the Health professional card.

[104] "Daily Life Cards" [*Cartes de vie quotidienne*] are smart cards delivered by the municipality, region or province to their citizen in order to give them access to a series of services such as public transportation, library, school, and swimming pool. See also Braun G., Informative report to the Senate n°402, For an electronic government at the citizen's service [*Pour une administration électronique au service du citoyen*], 6 July 2004, available at http://www.senat.fr/rap/r03-402/r03-4023.html (last accessed on 31 October 2007).

[105] Ministry of Civil Service, State Reform and Land Settlement, *Electronic Administration Strategic Plan (PSAE) 2004-2007*, p.16.

de la modernisation de l'État][106] is a governmental partner of Liberty Alliance and has opted for the use of federated identities. This option is presented to allow every public service provider to use its sector-based identifier but to prevent any link between public databases and separate identifiers. Furthermore, the authentication is facilitated for the user,who does not have to repeat the action several times.

In the private sector, stringent requirements surround its use. The use of the national number, the NIR, and the mere access to the national directory of natural persons, the RNIPP, are subject to prior authorisation of the CNIL (Article 25.6 Data Protection Act[107]). It should be proportionate to the purpose of the processing and should be founded on a public interest. On these grounds, the CNIL rejected the request of credit and debt recovery and insurance companies. It stated that even if the fight against homonymy was legitimate, it was not sufficient by itself to justify the use of the NIR in the field of management of saving products, credits or debt recovery. It appears from these decisions that the CNIL will judge the existence of a public interest on the possibility to base the use of the NIR on a legal provision. However, the mere fact that some entities, due to their collaboration with health public agencies are allowed to use the NIR for certain activities, does not entitle them to extend such use to other activities, in particular to improve their commercial relations with customers. The CNIL considered that the legal provision that based the use of the NIR in the first place could not warrant other uses of the NIR.[108] The same reasoning is applied to public bodies authorised to use the NIR for their public activities which can not use it for the management of a commercial relation with the user. These entities should use a specific identifier for their commercial relations.[109]

3.4 Countermeasures

3.4.1 Legal countermeasures

Identity fraud is protected in several ways under French law but not as a specific offence. First of all, identity theft will qualify as an offence in circumstances that lead or could have led to the initiation of a criminal prosecution against such a person (Article 434-23 of the Penal Code). To qualify as a conduct of identity theft under this provision, the thief also has to "assume the name of another person". As of today, no judgement has been rendered in the sense that the concept of "name" could be understood to include IP addresses, email addresses or pseudonyms.[110]

•

---

[106] Created in 2006, this General Directorate, under the resort of the Budget and State Reform Ministry, has replaced three specific agencies established in 2003 to carry out the Action Plan 'RE/SO 2007, For a Digital Republic in the Information Society' [*Pour une République numérique dans la Société de l'Information*] presented in November 2002. It is in charge of the global strategy aiming at the reform and modernization of the State.

[107] Act n° 78-17 of 6 January 1978 *relative à l'informatique, aux fichiers et aux libertés.*

[108] CNIL, Decision 2006-043 of 23 February 2006 denying autorisation to GIE 50 to process the social security number for purposes of multi-channel customers relationship.

[109] CNIL, Decision of 26 February 2006, available at http://www.cnil.fr/index.php?id=2003 (last accessed 31 October 2007).

[110] Iteanu O., Usurpation d'identité: la loi ou la technique pour se protéger?, Journal du Net, 9 March 2004, available on-line at: http://www.journaldunet.com/juridique/juridique040309.shtml, last accessed on 29 October 2007.

In most cases, identity theft is only a means to perpetrate other crimes. For this reason, article 434-23 of the Penal Code states that the conviction of identity theft is cumulative with other sanctions. This article is however hardly used in legal actions against online identity fraud. Other crimes provide better grounds for prosecution.

Indeed, in many cases, the sole act of assuming the name of another person will qualify as an offence. For example, offences such as fraud (article 313-1 Penal Code), forgery (article 441-1 Penal Code) or public defamation (Article 29 of the Press Act of 29 July 1881) could be mentioned. In a 2004 judgment, the First Instance Tribunal of Paris sanctioned a perpetrator of a *phishing* attack on the basis of fraudulent representation. The convict had mirrored a bank website and managed to order transfers of funds from his victims' bank account.[111]Other crimes prove useful for sanctioning identity-related crimes. Such is the case for unauthorised access to automated data processing systems (Article 323-1 Penal Code), mainly used as a legal basis in IP spoofing or in sniffing; brand counterfeit (Article L713-1 of Intellectual Property Code), *phishing* being here an example of a conduct that could be punished under this article; or fraudulent breach of trust (Article 314-1 Penal Code). In that sense, in the aforementioned judgment, the offender was also convicted for attempted fraud and fraudulent access to an automated data processing system; he received a suspended prison sentence of one year and a fine of 8,500 euros.

It is worth mentioning that, lately, some jurisprudence has also sanctioned *phishing* on the basis of brand counterfeit. In a judgment of 21 September 2005, the First Instance Tribunal of Paris convicted an offender who had created a mirror website of the registering page of MSN Hotmail with the aim to collect login and passwords of users to their email accounts on the basis of brand counterfeit. The court considered that this mirror website illegally owned the brand of Microsoft and reproduced and distributed it without prior authorisation. [112] The sanction, however, remains low (500 euros of fine in suspended sentence and 700 euros of damages to be paid to the Company) because of the young age of the offender and the fact that no personal data had been gathered.

The victim of the theft could also hold the fraudster liable in civil proceedings on the basis of the general rules of civil liability. For instance, if the perpetrator of the crime were to reveal part of the private life of the victim using his/her name, he/she could be found liable under article 9 (which acknowledges the right to privacy) and 1382 (general rules of civil liability) of the Civil Code. The most notable example lies in a judgment of the First Instance Tribunal of Carcassonne of 16 June 2006. In this case, a woman used different pseudonyms in a dating service website and described herself as an "easy woman willing to have sexual relations". She provided her colleague's contact details who started receiving numerous messages from individuals eager to meet her. This led her to fall into a depression and to ask for a sickness leave. The woman was deemed liable for voluntary duress ("*violences volontaires"*) with premeditation and had to compensate both her victim and the Public Health Insurance.

Finally, according to part of the doctrine, civil liability could even exist without any misconduct. The mere use of the name of third parties without their prior consent could be the basis for a tort action. This doctrine is based on an old judgement of 1965 which states that

---

[111] Tribunal de Grande Instance of Paris, 13rd Chamber, 2 September 2004, *Ministère public, Crédit Lyonnais and Caisse nationale du Crédit agricole* v. *Radhouan M. and others*, available at http://www.foruminternet.org/specialistes/veille-juridique/jurisprudence/tribunal-de-grande-instance-de-paris-13e-chambre-2-septembre-2004.html (last accessed 31 October 2007).

[112] Text available at: http://www.legalis.net/jurisprudence-decision.php3?id_article=1520.

identity theft victims should be protected from any theft of their name even if the victim is not 'damaged' in any sort of way.[113] However, as of today, no jurisprudence in that sense has been pronounced.

Finally, it is worth mentioning a Bill[114] presented in July 2005. This proposal tried to introduce a new crime (and thus the identity theft terminology) into the Penal Code entitled "digital identity theft on electronic communications networks". This Bill would have made punishable everyone assuming the identity of another person, company or public authority, in an electronic communication network, with a prison term of up to one year and a fine of up to 15.000 euros. On the basis that "identity is what forms the legal existence of a person", the proposal intended to address identity theft in the "virtual world". Its author argued that in the "real world" identity mainly consisted out of the information written in the Civil Registry and is protected as such by French law. However, in the "virtual world", identity is a broader concept with undefined borders. Identity could be materialised by "identifiers", e.g., a login and a password, elements not acknowledged by French law as part of the legal identity of a person.[115] This law proposal would actually be useful in cases where the identity fraud were not intended for fraudulent representation or without any fraudulent access to an automated data processing system. As mentioned above, the other cases are actually covered by the provisions of the Penal Code.[116]

The Bill was rejected, however, because the government in place at the time considered identity theft sufficiently covered under existing French law.[117] Nevertheless, in a recent discourse about the next measures the government will take to fight cybercrime, the Ministry of Defence has mentioned the introduction of a new offence punishing on-line ID theft with a prison term of one year and a fine of up to 15.000 euros.[118]

3.4.2 Technical and organisational countermeasures

Various technical and organisational safeguards have been spearheaded by financial institutions and online merchants. As such they mainly intend to secure the payment procedure.

Apart from the large-scale implementation of SSL protocols and in order to reduce the circulation of the numbers during a transaction and fight against the fraudulent obtaining of credit card numbers, several mechanisms targeted at the total or partial suppression of credit card numbers for the payment procedure have been put in place.

- The virtual dynamic card: the e-credit card [*e-carte bleue*]. This service allows the consumer to create in real time a new credit card number for each transaction. This number remains valid for a certain time and is deactivated once it has been used. It thus prevents the

---

[113] First Instance Tribunal (Tribunal de Grande Instance) Marseille, 9 February 1965, D.1965 270.
[114] Dreyfus-Scmidt M., Law proposal tending to the criminilisation of ID theft on electronic communications networks [*Proposition de loi tendant à la pénalisation de l'usurpation d'identité numérique sur les réseaux informatiques*], doc. N°452, Senate, 4 July 2005.
[115] CNIL, *supra* n. 109.
[116] Marc-Antoine LEDIEU, Usurpation d'identité: vers un délit spécifique, Communication Commerce électronique n° 9, Septembre 2005, Alerte 232.
[117] Ministerial answer of 19 October 2006, Senate O.J. 19 October 2006, p. 2665, available online at: http://www.foruminternet.org/documents/rapports_avis/lire.phtml?id=1129.
[118] AFP, Press realease, Cybercriminalité: Alliot-Marie présente un plan d'action "ferme et résolue", 14 February 2008, http://afp.google.com/article/ALeqM5hlRmL59Lhk7pRq1gwgEFOxHSHf2w.

reuse of the credit card number and double invoicing. In 2006, this mechanism was used in 2,5 million transactions with 130,000 new card holders, for a total of half a million users.[119] The use of this system requires the user to first register with his bank (on-line or via a paper-based form). The bank then provides the user with an identifier of 8 characters and sends him a password by mail. The use of the tool also requires the download of specific software to be installed on the user's computer.

- The system Sympass: Sympass is a company created in 2001 which has developed a tool relying on the principle of double keyboards: the computer's and the telephone's. When buying online, the user gives the 8 first digits of his credit card and a phone number. He then immediately receives a phone call of an automated voice service asking him to key the last 8 numbers of the credit card. Sympass counted 170,000 users in 2005.

- Payment by card without any indication of the number: the ID Tronic solution. In this system it is not necessary to provide the credit card number when conducting a transaction. When registering, the user provides his payment data to the bank which provides him with a password. When making the payment, the user provides his password or email address and receives a text message with a second password to authenticate the user.

- Use of a visual cryptogram to fight against the fraudulent obtaining of credit card numbers in off-line payments. It permits the cyber-merchant to check that the holder is physically in possession of the credit card. The conservation of the cryptogram is formally forbidden for security (and privacy) reasons.[120]

- 3D secure system: In order to fight new fraud such as *phishing*, a reinforcement of security of online payments is proposed through the 3D secure solution. This system integrates an additional step in the payment procedure. When the card number is sent by the merchant to the bank for authorisation, this entity will request the cardholder to authenticate to the system before sending such authorisation to the merchant. The merchant will thus not be held liable in case of identity fraud due to the additional check made by the bank during the payment. However, full implementation of the system faces strong opposition from both merchants and banks on the basis of economical and technical reasons.[12187]

- Finally, micro-payments instruments such as dialers, SMS premium, and the use of electronic wallet have been proposed to consumers for payments of less than 15 euros (threshold under which there is no legal obligation for the merchant to issue an invoice to the consumer). These payments instruments have the advantages of being quick, friendly, and cheap and of relatively preserving the anonymity of the buyer.

3.4.3 Credit reporting

Credit reporting in France is centralised by the French National Bank, a body which manages credit information on individuals provided by financial institutions. Several databases are maintained by this body. The *Fichier national des Incidents de remboursement de ces crédits aux particuliers* (FICP) includes information on significant overdue payments related to individual credits (personal loans, authorised uncovered balances, leasing, and installment buying). Measures taken in case of too high debts are also included. The body records only

---

[119] Press release, E-carte bleue: 2,5 millions de transactions en 2006, 24 January 2007, available online at: http://www.carte-bleue.com/page.asp?menu_id=74, last accessed on 24 October 2007.
[120] CNIL 2003, *supra* n. 88.
[121] Forum des Droits sur l'Internet 2005, *supra* n. 87.

the name, place and date of birth, the name of the body which requested the record and its origin and the date of deletion presumed.

Storage periods vary according to the procedure which has led to the record. As a general rule, the information is stored for a maximum of 5 years but it will be stored for 8 years in case of personal recovery procedure and for 10 years in case of recovery plan or if the over-indebtedness Commission formulated some recommendations in that sense. If the payment is made before the end of these periods, the records are deleted.

Other databases are managed by the French National Bank, on the basis of the information provided by financial institutions, relative to check bans when a bad check has been issued (*Fichier central des chèques*), to credit cards abuse or to irregular checks, stop payments relative to checks orders due to loss or theft, or closed accounts.

Furthermore, the private sector has created black-lists of individuals with overdue payments. This practice is however strictly regulated by the Data Protection Act and the CNIL. According to the principle of proportionality, the CNIL has put limits on the basis of the principle of "sectorisation". This principle implies that the generation of and access to databases which contain information on debts and non-payments of a certain category of persons, e.g., tenants, should be limited to the mere sector activity and its professionals. It considers that widespread access given to non-payment information to controllers outside that specific sector would be a disproportionate intrusion in the private lives of individuals because of the risk of function creep. According to the CNIL, the fact that a phone bill has not been paid should not prevent anyone from receiving the opportunity to rent living quarters.

In that sense, in the renting sector, the CNIL considered that providing real estate owners who were not strictly real estate professionals with information about unpaid rents was not in conformity with the obligation of security and the principle of proportionality. This doctrine has been confirmed by the State Council in a judgment of 28 July 2004.[122]

3.4.4 Public awareness campaigns

Several public awareness campaigns have been launched on the basis of private initiatives. As online consultation of bank accounts and conducting online transactions have become the second activity of French Internet users, French banks have undertaken initiatives to raise awareness of the risks involved in online banking to Internet users. The Federation of French Banks, FBF [*Fédération Bancaire Française]*, helped to sponsor a campaign to help teach people how to use the Internet safely. As part of this, almost three million brochures, comics and books were distributed in branch offices (of banks) and on bank websites. Advice was included on how to detect and avoid phishing, and on the importance of anti-virus software on computers. Banks also sent letters to their customers and posted alert messages online warning of potential dangers. The FBF regularly update their practical guide to secure online banking..[123] In addition, e-commerce actors have offered specific tool bars to enable users to identify secure websites.[124]

---

[122] See http://www.fbf.fr and http://www.lesclesdelabanque.com. See also State Council, Judgement n° 262851, published in Recueil LeBon, available at http://www.legifrance.gouv.fr/WAspad/UnDocument?base=JADE&nod=JGXAX2004X07X000000262851 (last accessed 31 October 2007).

[123] Information extracted from the French Banking Federation, *Press release 'Banks mobilise to increase Internet security'*, 31 December 2005, available at

The Forum of Rights on Internet also published several on-line guides and fact sheets for Internet users in order to provide them with useful tools for preventing abuses or defending themselves against such abuses. Worth mentioning, for instance, is the guide on on-line shopping[125] published on 17 November 2005 and updated regularly since, which furthermore includes advice against *phishing*. This guide includes advice for every step of the purchase, from the selection of the online merchant to the payment process and the exiting recourses in case of problems. A specific part is dedicated to C2C websites. The 2008 edition furthermore includes advice on online video games and travel online booking.

3.5 Conclusion

This chapter shows that, from a policy standpoint, identity fraud is considered a big problem only from a document fraud point of view. This is actually the main argument advanced by the government to legitimise the introduction of an eID card with biometrics identifiers and based on centralised databases. However, it has appeared difficult to obtain accurate statistics on the prevalence of the phenomenon as no benchmarks have been developed so far.

Another type of identity fraud, financial fraud, is considered a problem which is considered to be best combated by technical and organisational measures and by educating Internet users. Statistics reveal an increase in credit card fraud, which however does not seem to be perceived as a real threat by organisations such as the Forum of Rights on Internet or even by Internet users, as shown by a recent survey conducted by Unysis.[126]

From a legal point of view, the previous government estimated that the legal framework provides sufficient protection against this kind of practice. Actually, identity fraud offences are hardly used in legal procedures when it comes to new forms of identity-related crime, such as *phishing*. Other crimes are better suited to prosecute offenders , such as fraud or unauthorised access to an information system. Cases where identity theft is not intended to result in fraudulent representation nor perpetrated through unauthorised access to an information system remain however unprotected. In that sense, Eric Braby and Vincent Dufief[127] highlighted that only one case does not fall under the legal provisions: when a person steals the digital identity of another without his/her knowledge. This could be the case when an individual creates false email addresses or digital identifiers without using them yet. The act would qualify as preparatory act and would not be criminally punishable. The victim would thus have no penal remedy against such conducts. Victims could, however, obtain remedies in civil courts on the basis of a judgement of 1965 giving protection to the sole use

---

http://www.fbf.fr/web/internet/content_europe.nsf/(WebPageList)/662BED67AF6A21F4C125717100560858 (last accessed on 31 October 2007).

[124] C. Guillemin, 'Des barres d'outils pour Internet Explorer et Firefox protègent du "phishing"', *ZdNet*, 4 January 2005.

[125] Forum des droits sur l'Internet, Online purchase: follow the guide [*Achats en ligne: suivez le guide*], edition 2008 available at http://www.foruminternet.org/particuliers/guides/IMG/pdf/Guidedesachatsenligne2008.pdf, last accessed on 3 December 2007.

[126] Unysis, press release, "Key Growth Economies Most Worried About Security Threats, Unisys Global Survey Reveals, 30 October 2007, available online at: http://home.businesswire.com/portal/site/google/index.jsp?ndmViewId=news_view&newsId=20071030005080&newsLang=en, last accessed on 31 October 2007

[127] Barby E. & Dufief V., Note to the Judgment of the TGI Carcassonne (corr.), 16 June 2006, *Gazette du Palais*, 19 October 2006 n° 292, p. 36.

of the "name".[128] In this case it would however remain to be seen whether digital identifiers qualify as "names".

[128] *Supra*, n. 113.

4 Germany

This Chapter provides an overview of the prevalence of and debate about identity-related crime in Germany. After a brief discussion of concepts used, figures are given for various forms of crime. Subsequently, vulnerabilities in the infrastructure that facilitate identity-related crime are discussed, as well as countermeasures currently taken.

4.1 Concepts

In Germany, no explicit codification of identity-related crime exists which actually refers to the term 'identity' in the statute.[129] Generally speaking, criminal law is laid down in the German *Strafgesetzbuch*, the Penal Code.[130] In addition, criminal offences can be regulated in specific areas of the law, like environmental law, copyright law, or data protection law.

In public discourse, the term *'Identitätsdiebstahl'* ('identity theft') is sometimes used. In addition, the term *'Identitätsmissbrauch'* (identity misuse) is used. The focus of the public and academic discussions on identity-related crime in Germany rests with phishing as a means of unlawfully taking over a chosen identity[131] and on fraud enabled by misuse of credit card information. Furthermore, there has been debate on cases of eBay account misuse and account takeover. Again, these forms of crime are not always discussed in the context of 'identity-related' crime but with regard to the applicable provisions of the German Penal Code.

Even though the terms *Identitätsdiebstahl* and *Identitätsmissbrauch* are used regularly in the media, only few definitions are available in German studies. The few available distinct definitions of identity theft (*Identitätsdiebstahl*) in German sources are given by the Arbeitsgruppe Identitätsschutz im Internet (ai3)[132] and Gercke[133]. Another, non-academic, source is Wikipedia.[134] None of these sources, however, discuss different forms of identity-related crime and result in a categorisation comparable to the level of detail of the FIDIS typology.

Ai3 defines 'identity theft' as follows: an offender makes use of another person's identifying data, in order to take over that person's identity. In the FIDIS categorisation, this definition concerns the subcategory of 'identity takeover'. Wikipedia defines identity theft as misuse of a natural person's personal data by a third party, and further states that identity theft usually aims at obtaining financial benefit or discrediting another person.

Identity misuse (*Identitätsmissbrauch*) is defined by Borges and Schwenk[135] as an offender causing false attribution of an action to a natural person.

Judgments explicitly mentioning the term identity theft are scarce and occur only in civil lawsuits.[136] In criminal law cases, the various forms of identity-related crime are addressed in

---

[129] See result of the first survey on legislation on ID theft in the EU, FIDIS Deliverable 5.1.
[130] Available in German at http://www.gesetze-im-internet.de/stgb/BJNR001270871.html.
[131] For terminology, see Koops, Bert-Jaap, Ronald Leenes, Martin Meints, Nicole van der Meulen & David-Olivier Jaquet-Chiffelle (2008), 'A Typology of Identity-related Crime: Conceptual, Technical, and Legal Issues', *Information, Communication & Society* (forthcoming).
[132] Available at https://www.a-i3.org/content/view/930/201/.
[133] Gercke, M., ‚Die Strafbarkeit von „Phishing" und Identitätsdiebstahl"', *Computer und Recht* 2005, p. 606.
[134] See http://de.wikipedia.org/wiki/Identitätsdiebstahl.
[135] Borges, G. and Schwenk, J. ‚Identitätsschutz: Eine zentrale Herausforderung für IT und E-Commerce', 2007. Available at https://www.a-i3.org/images/stories/recht/itgipfel_paper061218.pdf.

several Penal Code provisions without discussing the action with regard to identity-related crime. Hence, discussion of identity-related crime mainly takes place in relation to the codified statutory offence which covers the action in question.

4.2 Prevalence

Specific figures on the prevalence of identity-related crime are scarce. No comprehensive study on the situation in Germany is available, and the figures presented are not broken down into the FIDIS conceptual categories. Sources for assessing the extent of identity-fraud include rather small online surveys,[137] the 'Crime Statistics of the German Federal Criminal Police Office (BKA)',[138] as well as the German Federal Office for Information Security's (BSI) report on 'The IT Security Situation in Germany in 2007',[139] where figures on phishing incidents and Internet-related crime are presented.

The Internet is a commonly used tool for identity-related crime. However, the Crime Statistics contain no figures broken down to whether regulated criminal offences were committed in relation to creating a new or taking over an existing identity. The Crime Statistics 2006 present the following figures[140] regarding crimes 'committed by means of the Internet'.

Type of criminal offence	**Reported number**		**Difference**		**Success rate in solving crimes**	
	2006	**2005**	**total**	**in %**	**2006**	**2005**
Total number	150.785	118.036	32.749	27,7	84,0	84,9
Offering and distributing child pornography	5.351	5.624	-273	-4,9	78,5	76
Fraud	124.501	93.816	30.685	32,7	86	86,1
Fraud to obtain a good on credit	15.555	10.322	5.233	50,7	94,8	94,3
Fraud to obtain a good	78.235	53.092	25.143	47,4	95,3	94,2
Fraud to obtain a public benefit	3.153	800	2.353	294,1	88,3	84,4
Fraud to obtain a service on credit	5.235	2.337	2.898	124,0	47,9	77,6

[136] Civil law cases mentioning the term ‚identity theft' cover fraud related to taking over eBay accounts or creating new accounts using identifying data of another person. The higher regional court (*Oberlandesgericht*) Brandenburg ruled that eBay, in case it gains knowledge of a prior creation of a fake account, has to take precautionary measures preventing a similar action concerning the victim of the prior unlawful activity (4 U 5/05). The German Federal Supreme Court (*Bundesgerichtshof*) upheld the decision under appeal in a verdict decided on 11 April 2008. See http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2008&Sort=3&nr=43425&anz=72&pos=0&Blank=1.

[137] Like the monthly online survey at 'a-i3.org' (Arbeitsgruppe Identitätsschutz im Internet). Available at https://www.a-i3.org/component/option,com_exitpoll/task,results/id,18/.

[138] The ‚*Polizeiliche Kriminalstatistik*' is available at http://www.bka.de/pks/.

[139] Bundesamt für Sicherheit in der Informationstechnik, ‚The IT Security Situation in Germany in 2007', p. 27-28. Available at http://www.bsi.de/english/publications/securitysituation/Lagebericht_2007_englisch.pdf.

[140] Available in German at http://www.bka.de/pks/pks2006/ex_i_1.pdf.

Type of criminal offence	Reported number		Difference		Success rate in solving crimes	
	2006	2005	total	in %	2006	2005
Computer-related fraud	8.285	8.168	117	1,4	41,8	35,6
Other types of fraud	8.694	13.207	-4.513	-34,2	69,9	88,2
Offences related to infringements of copyright	10.286	10.432	-146	-1,4	85,5	92,6

Table 4.1. Crime Statistics 2006: offences committed by means of the Internet

Further figures exist regarding 'computer system related criminal offences'.[141] These include information referring to identity-related crimes like fraud by means of illegally obtained debit cards and the corresponding PIN number, cases of spying out PIN numbers as well as cases of fraud regarding access rights to communication services.

Type of criminal offence	Reported number		Difference		Success rate in solving crimes	
	2006	2005	total	in %	2006	2005
Fraud by means of illegally obtained debit cards and the according PIN	27.347	32.232	-4.885	-15,2	40,6	40,9
Spying out data (including PIN)	2.990	2.366	624	26,4	43,8	42,2
Fraud regarding access rights to communication services	5.822	5.788	34	0,6	57,7	64,4

Table 4.2. Crime Statistics 2006: computer -related offences

Further criminal offences[142] listed in the Crime Statistics 2006 which are relevant in the context of identity-related crime are presented in Table 4.3. It is however not known how many of these crimes were committed in relation to creating a new or taking over an existing identity. These figures do not differentiate between offences committed by means of the Internet and other offences.

Type of criminal offence	Reported number		Development		Success rate in solving crimes	
	2006	2005	total	in %	2006	2005
Fraud by means of illegally obtained debit cards without PIN	41.561	48.143	-6.582	-13,7	53,1	48,7

[141] Available in German at http://www.bka.de/pks/pks2006/p_3_21.pdf.
[142] Taken from http://www.bka.de/pks/pks2006/p_3_09.pdf, and http://www.bka.de/pks/pks2006/tab_01.pdf.

Fraud by means of illegally obtained debit cards with PIN	27.347	32.232	-4.885	-15,2	40,6	40,9
Fraud by means of illegally obtained credit cards	8.932	14.184	-5.252	-37,0	48,4	52,5
Forgery of debit cards, cheques and bills	3.562	1.765	1.797	101,8	35,8	40,6
Fraud by means of illegally obtained data from debit cards	3.646	3.610	36	1,0	39,6	51,0
Fraud on the occasion of opening a bank account / making a remittance	13.297	11.130	2167	19,5	74,8	74,0

Table 4.3. Criminal Statistics 2006: other criminal offences in relation to identity

In addition to these numbers concerning frequency, the Crime Statistics also offer figures on the amount of damage resulting from some of these offences.[143] In almost all categories a declining amount of damage can be observed. This observation holds true also for the overall number of cases.

Type of criminal offence	**Reported number**			**Amount of damages in EURO**		
	2006	**2005**	**2004**	**2006**	**2005**	**2004**
Fraud by means of illegally obtained debit cards without PIN	41.561	48.143	67.591	10.760.504	12.948.112	20.110.122
Fraud by means of illegally obtained debit cards with PIN	27.347	32.232	36.088	21.441.580	23.266.608	26.294.895
Fraud by means of illegally obtained credit cards	8.932	14.184	17.057	6.628.849	8.151.324	8.060.263
Fraud regarding access rights to communication services	5.822	5.788	7.357	15.161.869	17.027.727	134.473.720
Fraud by means of illegally obtained data from debit cards	3.646	3.610	3.373	2.544.062	3.063.804	1.773.783

[143] Available at http://www.bka.de/pks/pks2006/tab_07.pdf, http://www.bka.de/pks/pks2005/tab_01.pdf, and http://www.bka.de/pks/pks2004/tab_07.pdf.

Type of criminal offence	Reported number			Amount of damages in EURO		
	2006	2005	2004	2006	2005	2004
Fraud on the occasion of opening a bank account / making a remittance	13.297	11.130	11.694	35.510.921	45.665.820	49.467.481

Table 4.4. Criminal Statistics 2006: damages for criminal offences in relation to identity

With regard to forgery of passports, an official answer[144] of the German government to a parliamentary request of the parliamentary group DIE LINKE presented the following figures. In April 2007 about 28,2 million German passports were issued. Checks upon entry to Germany and other occasions have revealed 6 forged and 344 altered passports from 2001 to 2006.

In March 2008 the BKA president Jörg Ziercke lead the German Federal Criminal Police Office's annual press conference 2007. On this occasion he presented figures and recent developments regarding debit card related crime as well as information and communications technology related crime.[145] On this event Ziercke explicitly mentioned 'identity theft (*Identitätsdiebstahl*)'. The figures were presented not as part of the Crime Statistic 2007[146] but with regards to the BKA's strategy concerning new challenges in crime prevention. According to the numbers reported, 1,349 attacks aimed at 459 ATMs were carried out in Germany in 2007. This equates to a rise of almost 50% compared to 2006. The amount of damages sums up to some 21 million EURO caused in 70.000 cases. The method mainly used for such an attack is skimming. The BKA states that taking into account the international figures regarding debit card related crimes gives rise to the expectation that this 'phenomenon will gain further relevance' in Germany, too. The figures presented with regards to information and communications technology related crime are presented to be preliminary. In 2007 overall 34,000 cases of information and communications technology related crime were reported which means a rise of 17% in comparison to 2006. A rise of 8% (180.000 cases overall) regarding offences committed by means of the Internet is mentioned. Specific figures concerning 'phishing' are accounted by the BKA regarding 2007: 4,200 cases (a rise of 20%) were reported. The average amount of damages caused by phishing attacks is described to range between 4,000 and 4,500 EURO in 2007. In 2006 the average amount of damages ran up to 2,000 to 3,000 EURO per case. With regards to 'identity theft' the BKA stated that no longer only online banking has been in the focus of criminals. In addition access data regarding all kind of citizens' internet accounts is targeted by identity theft attacks.

While the German Crime Statistic[147] 2006 painted a positive picture regarding the declining number and amount of damage resulting from criminal offences which under current German law mainly cover criminal actions relating to identity, this trend seems to have stopped in

[144] Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE – Drucksache 16/5228 – Notwendigkeit neuer biometrischer Pässe aus Sicherheitsgründen, 29 May 2007. Available at http://dip.bundestag.de/btd/16/055/1605507.pdf.

[145] See http://www.bka.de/pressemitteilungen/2008/pm080328.html.

[146] The Crime Statistic 2007 was not yet available on 22 April 2008.

[147] The German Crime Statistic is derived from figures reported by all German police offices. Detailed keys exist for all crimes and applied by the police personnel when reporting on their files.

2007. The overall number of phishing attacks is however rather small. Reports and figures presented by companies offering IT-security software and technology present an even more negative trend regarding especially the frequency of phishing attacks.[148] Moore and Clayton define phishing as 'the process of enticing people into visiting fraudulent websites and persuading them to enter identity information such as usernames, passwords, addresses, social security numbers, personal identification numbers (PINs) and any further information that can be made seen plausible. This information is then used to impersonate the victim so as to empty their bank account, run fraudulent auctions, launder money, apply for credit cards, take out loans in their name, and so on'.[149]

Worldwide, according to the Anti-Phishing Working Group, an average of over 30,000 phishing websites are detected every month.[150] In March of 2007, Symantec reported that 32% of all phishing websites were hosted in Germany,[151] which made Germany Europe's leading nation in this respect. Furthermore, Symantec stated that 'identity theft and selling of data via the internet is growing steadily' (March 2007) and 'identity theft is becoming ever more sophisticated' (September 2007)[152]. In this statement Symantec explains that 'already 65% of the top-50 worldwide attack tools aim at identity theft' and further: '23% of bot-infected computers are located in Germany'. Arrests have been reported with regard to phishing activities.[153] The Federal Office for Information Security's IT Security Report 2007 discusses identity theft in the form of phishing attacks and states: 'According to the banks only around ten percent of the damage occurring in Germany in 2006 was caused by the classic E-mail method. Trojan horses were responsible for the remaining 90 percent'.[154] While at the beginning of 2006 forged websites were still responsible for about 30% of phishing attacks, their share decreased to less than 10% at the end of 2006. The German Association for Information Technology, Telecommunications and New Media (BITKOM) estimates damages of 13 million Euro caused by 3,250 phishing attacks in 2006.[155]

The Federal Office for Information Security's IT Security Report 2007 describes that not only financial institutions, but also e-commerce applications and online shops are being targeted more often by phishers. According to this report the data obtained covers short-term access and transaction data as well as identity information such as birth dates, addresses, driver's license numbers as well as account and credit card information.

---

148 It is controversial among German legal scholars whether sending phishing emails is covered by any existing provision of the German Criminal Code. See for example Borges, G., 'Rechtsfragen des Phishing – Ein Überblick', *Neue Juristische Wochenzeitschrift* 2007, p. 3313-3317 and Gercke, M, ‚Die Strafbarkeit von „Phishing" und Identitätsdiebstahl.', *Computer und Recht* 2005, p. 606. It is however not controversial that if phishing emails result in financial damages, the activity is covered by provisions of the Penal Code.

149 Moore, T. and Clayton, R. 'An Empirical Analysis of the Current State of Phishing Attack and Defense'. Available at http://www.cl.cam.ac.uk/~rnc1/weis07-phishing.pdf.

150 Anti-Phishing Working Group, ‚Anti-phishing Trends – Report for the Month of August 2007'. Available at http://www.antiphishing.org/reports/apwg_report_august_2007.pdf.

151 Symantec, ‚Symantec Sicherheitsreport: Deutschland mit den meisten Phishing-Webseiten in Europa', 19 March 2007. Available at http://www.symantec.com/de/de/about/news/release/article.jsp?prid=20070319_01.

152 Symantec, ‚Symantec Sicherheitsreport: Mit dem Breitband kamen die Bots', 17 September 2007. Available at http://www.symantec.com/de/de/about/news/release/article.jsp?prid=20070917_01.

153 Heise security, 'BKA verhaftet Phisher-Gruppe', 13 September 2007. Available at http://www.heise.de/security/news/meldung/95928/BKA-verhaftet-Phisher-Gruppe.

154 Bundesamt für Sicherheit in der Informationstechnik, ‚The IT Security Situation in Germany in 2007', p. 27-28.

155 See http://bitkom.org/de/presse/8477_47739.aspx.

4.3 Vulnerabilities in the infrastructure

4.3.1 Identification Processes

In general it is possible for companies to require a special form of documentation from the other contracting party. The German ID Card Act (*Personalausweisgesetz*)[156] contains provisions concerning use of the German ID card in the relation between citizens and public authorities as well as between citizens and companies. Section 4 para 1 *Personalausweisgesetz* lays down an opening clause generally permitting use of ID cards for identification in the private sector. However, using the ID card number in a way which allows linking of data is not permissible (Section 4 para 2 *Personalausweisgesetz*). In addition, a specific legal basis is needed for each case where a company intends to require someone to show an ID card or passport for identification purposes. Usually this legal basis will be section 28 para 1 number 1 Federal Data Protection Act (*Bundesdatenschutzgesetz*) if the provision's requirements are fulfilled.

When engaging in business relations with companies, the forms of documentation used and even required as identification depend on the kind of service or contract the data subject is seeking to obtain or conclude. For some kinds of contracts specific legal requirements exist regarding the documentation to be used. These specially codified provisions usually cover the obligation to present an ID card upon entering into a contract or using a service.

Showing an ID card or passport in Germany is required when opening a bank account. This obligation is derived from section 154 para 2 Tax Code (*Abgabenordnung*) and section 1 para 5 and section 2 para 1 Money Laundering Act (*Geldwäschegesetz*).[157] The former lays down the obligation for entities running bank accounts to obtain certainty about the identity and address of individuals entitled to dispose. Requiring new customers who try to open an account to show their ID card or passport is regarded[158] as an appropriate means to obtain this certainty. The latter law defines the obligation of credit institutions, financial service institutions, financial enterprises and insurance companies to establish the identity of the other contracting party when concluding a contract, establishing a business relationship intended to operate on a lasting basis. In this context identification means the establishment of a person's name by means of a valid ID card or passport, as well as the date of birth, the place of birth, the nationality and the address.

Further occasions where companies require presenting an ID card or passport include closing a cell phone or landline service contract. Section 95 para 4 of the Telecommunication Act (*Telekommunikationsgesetz*)[159] allows for the service provider to require presentation of an official identity card where it is necessary 'to verify the subscriber's particulars'. The service provider may make a copy of the identity card. The copy is to be destroyed by the service provider without undue delay once the particulars needed for the conclusion of the contract

---

[156] Available in German at http://www.gesetze-im-internet.de/pa_g_1986/BJNR105370986.html.
[157] An unofficial translation to English is available at http://www.anti-moneylaundering.org/uploads/Germany.pdf.
[158] See for example opinion of the Privacy Commissioner of Berlin at http://www.datenschutz-berlin.de/jahresbe/00/teil4-6.htm.
[159] Available in English at http://www.bfdi.bund.de/cln_027/nn_946430/EN/DataProtectionActs/Artikel/TelecommunicationsAct-TKG,templateId=raw,property=publicationFile.pdf/TelecommunicationsAct-TKG.pdf.

have been established. The transposition of Directive 2006/24/EC has also led to new know your customer obligations in the telecommunications sector.[160]

In order to provide public authorities with the most recent address citizen registers are run in all German *Bundesländer*. In addition, also natural persons may obtain address information on citizens from these registers. Citizens are obliged[161] to notify the responsible registration authority (*Meldebehörde*) within two weeks when

- moving into a new domicile, or
- moving out of a domicile and not moving into a new domicile in Germany.

Decentralized registers of residents are run according to the registration laws[162] (*Melderecht*) of the German *Bundesländer*.[163] These registers provide[164] the latest address information which is available at the request of public authorities, if transmission is necessary for carrying out responsible tasks. Citizens are obliged to present all necessary documents to prove their statements, upon request to the registration authority. These documents usually cover an ID card or passport as well as the tenancy agreement.[165]

The registration laws also provide[166] an information right (*Melderegisterauskunft*) for natural persons other than the data subject. If a natural person or entity requesting the current first name and surname, doctoral degree, and address is able to identify the data subject based on first name and surname, date of birth, or a former address, the requested current information is generally provided (so called *einfache Melderegisterauskunft*).[167] In addition, if the requesting natural person or entity can show probable cause of a justified interest, also the following data will be transmitted:

- date and place of birth,
- former first and surnames,
- marital status,
- citizenship,
- former addresses,
- day of moving into / out of domicile,

---

[160] Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EC. Available at http://www.bundesrat.de/cln_051/nn_8336/SharedDocs/Drucksachen/2007/0701-800/798-07,templateId=raw,property=publicationFile.pdf/798-07.pdf.

[161] Section 11 MMRG and for example section 11 LMG SH.

[162] See for example the Meldegesetz für das Land Schleswig-Holstein (LMG SH). Available in German at https://www.datenschutzzentrum.de/download/lmg2004_gesetz+hinweise.pdf. The Meldrerechtsrahmengesetz (MRRG) lays down the framework for the laws of the German Bundesländer. It is available in German at http://www.gesetze-im-internet.de/mrrg/BJNR014290980.html.

[163] See also Buitelaar, Hans (ed.) (2007), *D13.3: Study on ID Number Policies*, FIDIS deliverable, available at http://www.fidis.net, p. 82.

[164] See section 18 MRRG and section 24 LMG SH.

[165] See for example information given by the city of Kiel registration authority: http://www.kiel.de/Aemter_01_bis_20/10/Service_10/Service_10_6/Anmeldung.htm.

[166] See section 21 MRRG and section 27 LMG SH.

[167] Exemptions are regulated for example in case the information may cause a threat to life, physical integrity or freedom of the data subject.

- first name and surname of spouse or civil partner,
- legal guardian,
- day and place of death.

A justified interest is for example assumed in case the requesting entity can show probable cause of pursuing legal claims against the data subject. As of today there are no publicly known cases in which perpetrators of identity-related crime have been able to obtain personal data in this way.

4.4 Countermeasures

4.4.1 Legal Measures

4.4.1.1 Criminal Law

No specific criminal provisions have been introduced to criminalize identity theft or identity fraud. Most cases of identity-related crime can be prosecuted on the basis of existing criminal provisions, both traditional ones, like theft, fraud, and forgery, or on the basis of computer-related offences. With respect to the latter category, it is relevant that Germany is expected to ratify the Council of Europe Cybercrime Convention soon. The German *Bundesrat* passed the government's draft ratification law[168] on 9 September 2007 without objections or amendments. The Cybercrime Convention contains obligations for the ratifying countries[169] to adopt legislative measures to criminalize various forms of cybercrime. These forms, which under certain circumstances can be used to prosecute identity-related crime, are already largely regulated in German criminal law. In August 2007, a law changing the Penal Code was passed which aimed at adjusting the German Penal Code to the Cybercrime Convention[170] as well as at transposing Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.[171] presents a rough overview of the corresponding German provisions.

Cybercrime Convention requirement	**Applicable provision(s) in German Penal Code**
illegal access to computer systems	§202a
illegal interception of non-public transmission of computer data to, from or within a computer system	§202a, §202b
data interference (intentional damaging, deletion, deterioration, alteration or suppression of computer data without right)	§303a

[168] The draft ratification law is available at http://www.bundesrat.de/cln_051/nn_8336/SharedDocs/Drucksachen/2007/0601-700/666-07,templateId=raw,property=publicationFile.pdf/666-07.pdf.

[169] The current status of ratification can be found at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG.

[170] So called *41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität (41. StrÄndG).* Available in German at http://www.bgblportal.de/BGBL/bgbl1f/bgbl107s1786.pdf. An overview on the changes resulting from this law is given by Ernst, S. 'Das neue Computerstrafrecht', *Neue Juristische Wochenzeitschrift* 2007, p. 2661-2666.

[171] Available at http://eur-lex.europa.eu/LexUriServ/site/en/oj/2005/l_069/l_06920050316en00670071.pdf.

system interference (intentional hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data)	§303b
misuse of devices	§202c, §303b
computer-aided forgery	§269, §270
computer-aided fraud	§263, §263a
content-related offences	§184, §184a, §184b, §184c

Table 4.5. Cybercrime Convention and German criminal law

4.4.1.2 Security breach notification

Companies do not provide data on cases of identity-fraud on a regular basis. In Germany, currently no security breach notification law is in place. In June 2006 the parliamentary group Bündnis 90/Die Grünen submitted a request to the German Bundestag, calling for the introduction of such a law.[172] In this request, which is expected to be denied by the majority of members of parliament,[173] the parliamentary group voices its concern regarding the 'growing number of cases of Identity Theft'. Furthermore, the representatives refer to the security breach notification laws passed in California and several other US states,[174] and call to strengthen affected citizens' rights regarding improper use of data by private entities. The US approach is regarded as a promising approach to fight criminal activities with regard to identity related security breaches. A reference to existing sanction powers of the Federal Trade Commission (FTC), the Federal Communication Commission (FCC), and banking supervision institutions is made. The parliamentary group even calls for the implementation of a claim for a provision of damages in case of a security breach as well as a provision regulating fines in case of violation of the notification obligation. Even though not explicitly mentioned in the request, these instruments would significantly increase pressure on private entities to implement state of the art technical and organisational measures to prevent identity-related criminal activities. In addition to financial consequences, an existing notification obligation may affect customers' trust in case a security breach occurred.

In May 2007 the *'Innenausschuss'* (Committee for interior issues) of the German Bundestag conducted a consultation on the 'Modernization of Data Protection Law',[175] Some of the invited experts addressed the request and supported passing security breach notification legislation as the aforementioned request was part of the agenda.[176] One invited expert was of the opinion that a German security breach information law should not only be addressed at

[172] Antrag der Abgeordneten Silke Stokar von Neuforn und der Fraktion BÜNDNIS 90/DIE GRÜNEN: ‚Informationspflichten für Unternehmen bei Datenschutzpannen einführen', 20.6.2006. Drucksache 16/1887. Available at http://dip.bundestag.de/btd/16/018/1601887.pdf

[173] The parliament's leading committee for interior issues as well as the legal committee, the committee for economy and technology and the committee for culture and media advised the parliament to reject the request. See http://dip.bundestag.de/btd/16/067/1606764.pdf.

[174] For an overview see http://www.ncsl.org/programs/lis/cip/priv/breach.htm.

[175] Information is available at http://www.bundestag.de/ausschuesse/a04/anhoerungen/Anhoerung05/index.html

[176] Agenda available at http://www.bundestag.de/aktuell/presse/2007/pz_0702281.html.

private entities but also at public entities.[177] However, she stated that a security breach notification law would damage the economy (due to potential costs of notification via ordinary mail as well as negative impact on private entities' reputation in case of a security breach which was 'not the company's fault'). She therefore called for self-regulation of companies. The Federal Data Protection Commissioner[178] supported security breach notification legislation pointing to the fact that only in case a security breach was brought to the attention of affected customers were they put in a position to take countermeasures or file a lawsuit for compensation of damages. The Federal Data Protection Commissioner highlighted in his opinion that the market would 'punish' companies unable to process and protect data appropriately if a security breach was brought to the attention of affected customers. The Commissioner further indicated that US companies are known to have put far greater effort on implementing a strategy for better data protection after security breach laws had been passed and that security breach laws in general help to limit customers' damages as it enables them to take countermeasures. The Privacy Commissioner of Berlin[179] supported this view and stated that transparency with regard to security breach fosters the implementation of preventive measures as well as a quick response to actual breaches. Finally, he supported the Art. 29 Data Protection Working Party's opinion 8/2006 on the review of the regulatory Framework for Electronic Communication and Services which advocates the requirement of notification of security breaches by network operators, ISPs, and data brokers, banks and other online service providers.

The German Association for Data Protection and Data Security[180] (GDD) voiced its concerns regarding proportionality of a security breach notification law. Only in case of 'severe' infringement of personal rights should private entities be obliged to notify customers, according to GDD. GDD regards a general obligation to notify of any security breach an 'inadequate burden' for companies. Finally, the Deputy Privacy Commissioner of Schleswig-Holstein pointed[181] to existing international management standards which already today include obligations to notify according to the severity of the security incident in question. In this light he regards security breach notification as part of a Data Protection Management Process (DPMP).[182] Finally, he stresses that security breach notification would foster competition on privacy-compliant technologies and processes assuring compliance.

4.4.2 Technical and organisational measures

The Federal Office for Information Security's IT Security Report 2007 describes countermeasures taken by the German government as follows: 'Main measures of the Federal Government for ensuring a secure electronic identity and for protection against identity theft are the introduction of an electronic ID card and funding for citizen portals within the framework of the E-Government 2.0 campaign. Both projects enable binding authentication

---

[177] Sasse, C. ‚Schriftliche Stellungnahme der Sachverständigen zur Öffentlichen Anhörung im Innenausschuss des Deutschen Bundestages zur Thematik „Modernisierung des Datenschutzes" am 05. März 2007'. Available at http://www.bundestag.de/ausschuesse/a04/anhoerungen/Anhoerung05/Stellungnahmen/Stellungnahme02.pdf.

[178] See http://www.bundestag.de/ausschuesse/a04/anhoerungen/Anhoerung05/Stellungnahmen/Stellungnahme03.pdf.

[179] See http://www.bundestag.de/ausschuesse/a04/anhoerungen/Anhoerung05/Stellungnahmen/Stellungnahme05.pdf.

[180] See http://www.bundestag.de/ausschuesse/a04/anhoerungen/Anhoerung05/Stellungnahmen/Stellungnahme07.pdf.

[181] See http://www.bundestag.de/ausschuesse/a04/anhoerungen/Anhoerung05/Stellungnahmen/Stellungnahme08.pdf.

[182] See FIDIS Deliverable D14.2 at http://www.fidis.net/resources/deliverables/privacy-and-legal-social-content/d142-study-on-privacy-in-business-processes-by-identity-management/doc/23/ for an introduction to a DPMP.

of citizens and service providers in the electronic world.'[183] Recently the German government has commissioned several analyses regarding technical and legal requirements of such a citizen portal. This initiative is called *Bürgerportale.*[184]

Security measures have been implemented in the banking sector, aimed at combating phishing activities during online banking. These include awareness measures[185] and technical measures. In online banking, many banks in addition to simple TAN / PIN or iTAN procedures, are offering eTAN, eTANplus and mTAN, HBCI[186] (homebanking computer interface) or FinTS[187] (financial transaction service) interfaces and procedures.[188]

TANs (transaction authentication numbers) were introduced for online banking services as single use passwords in addition to the permanent PIN (personal identification number) set by the customer or provided to the customer usually upon registration to the online banking service. The bank customer receives a letter with a list of usually 50 TANs, each 8 characters long. Every following transaction has to be verified with any unused TAN left on the list. The bank then verifies the TAN against the list issued to the customer.

It is common for banks to use iTANs (indexed TANs) today. This means the TANs are numbered and for every transaction made online a specific TAN is requested for verification by the bank. This method is considered to provide higher security than the ordinary TAN procedure, but it can be attacked by means of a man-in-the-middle-attack.[189] When iTANs were introduced by Deutsche Bank and Postbank in 2005 experts from Bochum University's '*Arbeitsgruppe Identitätsschutz im Internet*' were able[190] to successfully attack the method within one day. The attack involved two steps. First the customers were tempted to visit a forged website resembling the real bank website. By means of pretending that a 'security check' was required, customers were motivated to enter their bank account number and their online banking PIN. With these data the experts logged into the victim's online banking account and initiated a transaction. The iTAN requested by the bank for verification purposes was obtained from the customer still by means of the simulated 'security check'.

A further security procedure offered for online banking is eTANs (electronic TANs). Instead of TANs physically sent to the customer on a list the customer receives a TAN generator. During an online banking transaction the bank generates a check number which the customer

---

[183] Bundesamt für Sicherheit in der Informationstechnik: ‚The IT Security Situation in Germany in 2007', p. 28.

[184] See http://www.kbst.bund.de/cln_047/nn_1100856/Content/Egov/Bportale/bportale.html__nnn=true.

[185] The *Bundesverband Deutscher Banken* (Association of German banks) issued information brochures on online banking security measures. Available at http://www.bankenverband.de/index.asp?channel=161010. For example: 'Online Banking Security', available in English at http://www.bankenverband.de/pic/artikelpic/092006/06_09_Online-Security.pdf. The German Federal Office for Information Security's information: http://www.bsi-fuer-buerger.de/geld/10_04.htm.

[186] For an overview of banks offering HBCI: http://www.test.de/themen/geldanlage-banken/test/-Sicherheit-beim-Onlinebanking/1486871/1486871/1490749/1490787/.

[187] See http://www.hbci-zka.de/english/index.htm.

[188] For an overview (in German) see Arbeitsgruppe Identitätsschutz im Internet 'Online Banking' at https://www.a-i3.org/content/view/936/207/.

[189] A definition is e.g. given by Federal Deposit Insurance Corporation 'Putting an End to Account-Hijacking Identity Theft', 2004: "In a man-in-the-middle attack, a fraudster intercepts messages between the institution and the customer, learns the shared secret, and then impersonates the institution going forward. The customer is unaware of the fact that he or she is now communicating with the fraudster instead of the institution." Available at http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf.

[190] See http://www.handelsblatt.com/news/Default.aspx?_p=204016&_t=ft&_b=988167 and http://www.spiegel.de/netzwelt/tech/0,1518,384337,00.html and https://www.a-i3.org/content/view/411/28/.

enters into the TAN-generator. The device then generates an eTAN which can be used to verify the transaction. The algorithm used to generate is known only to the bank issuing the TAN-generator. An eTAN is valid only for a restricted period of time.

Further security features are implemented with the eTANplus method. The customer receives a TAN generator device into which he has to insert his debit card. Similar to the eTAN method, the bank provides a check number during the online transaction process, which the customer enters via a key pad into the TAN-generator. Generating the eTAN then takes into account information specific to the transaction requested by the customer (for example designated remittee's bank account number, and amount of the transaction) as well as a key stored on the debit card. This measure is considered more secure than the TAN/iTAN approach.

Furthermore, online banking can be conducted using HBCI-banking (Home Banking Computer Interface). HBCI is a German bank-independent protocol for electronic banking passed by the Central Credit Committee (*Zentraler Kreditausschuss* – ZKA) and in use by German banks. The customer has to install homebanking software on the computer used for online-banking and connects to the bank's HBCI server using that software and not a web browser. In addition customers need an HBCI-enabled card reader device. During an online banking transaction the customer inserts his debit card into the reader and enters the debit card PIN via the reader's key pad. The card electronically signs the transaction. HBCI has subsequently been refined and named FinTS (Financial Transaction Services). More than 2,000 banks support the FinTS specification.

A different way to receive a one-time TAN is the mTAN (mobile TAN) method. The customer requests a TAN by submitting a filled in transaction form at the online banking website. A TAN is then sent to the customer's registered mobile phone as a text message. The TAN is valid only for the ongoing transaction and the customer then has to finalize the transaction by entering the TAN.

A new approach reported by American banks is the use of biometric authentication during online banking.[191] The PARDA Federal Credit Union (23,000 customers) is using a software-based solution called BioPassword. This software analyzes the customers' individual key stroke pattern upon entering user name and password. The interval between two keystrokes (called "flight time") is measured as well as the duration of pressing a key.

4.5 Conclusion

Currently the term 'identity theft' is not mentioned in any German statute. The existing criminal and civil laws do cover acts related to as 'identity theft'. The topic and use of the term 'identity theft' is not discussed widely among German legal scholars. The concept of identity related crime is not discussed applying the focus on 'identity'. It is for these reasons that no meaningful figures with regard to numbers of identity related crime and damage caused by these acts exist. Identity related crimes are often carried out either by means of using the Internet or with regards to debit and credit card data. For some of these kinds of crimes declining figures were reported in 2006 in comparison to the numbers known for 2005. In 2007 rising figures are reported regarding offences committed by means of the Internet (8%), phishing (20%) and information and communications technology related crime were reported (17%). To which extend these cases can be mapped to the FIDIS typology is not

[191] EURO SECURITY: ‚Online-Banking mit Rhythmusgefühl', issue 8/9-2007, p. 362-364.

clear. It has to be taken into account that the key 'offence committed by means of the Internet' was added to the Criminal Statistics only in 2004 and that by 2006 still not all German states were able to use this key when reporting their figures.[192] The rising number of Internet related crimes (2005: 118,036; 2006: 150,785; 2007: 180,000) could only reflect the increased ability of states to report crimes using this key. The overall figure of phishing cases in 2007 (4,200) is surprisingly low considering the big attention phishing receives in the media. An average damage of more than 4,000 EURO per case could explain this attention.

Legal and technical countermeasures have been passed. Legal countermeasures include the amendment of the German Penal Code to incorporate requirements laid down by the cybercrime convention. Security breach notification laws are being discussed and would significantly raise the ability of victims to react quickly and possibly prevent considerable damage. Passing such a law does currently not find the necessary support of the required majority of members of parliament and a distinct agenda for progress on this matter is not available.

Technical countermeasures were developed in the online banking sector. However, measures known to be effective (like HBCI) are not used on a large scale. Instead, mainly the TAN and iTAN method is used which is known to be vulnerable to man-in-the-middle attacks.

Coming from an eGovernment approach, the German government currently explores the possibility of citizen portals ensuring binding authentication of citizens and service providers in the electronic world.

[192] See http://www.bka.de/pks/pks2006/ex_i_1.pdf.

5 United Kingdom

5.1 Concepts

Next to the United States, the United Kingdom certainly has an extensive history when it comes to identity-related crime. Within the European Union, the United Kingdom remains a territory which is often singled-out with regard to identity-related crime when general remarks are made about the state of affairs. In February 2004, the European Commission held a Forum on identity theft where the attendees noted how "Identity theft is growing fast outside the EU (US, Canada, Australia) and is very relevant in the UK. For now, it does not seem to be equally prominent in the other Member States."[193]

Within the United Kingdom, individuals, from policy makers to academics, use both identity theft and identity fraud when they discuss identity-related crime. In general, they most often use the term identity fraud. The Home Office provides various definitions for the different terms. According to the Home Office, "Identity fraud and identity theft are often used very loosely to describe any situation in which personal details are misappropriated for gain. The following definitions have been developed by the Identity Fraud Steering Committee to clarify these terms":[194]

1. **Identity Crime** is a generic term for Identity Theft, creating a False Identity or committing Identity Fraud.
2. **False Identity** is: (a) a fictitious (i.e. invented) identity; or (b) an existing (i.e. genuine) identity that has been altered to create a fictitious identity.
3. **Identity Theft** occurs when sufficient information about an identity is obtained to acilitate Identity Fraud, irrespective of whether, in the case of an individual, the victim is alive or dead.
4. **Identity Fraud** occurs when a False Identity or someone else's identity details are used to support unlawful activity, or when someone avoids obligation/liability by falsely claiming that he/she was the victim of Identity Fraud.[195]

With regard to definitions set forth in the FIDIS typology, there is a significant difference. The definitions used in the United Kingdom do not consider identity fraud as a more general term which includes, or can include, identity theft. Rather, identity theft is a prepatory action taken to commit identity fraud which certainly changes the overall debate but also the (legal) countermeasures introduced. This is primarily a result because incidents of identity-related crime are broken into two distinct parts which means actions taken to prevent or reduce the problem need to focus on both aspects of the problem. This clearly has both benefits and drawbacks. Certainly through dividing the problem into two stages, oversight of how to counter the problem is clearer because policy makers and other involved individuals can target certain actions in a more specific manner. The identity theft stage, for example, requires policymakers to institute better or more effective means of data protection with regard to both the public and the private sector and also with regard to consumers, because the identity theft stage is all about gaining the personal identifying details to actually commit fraud with the

[193] European Commission (2004), 'Minutes of the Forum on Identity Theft.' p. 2.
[194] http://www.identity-theft.org.uk/definition.html.
[195] http://www.identity-theft.org.uk/definition.html.

'stolen' identity. The actual identity fraud, on the other hand, requires different types of countermeasures because perpetrators target other vulnerabilities within the identification infrastructure which allows them to gain financial benefits at the expense of another individual.

The predominant focus within the United Kingdom remains with fraud committed with the purpose of obtaining financial benefits. The focus is mainly on the private sector but to a certain extent also on the public sector, with regard to potential for government benefit fraud. To speak in more specific terms, the focus within the United Kingdom is on both account take over and true name fraud. In an interview with Martin Gill, Professor of Criminology at Leicester University, he acknowledged how recently 'false applications' have been on the rise and as such have become an area of focus. After follow up questions, Gill clarified that he was referring to true name fraud, where perpetrators file applications, for credit cards, mortgages, etc., using both existing and false identities.[196] This development could perhaps introduce or at least increase the use of other (sub-)concepts within the discussion within the United Kingdom.

5.2 Prevalence

Data on the prevalence of identity fraud within the United Kingdom continues to grow and is significantly more comprehensible than in other European countries. The Credit Industry Fraud Avoidance System (CIFAS), for example, has records of consumer complaints about identity fraud dating back to 1999. The table below demonstrates how from 1999 until 2006 identity fraud complaints continued to rise consistently. The most recent data on 2007, however, indicate a small decline in the number of complaints filed by victims of identity fraud. Whether this decline is the beginning sign of an overall declining trend is a question which only time can answer.

Year	Cases Recorded
1999	9,000
2000	16,000
2001	24,000
2002	34,000
2003	46,000
2004	56,000
2005	66,000
2006	80,000

[196] Interview with Martin Gill in Leicester on April 21, 2008.

2007	77,500

Table 5.1. Number of Victims per year according to the Credit Industry Fraud Avoidance System (CIFAS).

In addition to the data provided and maintained by CIFAS, there is also (limited) survey data available. The Home Office published statistics on plastic card and identity fraud in 2007. These statistics are the findings of the 2005/06 British Crime Survey. The findings on identity fraud provided within the Home Office Statistical Bulletin contain results from the 'newly-introduced BCS module on this emerging new crime type.' The authors describe how "Whilst...there are inherent difficulties with obtaining good measures of crimes involving deception, the BCS can provide useful evidence on the experience of such crimes amongst the general population."[197] The BCS module is also an attempt to increase the knowledge base about identity fraud prevalence. Within the report, it is stated how due to the problems with the accuracy of police records due to lack of reporting and categorization issues (i.e. fraud as deception), "The Home Office, following discussion with the Association of Chief Police Officers and the financial sector, have decided that to reduce the level of bureaucracy involved in fraud recording, and to streamline the reporting and initial investigation of frauds, all cases of economic fraud (involving the use of plastic cards, online banking, or cheques) will be recorded by the financial institution concerned from 1 April 2007. The financial organisations will then be responsible for undertaking further verification and initial investigation, and, as appropriate, reporting cases of criminal activity directly to the police for further investigation."[198] The survey posed questions to the respondents in a number of categories including plastic card usage. With regard to usage of plastic cards, 83 per cent of all respondents used plastic cards during the previous year. Other findings demonstrate how, "[a]dults living in households in the higher income groups had the highest levels of usage and other variables associated with higher income status reflected this pattern."[199] Of all the respondents using plastic cards, four per cent became a victim of fraud during the previous year.

Jacqueline Hoare and Charlotte Wood also provide an analysis on which individuals are more likely to fall victim to identity fraud based on the demographic make up of the victimised respondents. According to the authors, men between the ages of 35 and 44 are more likely to fall victim to identity fraud than those between the ages of 16 to 24.[200] With regard to women, the lowest age category appears to be more likely to fall victim to identity fraud than their male counterparts of the same age. The survey also provides data on identity fraud through the misuse of personal information. According to the findings, two per cent of respondents fell victim to this type of identity fraud.[201]

---

[197] Home Office Statistical Bulletin (2007), 'Mobile phone theft, plastic card and identity fraud: Findings from the 2005/06 British Crime Survey', available at http://www.homeoffice.gov.uk/rds/pdfs07/hosb1007.pdf, p. 7.
[198] Home Office Statistical Bulletin (2007), p. 30.
[199] Home Office Statistical Bulletin (2007), p. 29.
[200] Home Office Statistical Bulletin (2007).
[201] *Ibid.*

Table 3.5 Proportion of adults whose personal details have been used without permission

Percentages	2005/06 BCS
Personal details *ever* used without permission	6
Credit or debit card used to make a purchase	4
Applied for and obtained a credit card	1
Obtained a loan, mortgage or credit agreement	1
Applied for state benefits	0
Applied for a mobile phone contract	0
Opened a bank or building society account	0
Registered a vehicle	0
Applied for a passport	0
Applied for driving licence	0
Personal details not *ever* used in any of these ways	94
Personal details used without permission *in the last year*	2
Credit or debit card used to make a purchase	1
Applied for and obtained a credit card	0
Obtained a loan, mortgage or credit agreement	0
Applied for state benefits	0
Applied for a mobile phone contract	0
Opened a bank or building society account	0
Registered a vehicle	0
Applied for a passport	0
Applied for driving licence	0
Personal details not used in any of these ways *in the last year*	98
Unweighted base	*11,166*

Table 5.2. Proportion of adults whose personal details have been used without permission

In addition to assessing the percentage of victims and the likelihood of someone falling victim to identity fraud based on age and gender, the BCS also questioned respondents on their fears of falling victim to identity fraud. The findings indicate how more than half (57%) of plastic card users were fairly or very worried of falling victim to card fraud. Hoare and Wood note how that is "a level that is higher than other crime types asked about in the BCS."[202] This can be observed in Figure 5.1 below.

[202] Home Office Statistical Bulletin (2007), p. 29.

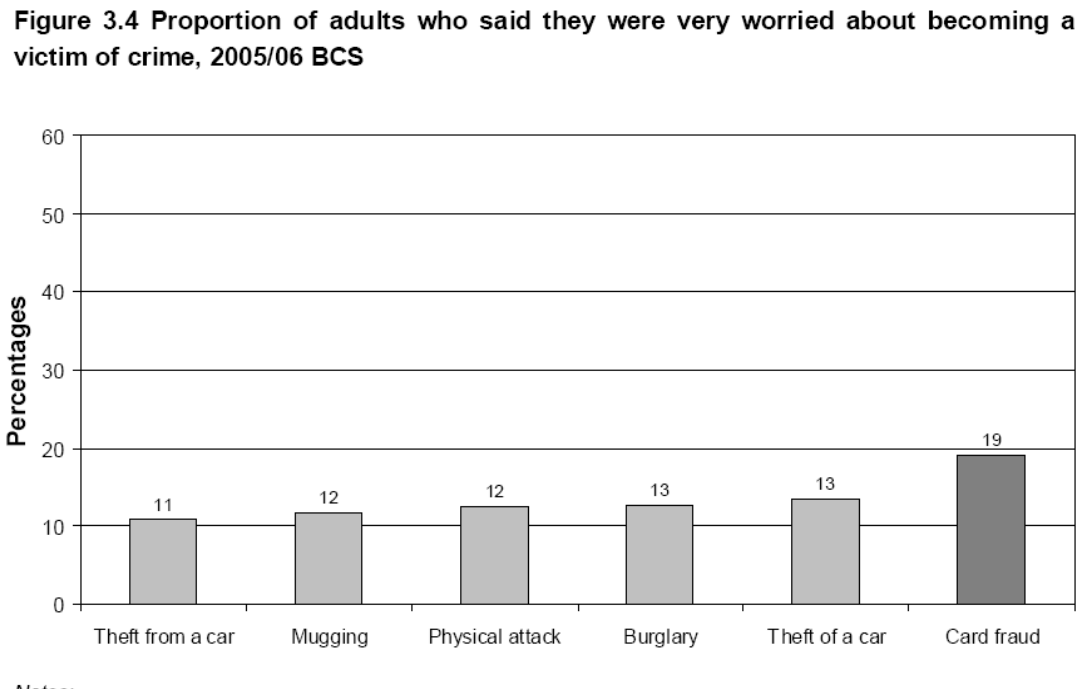


Figure 5.1. Proportion of adults who said they were very worried about becoming a victim of crime

In October 2008, results from another module will become available and will provide an opportunity to unravel any patterns with regard to identity-related crime in general and with regard to specific aspects of identity fraud. Individuals within the Home Office place a lot of confidence in the BCS. The reliability and importance of the British Crime Survey rest in the fact that it is a proper survey conducted on random samples of the population and does not start with reports of crime.

Currently, a National Fraud Reporting Centre is under construction. The funding for this Centre just came through and developments are under way. Through three different sources, the future Centre is currently running a trial. These three different sources include CIFAS, Consumer Direct and APACS. The Centre is expected to be up and running in 2009. The main aim of the Centre is to get better statistical data and improve intelligence and awareness. The Centre should also provide an opportunity to analyse trends and patterns in order to build a greater awareness of the problem.

5.3 Vulnerabilities

Within the United Kingdom, various vulnerabilities exist which facilitate the occurrence of identity fraud. With regard to identity theft, the public availability of information is a significant issue. Kevin McNulty,[203] Head of the Identity Fraud Reduction Team, acknowledged how there is a "huge availability of public data" including records of births, marriages and deaths. Furthermore, several websites exist which provide perpetrators with extensive personal details of potential victims. Staff members, especially within call centres, also have access to significant amounts of sensitive personal data including credit card numbers and ccv numbers. These employees are a major vulnerability because they can either

[203] Interview with Kevin McNulty on April 22, 2008 at the Home Office in London.

access the information voluntarily to commit dishonest acts or organized crime networks can bribe them into handing over the customer information.

Nicola Westmore[204], from the UK Ministry of Justice, described an important recent case which emphasized this data availability vulnerability in the United Kingdom. This issue related to land registry which were posted online. New legislation allowed them to put details of people's titles and properties on the internet which created a massive database of sensitive personal information. These included photocopies of mortgage deeds, including signatures. Thankfully enforcement came to take it off, due to the fact that individuals felt as though there was the potential for identity theft, because anyone had access to all information. According to Westmore, "They should have blacked out information which was personal and could have been used for other purposes. People tend to develop policies in isolation without thinking it through entirely."

In addition, the recent high-profile data losses within the United Kingdom have introduced an entirely different dimension to the availability of sensitive personal data. Interviewees all mentioned this recent issue. A prime example is the data loss which occurred in November 2007, when news broke about how the HM Revenue & Customs lost disks which contained records of 25 million child benefit recipients. These disks were lost in the mail, when they were handed to TNT by courier mail and were supposed to arrive at the National Audit Office. According to Iain Thomson, "The material was apparently put in the post by a junior employee at the HMRC office in Washington, Tyne & Wear."[205] The disks contained rather sensitive information. The following data was password protected but not encrypted: names, addresses, dates of birth, child benefit numbers, National Insurance numbers and bank or building society account details.

While this data loss receives tremendous attention from both the government and the media, it was the not the first data loss at HMRC. In October 2007, an HMRC member left a laptop in his car, which was subsequently stolen. According to Iain Thomson, "The computer contained records from finance houses revealing the identity of high value customers who had invested in Individual Savings Accounts." Ever since the media caught on to the HMRC data loss, many other organizations have come forward about data losses. The data loss also led to, perhaps expected and inevitable, new phishing attacks.

Problems within the private sector also exist. The Information Commissioner's Office describes[206] how a freelance journalist, based in Southampton, decided to check local banks in his area. He went along to several banks and a post office, looked in the bins placed outside them and found a significant number of discarded personal data (cut up debit/credit cards, torn up bank statements/insurance application forms etc). He contacted the banks, did not receive a very favourable response and as result contacted the ICO. The ICO commenced an investigation but before that was completed the journalist contacted the BBC Watchdog program. Watchdog visited several towns in the UK and their 'researchers' found similar discarded personal data in bins outside banks/building societies.

---

[204] Interview with Nicola Westmore on April 23, 2008 in at the Ministry of Justice in London.
[205] Thomson, I. (2007), 'HMRC Data Loss Leaves 25 Million Exposed', available at http://www.vnunet.com/vnunet/news/2203916/hmrc-boss-resigns-loss.
[206] Information derived from an emailed document to the author by Iain Bourne from the ICO.

About a month later, BBC Watchdog researchers repeated the operation in other towns and again got similar results. In addition, a journalist in Scotland carried out a similar operation in his local town and recovered personal data. All the documentation recovered was forwarded to the ICO and it resulted in the undertakings being obtained from the Post Office, 11 Banks and the Immigration Advisory Service. The ICO hopes that these undertakings signed by chief level executives will assist in the prevention of sensitive data being disposed of in a rather careless manner which could subsequently lead to identity theft.

Another vulnerability identified by McNulty is how individuals within the United Kingdom can rather easily change their name. A name change does not require a legal deed, which means perpetrators who want to commit an act of identity-related crime can simply change their name to correspond with whatever documentation they have managed to obtain and subsequently commit fraud.

While particular vulnerabilities exist with regard to the identity theft stage, societal factors also facilitate the actual occurrence of identity fraud. Within one research 'experiment' Gill along with a colleague tried to assess to what extent they could accomplish certain activities with a voter registration card. Within the United Kingdom, any eligible citizen has a voter registration card. This card is not a form of identification, yet Gill and colleague tried to see whether people (i.e. employees at a financial institution and the post office) would be willing to accept it as a form of identification. As they went to withdraw money, the bank employee did not even bother asking for identification and neither did the post office employee when they went to pick up a parcel. This clearly hints at potential problems with regard to verification of a client's identity. When asked about this McNulty acknowledged how certainly this is a vulnerable area within the United Kingdom.

5.4 Countermeasures

In *Identity Fraud: A Study*, published in 2002, the Cabinet Office recommends and urges for "more effective joint working, more sharing of data and intelligence and more active and effective prosecution policies."[207] As a result of the Cabinet study, the UK government heightened its initiatives to develop means to prevent and detect identity fraud. The Home Office created the Identity Fraud Steering Committee (IFSC) and the Identity Fraud Forum (IFF) in 2003, which developed a framework to identify effective measures to prevent and react to subsequent occurrences of identity fraud. More specifically, both IFSC and IFF members highlight a number of significant priorities in their work to reduce the occurrence of identity fraud. These include:

(a) identify new opportunities for data-sharing across the public and private sectors;

(b) reduce fraud involving the impersonation of deceased persons;

(c) establish the cost of identity fraud to the UK economy on an ongoing basis;

(d) researching the impact of identity fraud on victims and statistically tracking those cases;

[207] United Kingdom Cabinet Office (2002), 'Identity Fraud: A Study', United Kingdom: Cabinet Office Publications, p. 27.

(e) improve both the public awareness of identity fraud through joint working with the financial services industry and the training provided to those in the financial sector responsible for checking customers' identity.[208]

As a result of these priorities, the IFSC and the IFF managed to develop a number of regulatory instruments in their battle against identity fraud. Important measures introduced by the Government primarily include aligning penalties, defining a new criminal offense, developing and sharing good practice, and raising public awareness. The Government decided to increase the maximum punishment for fraudulently obtaining a driver's license from a maximum fine of £2,500 to a maximum two year prison sentence, which is the current punishment for fraudulently obtaining a passport.[209] Furthermore, in 2003 the Government decided to introduce a new criminal offense. Under the new criminal offense, any individual who is either in possession or in control of false identity documents, whether genuine documents illegally obtained or derived from another person, is in violation of the law and subject to criminal sanctions. The underlying motive for the introduction of a new criminal offense is the connection between use of false identity documents and organized crime; consequently, the UK government hopes to use the new offense to provide the police with additional means "to disrupt the activities of organised criminals in the early stages of their crimes."[210] The new offense is part of the Identity Cards Act, which will later be elaborated upon.

On 15 January 2007, the Fraud Act of 2006 came into force. The Fraud Act "created a new offence of fraud that can be committed in three ways: by making a false representation (dishonestly, with intent to make a gain, cause loss or risk of loss to another), by failing to disclose information, and by abuse of position. Offences were also created of obtaining services dishonestly, possessing equipment to commit frauds, and making or supplying articles for use in frauds."[211] The Fraud Act certainly criminalizes many aspects of identity theft and identity fraud which could help in the prosecution of perpetrators of identity-related crime. According to Kevin McNulty, the new legislation has proven easy to prosecute. So far, approximately 525 people have been prosecuted under the new legislation. As Anne Savirimuthu and Joseph Savirimuthu state, "the Fraud Act 2006 facilitates the prosecution of identity theft and therefore makes a valuable contribution to Internet governance."[212] The main benefit of the legislation is the change made with regard to fraud. Previously, fraud could not be conducted against a machine (i.e. a computer or an ATM). Deceiving a machine, as a result of the Fraud Act, can now be prosecuted. Savirimuthu and Savirimuthu provide concrete examples of how simply sending a phishing email provides prosecutors with grounds for prosecution. As the authors state, "There is no requirement for the phisher to be shown to have used the information to access the funds in the victim's account. The victim need not respond to the email or act on the request."[213]

---

[208] Courtney, K. (2005), 'Home Office Identity Fraud Reduction Programme', Chair's Progress Report, Identity Fraud Steering Committee, p. 1.
[209] United Kingdom Home Office (2006). 'What is Being Done About Identity Theft in the UK?', http://www.identity-theft.org.uk/what-is-being-done.htm.
[210] *Ibid.*
[211] *Ibid.*
[212] Savirimuthu, A. & Joseph Savirimuthu (2007), 'Identity Theft and Systems Theory: The Fraud Act 2006 in Perspective', *4 Script-ed* (4), p. 460.
[213] *Ibid.*, p. 440.

While Savirimuthu and Savirimuthu welcome the Fraud Act and its changes to the landscape of crime prosecution, others recognize the potential pitfalls of the Act. Maureen Johnson and Kevin M. Rogers describe how the Fraud Act has made fraud into a crime of conduct rather than a result crime. As the authors note, "The shift of the fraud offence into the realms of the conduct crime should not be underestimated. Conduct will now be caught and criminalised which would not even have sufficed for an attempted offence prior to the Act, and as a result fraud has become a very wide offence indeed."[214] Others agree and claim how the broadness of the provisions included in the Act are both a 'blessing and a curse.'[215]

Within the United Kingdom, the introduction of chip and pin is a successful initiative proposed and implemented by the private sector. Chip and pin altered the method of authentication for credit card users. Whereas previously users simply needed to sign their name during a credit card transaction, chip and pin required them to also enter a pin code. This changed the transaction from a one-factor authentication to a two-factor authentication. The two-factor authentication makes it more difficult, although hardly impossible, for perpetrators to commit account take over if they only have the credit card and do not know the accompanying pin code. This initiative helped to reduce the number of credit card related identity fraud cases within the United Kingdom. Overall, fraud, however, did not go down due to the fact that other countries failed to introduce similar measures. The benefit of this countermeasure is how it directly targets the vulnerability of verification when a client makes use of his or her credit card through introducing an additional authentication factor. According to APACS, "2007 card fraud figures...show that total card fraud losses rose by 25 per cent in the past year to £535.2m. A key driver behind this is the 77 per cent increase (up £90.5m) in fraud committed overseas by criminals using stolen UK card details – which typically occurs in those countries yet to upgrade to chip and PIN. Fraud abroad now accounts for over one third (39 per cent) of total card fraud losses."[216] Clearly, chip and pin, while effective, also led to a redistribution of fraud to other territories.

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

5.5 Conclusion

Within the United Kingdom, there is more clarity and perhaps also more concern about identity-related crime than anywhere else in the European Union. The recent data losses along with the introduction of the Fraud Act of 2006 maintain a significant focus on the issue of

---

[214] Johnson, M. & Kevin M. Rogers (2007), 'The Fraud Act 2006: The E-Crime Prosecutor's champion or the creator of a new inchoate offence?' Paper presented at the 2007 Annual Conference of the British & Irish Law, Education, and Technology Association in Hertforshire (16-17 April).

[215] Sullivan, G. R. (2003), 'Fraud – The Latest Law Commission Proposals', *67 Journal of Criminal Law* (2), p. 139-148.

[216] See http://www.apacs.org.uk/2007Fraudfiguresrelease.html.

identity fraud. Certain strong aspects within the United Kingdom, as compared to mainly the United States, do exist.

The Home Office acknowledges how the recording of incidents by the private sector is an important and reliable source. Furthermore, the private sector's prevalence data also circumvents problems encountered by police sources because many victims generally try to resolve their problem with the private institution without or before going to any law enforcement agency. As a result, data on the problem within the United Kingdom appears to be relatively reliable and well maintained. With regard to countermeasures, the recent Fraud Act certainly proved to be a step in the right direction according to some. While others fear its broad nature and the potential consequences associated with it. The interesting aspect of the Act is the manner in which it has increased the number of prosecutions of identity-related crime incidents. A rather thought-provoking question is whether the Fraud Act in the United Kingdom could actually serve as a deterrent, unlike the Identity Theft Assumption and Deterrence Act in the United States.

6 United States

6.1 Introduction

The term identity theft and the notion that this crime is one of the fastest growing crimes in recent years, stem from the United States. The intrinsic connection between identity theft and the United States continues to exist, despite the spread of the phenomenon to other regions, predominantly the European Union and Australia. The United States can look back at a decade filled with studies on and countermeasures taken against identity theft. This chapter provides an overview of identity theft in the United States with regard to the concepts used, the focus of the debate, the prevalence of the problem, vulnerabilities present in the infrastructure, and initiated countermeasures.

6.2 Concepts

Within the United States, the term identity theft is generally used to discuss identity-related crime. Unlike many, if not most, other countries the United States actually has a legal definition of identity theft. According to the Identity Theft and Assumption Deterrence Act, which Congress passed in 1998, identity theft occurs when someone "knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law."[217] The Government Accountability Office (GAO) provided a more concrete definition of identity fraud in 1998. According to GAO, identity fraud "...refers to the illegal use of personal identifying information—such as name, address, Social Security number (SSN), and date of birth—to commit financial fraud. Identity fraud can encompass a host of crimes, ranging from the unauthorized use of a credit card to a comprehensive takeover of another person's identity and financial accounts."[218] Interestingly enough is how in the early years, GAO, among others, used the term identity fraud rather than identity theft. It remains unclear what sort of influence led to the current dominant use of the term identity theft, although perhaps the focus of the debate explains the use of terminology. The main focus of the debate is on financial cases of identity theft, in particular those where perpetrators abuse the identity of an existing person rather than a false identity. Certain incidents and categories of identity-related crime do not, as a result, receive the necessary attention. Synthetic identity fraud, for example, as ID Analytics referred to it, is largely ignored. Synthetic identity fraud is identity-related crime through the misuse of a fabricated identity. Statistics on this type of identity-related crime indicate a worrisome trend which will be discussed in the section on prevalence.[219]

Other elements of identity theft which, according to certain individuals, do not receive equal attention are medical and criminal identity theft. Both can lead to awful consequences for victims. Medical identity theft is perhaps the newest type of identity theft recognized within the United States. According to Pam Dixon of the World Privacy Forum, "[m]edical identity theft occurs when someone uses a person's name and sometimes other parts of their identity –

[217] Identity Theft and Assumption Deterrence Act of 1998, Pub. L. No. 105-318, 112 Stat. 3007 (1998) (amending 18 U.S.C. § 1028).
[218] General Accounting Office (GAO) (1998), "Identity Fraud: Information on Prevalence, Cost, and Internet Impact is limited", Briefing Report to Congressional Requesters.
[219] See "'Synthetic' ID Fraud Poses New Challenge", available at http://www.insideid.com/idtheft/article.php/3482011.

such as insurance information – without the person's knowledge or consent to obtain medical services or goods, or uses the person's identity information to make false claims for medical services or goods."[220] Furthermore, medical identity theft often leads to crucial errors or fictituous information in existing medical records of victims. The World Privacy Forum convincingly claims that medical identity theft "...is the least studied and most poorly documented of the cluster of identity theft crimes."[221]

With criminal identity theft, the perpetrator commits a (serious) crime and provides a 'stolen' identity to escape prosecution. When individuals become victims of criminal identity theft they may, for example, be initially stopped for a minor traffic violation, but upon checking their records the law enforcement officer finds a warrant out of their arrest for a serious crime like murder. The identity theft victim is then wrongfully arrested and subsequently locked up in prison.

These types of identity theft largely remain in the background, as the debate continues to be about the presence and the potential elimination of financial identity theft within contemporary society. The problem with this exclusive focus on financial identity theft is to perhaps ignore patterns of vulnerabilities within the infrastructure which, when unraveled, could help to reduce all types of identity theft. All incidents of identity theft require perpetators to obtain certain 'tools' and to use them in some way. If the focus were to be broadened perhaps more facilitating factors could be discovered.

6.3 Prevalence

The United States has conducted perhaps more studies than any other country in the world. These studies have largely been conducted based on surveys.[222] Mainly consumer and victim surverys in an attempt to develop an accurate picture on the prevalence of identity theft inside of its geographical boundaries. The primary source of data is actually not a study but a complaint database which was introduced in 1999 after Congress passed the Identity Theft and Assumption Deterrence Act, which called for the Federal Trade Commission to "establish procedures to

> (1) log and acknowledge the receipt of complaints by individuals who certify that they have a reasonable belief that 1 or more of their means of identification (as defined in section 1028 of title 18, United States Code, as amended by this Act) have been assumed, stolen, or otherwise unlawfully acquired in violation of section 1028 of title 18, United States Code, as amended by this Act;
> (2) provide informational materials to individuals described in paragraph (1); and
> (3) refer complaints described in paragraph (1) to appropriate entities, which may include referral to—
> (A) the 3 major national consumer reporting agencies; and
> (B) appropriate law enforcement agencies for potential law enforcement action."[223]

As a result, the Federal Trade Commission has maintained the Identity Theft Data Clearinghouse for the past decade. As the GAO notes, "[f]or the 23-month period from its establishment in November 1999 through September 2001, the FTC Identity Theft Data

[220] Dixon, P. (2006), 'Medical Identity Theft: The Information Crime that Can Kill You', *The World Privacy Forum*, p. 5.
[221] Dixon (2006), p. 5.
[222] For an overview, see http://www.privacyrights.org/ar/idtheftsurveys.htm.
[223] Identity Theft and Assumption Deterrence Act of 1998, Pub. L. No. 105-318, 112 Stat. 3007 (1998) (amending 18 U.S.C. § 1028).

Clearinghouse received 94,100 complaints from victims, including complaint data contributed by SSA/OIG."[224]

In 2005, the database received 255,627 complaints, which was an increase from previous years. A year later, however, a decline occurred and the database received 246,124 complaints which led some to conclude identity theft in general was starting to decrease. The most recents results from 2007 indicate how this decline may have been a coincidence rather than a definite trend. In 2007, 258, 427 complaints about identity theft arrived at the desk of the database. Overall, it would be safe to conclude that identity theft is still rising, but not at a high pace. The interesting aspect of the complaints, however, is how the percentage of identity theft complaints in comparison to other fraud complaints received by the database is continuously decreasing. Other fraud related incidents as a result demonstrate a more disturbing growth.

In addition to the complaint database which appears to provide only a fraction of the total size of the problem, survey studies are also used as a source of data. The Privacy Rights Clearinghouse has developed an overview of some studies conducted to gain a picture of the prevalence of identity theft in the United States. The results from the Javelin Strategy & Research Survey demonstrates a hopeful decline. The study conducted various times throughout the past decade uses surveys among consumers to investigate the prevalence of the crime in the United States. The number of victims in 2003, the first year the study was conducted, was 10.1 million. Later studies conducted in 2005, 2006 and 2007 began to demonstrate a steady and significant decrease. In the table below, the year and the amount of victims are presented.

Year	**Victims**
2003	10.1 million
2005	9.3 million
2006	8.9 million
2007	8.4 million

Table 6.1. Number of victims of identity theft[225]

The survey studies conducted by Javelin Strategy receive a lot of criticism, for various reasons. Chris Jay Hoofnagle, for example, criticizes this source of data because of its heavy if not exclusive reliance on consumers. He states that "we are asking the wrong people about the crime. The surveys seek to obtain information about identity theft from its victims — individuals who have the most limited view of the problem. Victims often do not know how their personal data were stolen or who stole the information."[226] Hoofnagle therefore proposes a solution to the problems associated with obtaining reliable and insightful data. He suggests financial institutions ought to publicize the prevalence data they maintain on identity theft in order to help create an accurate picture of the size of the identity theft problem. The data

[224] Government Accountability Office (2002), "Identity Theft: Prevalence and Cost appear to be growing", Report to the Congressional Requesters.

[225] Data gathered from the overview provided by the Privacy Rights Clearinghouse available at http://www.privacyrights.org/ar/idtheftsurveys.htm

[226] Hoofnagle, C.J. (2007), "Identity Theft: Making the Known Unknowns Known", *21 Harvard Journal of Law & Technology* (1), p. 99.

provided by financial institutions could subsequently be a significant aid in the determination of the actual size of the problem. However, until, if ever, that happens the available data is the only source of information anyone can use, which is precisely what Hoofnagle did. This does make any definite remarks difficult, if not impossible, partially because the available data or perhaps the interpretations given to the available data by individuals is conflicting.

Hoofnagle himself decided to go beyond previous research to gain insight into the differences between companies and the likelihood of their clients falling victim to identity theft. He notes how there has been no previous research into the relative rate of incidents of identity theft among various financial service providers. Hoofnagle acknowledges that "[t]his is a first attempt—a work in process—to meaningfully compare institutions on their performance in avoiding identity theft."[227] His preliminary results provide a list of 25 institutions within the financial service provider and the telecommunications sector. The Bank of America tops the list with the highest number of complaints and is followed by two telecommunication carriers, AT&T and Sprint/Nextel. Figure 6.1 indicates the full results.

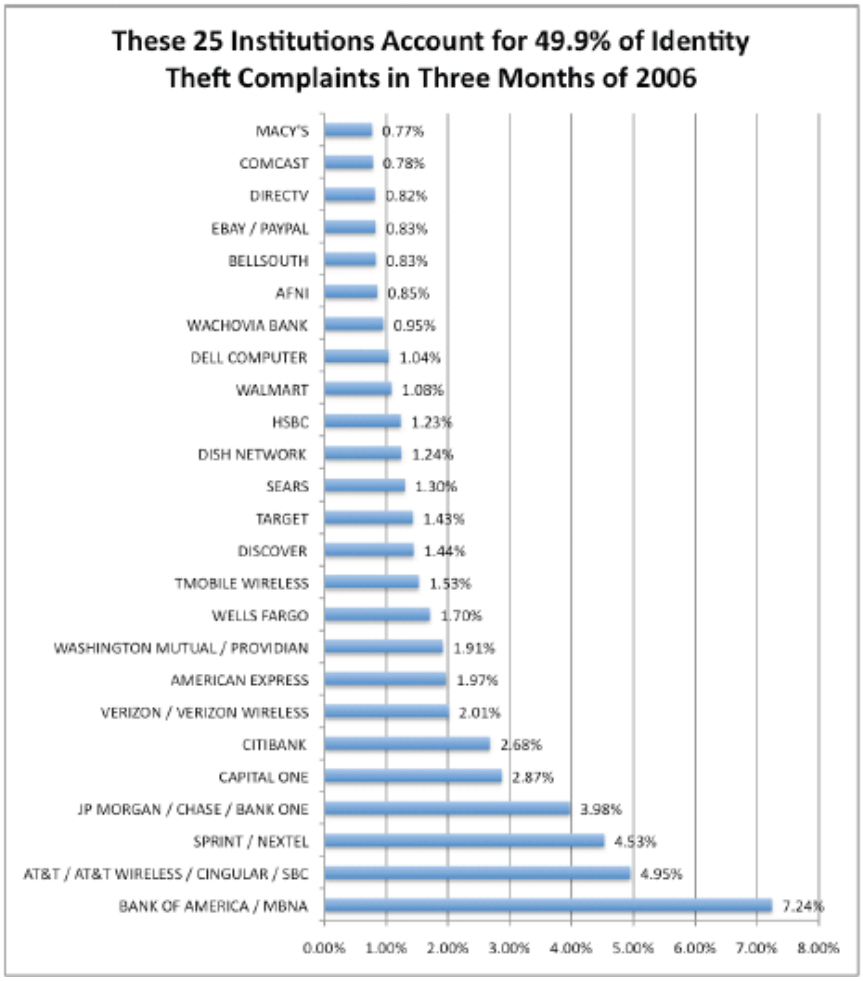


Figure 6.1. Identity theft complaints per institution (2006)[228]

[227] Hoofnagle, C. J. (2008), "Measuring Identity Theft at Top Banks (Version 1.0)", Berkeley Center for Law and Technology, available at http://repositories.cdlib.org/cgi/viewcontent.cgi?article=1045&context=bclt.

[228] Hoofnagle, C. J. (2008). "Measuring Identity Theft at Top Banks (Version 1.0)." *Berkeley Center for Law and Technology*. Available at http://repositories.cdlib.org/cgi/viewcontent.cgi?article=1045&context=bclt

The GAO also conducted studies to provide a comprehensive overview about the prevalence and cost of identity theft. In 2002, GAO reported on the costs of identity theft within the private sector. The GAO obtained data from MasterCard and Visa. These two associations considered identity theft to be made up of two categories including account take over and fraudulent applications. GAO notes how "the associations' aggregated identity theft-related losses from domestic (U.S. operations) rose from $79.9 million in 1996 to $114.3 million in 2000, an increase of about 43 percent. The associations' definitions of identity theft-related fraud are relatively narrow, in the view of law enforcement, which considers identity theft as encompassing virtually all categories of payment card fraud. Under this broader definition, the associations' total fraud losses from domestic operations rose from about $700 million in 1996 to about $1.0 billion in 2000, an increase of about 45 percent."[229]

With regard to the previously introduced issue of synthetic identity fraud, relatively little is known. ID Analytics conducted a study in 2005, which provided a rather troublesome result. According to the study, "[s]ynthetic identities are more commonly used to commit identity fraud than true-name identities. Overall, synthetic identity fraud comprises 88.3 percent of all identity fraud events and 73.8 percent of the total dollars lost by U.S. businesses."[230] The important thing to note, however, is how fabricated identities do partially rely on genuine personal data. As the study by ID Analytics shows, "[f]raudsters using synthetic identities to further their crimes typically employ the systematic manipulation of real Social Security numbers and create multiple variations of similar names across the numerous identities."[231]

Besides studies on the prevalence of identity theft, certain researchers also try to assess whether demographic characteristics influence potential victimization. In general, identity theft is a crime which can occur to anyone. Regardless of the fact that identity theft is indiscriminate with regard to its victims, certain citizens appear to be more prone to fall victim to the crime. Keith B. Anderson conducted a study to analyze whether certain citizens are indeed more likely to become victims of identity theft. While Anderson initially acknowledges how "[o]ne does not do something to become a victim – it just happens to you."[232] He also describes how "...a little deeper reflection suggests that this is really not the case. The risks faced by consumers do differ, and these differences may manifest themselves in differences across groups with different demographic characteristics."[233] Without trying to blame the victim, Anderson identifies a number of factors which may increase the likelihood of identity theft victimization for certain consumers. Anderson predicts that factors such as having a good credit record, engaging in more transactions, and having a higher income level may make a consumer more likely to fall victim to identity theft. Furthermore, Anderson also identifies the potential correlation between falling victim to identity theft and the place where a consumer does business and the victim's household composition.[234] Important to note, however, is how all consumers need to take the necessary precautionary measures in an

---

[229] Government Accountability Office (2002). "Identity Theft: Prevalence and Cost appear to be growing." Report to the Congressional Requesters.

[230] See "'Synthetic' ID Fraud Poses New Challenge", available at http://www.insideid.com/idtheft/article.php/3482011.

[231] *Ibid.*

[232] Anderson, K. B. (2005), 'Identity Theft: Does the Risk Vary With Demographics?', *Federal Trade Commission, Bureau of Economics* Working Paper No. 279, available at http://www.ftc.gov/be/workpapers/wp279.pdf, p. 11.

[233] *Ibid.*

[234] *Ibid.*

attempt to prevent identity theft, but that some may indeed be more likely to fall victim, even if they take measures to protect themselves. Anderson concludes in his study how, "[t]he likelihood that a person will be a victim of identity theft does appear to be related to demographics."[235] He identifies the following relevant demographic characteristics in particular: level of income, education, gender, age and household composition. According to Anderson, "[c]onsumers with higher levels of income are more likely to be victims of ID theft...Similarly, those with more education may be somewhat more likely to be victims."[236] Anderson's results furthermore indicate how the elderly run a lower risk to become victims of identity theft, but that households with only one adult are more likely to be victimized. Just as women appear to be more likely to fall victim to the crime than men. As Anderson rightfully notes in the end, however, "Socio-Demographic Characteristics do matter. However, no one is immune from the risk of ID theft."[237]

6.4 Vulnerabilities in the infrastructure

With regard to identity theft, the United States continues to dominate the debate through its extensive experience with the crime. Particular vulnerabilities within its infrastructure certainly provide perpetrators with sufficient tools and ammunition to continue committing the crime. While certain vulnerabilities clearly rest within the domain of one of the relevant parties, businesses, government agencies or consumers, others are a result of multiple parties.

6.4.1 Public Sector: Social Security Number

The main vulnerability within the infrastructure is the use and availability of the Social Security Number in the United States. The Social Security Number is used as the main identifier for individuals, both citizens and permanent residents, within the United States. The number, which originally was only supposed to be used for Social Security purposes, has been used in various sectors as a result of historical expansion. The main problem currently is the high level of usage and availability of the number. When individuals present the number at either a public or a private sector institution, the institution accepts this number as a means of identification which is clearly a weakness because the number is so publicly available that anyone can have access to it. So the combination of high value and easy access creates significant problems within the United States when it comes to identity theft through the illegitimate use of someone's Social Security Number. As Linnhoff and Langenderfer recognize, "[a]rmed with an SSN, a would-be identity thief needs very little additional information to effectively steal an individual's identity and wreak havoc."[238]

6.4.2 Private Sector: Verification

In addition to weaknesses or vulnerabilities which are result of government introduced initiatives, the private sector also indirectly facilitates the occurence of identity theft. With regard to financial service providers, for example, significant problems have occured. Mainly verification is a large issue, especially when it comes to new applications for credit cards or loans. As Frank W. Abagnale notes, "[i]n today's hotly competitive financial marketplace, speed is of the essence. Thieves love fast credit approval, because haste is the enemy of

[235] *Ibid.*, p. 23.
[236] *Ibid.*
[237] *Ibid.*, p. 24.
[238] Linnhoff, S. & Jeff Langenderfer (2005), 'The Emergence of Biometrics and Its Effect on Consumers', *39 Journal of Consumer Affairs* (2), p. 208.

accuracy. Credit card issuers, for their part, can be very sloppy in doling out cards, failing to match Social Security numbers and dates of birth and otherwise failing to take basic precautions in their eagerness to get cards in circulation."[239] Abagnale, among others, recognizes how many credit card companies claim their screening process is 'tight' and bullet proof, but that certain (media) stories have proven quite the opposite.

One of the more famous stories to prove the rather inaccurate verification mechanisms of credit card companies is the story of Clifford, a dog who managed to apply for a credit card. Clifford's owner, Steve Borba, opened up an email account using his dog's name. As time passed, he received a pre-approved credit card application in his email inbox. For Clifford's social security number, Borba used 9 zeros and he explicitly wrote on the application that Clifford was indeed a dog. Despite this comment and the seemingly impossible social security number, Clifford received his credit card three weeks later.[240]

Financial service providers carry a tremendous responsibility with regard to the prevention of identity theft, because they ultimately form the most crucial link between the perpetrators, the financial benefits, and the victims. Through inadequate verification mechanisms and aggressive marketing methods, they certainly help perpetrators along. Convenient yet highly insecure methods of online banking and credit card account checking also provide an opening for perpetrators. As Howard cleverly remarks, "[i]f financial institutions took reasonable precautions, they could curtail some of the identity fraud that occurs in the opening of bank accounts and the extension of credit. However, financial institutions currently lack incentives to adequately check an individual's identity before opening a bank account or extending credit. In a competitive market, these institutions fear that a more rigorous screening process might scare consumers away to competitors who do not take such measures."[241] An important point to make here is how the ways financial service providers use to verify the identity of a prospective client can either contribute to or prevent the occurrence of identity theft. Through effective verification, where financial service providers manage to distinguish perpetrators from legitimate clients, they can still prevent an act of identity theft, despite the fact that the perpetrator may already have the necessary personal information to commit such an act. The vulnerability in the online services area, on the other hand, poses a potential and significant threat for account take over, as a result of successful phishing operations and spy ware installations which begin as a consumer vulnerability but lead into a business vulnerability when perpetrators use personal information to drain accounts.

6.5 Countermeasures

One of the first actions taken against identity theft within the United States was to criminalize it. In 1996, the State of Arizona became the first government to initiate legislative action against identity theft through passing a law which made identity theft a felony and punishable with a prison sentence of up to one and a half year in addition to restitution and a fine of up to

[239] Frank W. Abagnale (2007), *Stealing your life: The ultimate identity theft prevention plan*, New York: Broadway, 2007.
[240] 'Dog Issued Credit Card: Owner Sends in Pre-approved Application as a Joke', http://www.nbcsandiego.com/money/2800173/detail.html.
[241] Howard, H. M. (2005). 'The Negligent Enablement of Imposter Fraud: A Common Sense Law Claim.' Duke Law Journal, Vol. 54, p. 1263.

$150,000.[242] After California followed Arizona's lead, the federal government introduced its first initiative. The 1998 Federal Identity Theft and Assumption Deterrence Act identified identity theft as a federal crime, provided a legal definition, and outlined penalties for any violation of the Act. To many the Act represented an important first step with regard to the fight against identity theft. Matejkovic & Lahey claim the Act accomplished a number of significant tasks. Among them are the classification of individuals as primary victims as opposed to financial institutions, and the federalization of the crime, which gives victims the opportunity to request aid from law enforcement officials.[243]

In 2004, the US Congress increased the potential punishments for convicted identity thieves. The Identity Theft Penalty Enhancement Act adds a two year prison sentence to any individual convicted of using a stolen credit card number or other personal information to commit a crime.[244] Furthermore, the Act also directs the US Sentencing Commission to think about enhancing the penalties for employees who illegaly obtain personal data from their company's database. When he signed the bill into law, President George W. Bush remarked how the Act would "dramatically strengthen the fight against identity theft and fraud. Prosecutors across the country report that sentences for these crimes do not reflect the damage done to the victim. Too often, those convicted have been sentenced to little or no time in prison. This changes today."[245] Whether enhancing penalties for identity theft violations is a step in the right direction is arguable. According to Betsey Broder, Assistant Director for the Federal Trade Commission's Division of Planning and Information, the Act will make it more likely for an identity thief to be prosecuted because "A prosecutor is less likely to bring a case if they're not going to get any serious jail time when the [sic] get a conviction."[246] The Act, therefore, is not a means to solve the problem but rather to increase the incentive for both prosecutors and law enforcement personnel to take a greater effort to convict and catch identity thieves. Additionally, one of the primary motives behind increasing the penalties is the fight against terrorism. As Dennis M. Lormel, Chief Terrorist Financial Review Group FBI, noted in his Congressional Testimony, "Terrorists and terrorist groups require funding to perpetrate their terrorist agendas (...) There is virtually no financing method that has not at some level been exploited by these groups. Identity theft is a key catalyst fuelling many of these methods."[247] Consequently, the ultimate drive behind the Act may be a good indication for its implementation. Prosecutors may be more inclined to make a greater effort to prosecute identity thieves but only if, or primarily if, they have some sort of terrorist connection. Therefore, if identity theft is committed as a stand alone crime penalties remain the same. An

---

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

[243] Matejkovic, J.E. & Karen Eilers Lahey (2001). 'Identity Theft: No Help for Consumers', *10 Financial Services Review*, p. 221-235.

[244] Identity Theft Penalty Enhancement Act of 2004, Pub. L. No. 108-275, 118 Stat. 831 (2004).

[245] Quoted in Olson, R.K. *et al.* (2005). 'Identity Theft: A Personal Risk Management Approach', *Chartered Property Casualty Underwriters (CPCU) eJournal*, p. 15.

[246] Quoted in McGuire, D. (2004). 'Bush Signs Identity Theft Bill.' *Washington Post Online* July 15, 2004.

[247] Lormel, D. M. (2002), 'Congressional Testimony', Hearing on Senate Bill 2541 "Identity Theft Penalty Enhancement Act" Before the Senate Judiciary Committee Subcommittee on Technology, Terrorism and Government Information, p. 1.

additional drawback is the fact that the Act applies "only to U.S. Postal Service and interstate acts of identity theft. For acts of intrastate identity theft, many states still do not classify this action as a felony and the criminal is given a lenient sentence."[248] The effectiveness of higher sentences, however, primarily relies on the conviction rate which appears to be relatively low. As a result, policy makers perhaps should focus more on prevention of identity theft through increased security instead of deterrence through higher sentencing.

In the years following the Identity Theft Assumption and Deterrence Act, Congress shifted its focus and began to draft legislation of a more preventative nature through increasing organizational responsibility. The shift began in 1999 with the introduction of the Gramm-Leach-Bliley Act[249] which became an essential piece of legislation through its provisions on the mandatory protection of consumers' personal financial information by financial institutions. More recently, California initiated legislation which requires private corporations to notify consumers in case of a data security breach. In 2003, California became the first state to pass two significant data security breach laws. First, the California Security Breach Information Act[250] requires any company which stores customer data electronically to notify its California customers of a security breach to the company's computer system when the company knows or has reason to believe that unencrypted information about customers has been disclosed. The second law, commonly known as the California Financial Information Privacy Act,[251] establishes new limits on the ability of financial institutions to share nonpublic personal information about their customers with affiliates and third parties. The legislation hardly comes as a surprise after hackers gained access to the state government's payroll database, which contained sensitive personal information of over 250,000 state employees, in 2002. The members of the California legislature were among the employees whose personal information was exposed through the data security breach. Benjamin Wright describes the onset for the current laws when he writes, "Many employees, including the legislators, felt the California government was too slow to notify them about the burglary."[252] Data security breach notification legislation is also an important debate at the federal level, especially after some particularly high profile cases involving major data security breaches. In the most highly publicized case, Choicepoint, a company which obtains and sells personal information, including names, Social Security Numbers (SSNs), birth dates, employment information, and credit histories to more than 50,000 businesses, settled a case after the FTC pressed charges as a result of a significant data security breach in 2005. The data security breach caused at least 800 cases of identity theft and personal financial records of approximately 163,000 consumers became available for identity thieves to take advantage of. The FTC pressed charges against Choicepoint claiming it "did not have reasonable procedures to screen prospective subscribers, and turned over consumers' sensitive personal information to subscribers whose applications raised obvious 'red flags.'"[253] Furthermore, the FTC also claimed Choicepoint was in violation of FTC provisions because the company made false and misleading statements about the privacy of consumer information. Choicepoint, ultimately, had to pay a

[248] Olson *et al.* 2005, p. 16.
[249] 15 United States Code, Subchapter I, Sec. 6801-6809 Disclosure of Nonpublic Personal Information.
[250] California Civil Code § 1798.82.
[251] California Civil Code § 1798.29.
[252] Wright, B. (2004). 'Internet Break-ins: New Legal Liability', *20 Computer Law & Security Report* (3), p. 171.
[253] Federal Trade Commission 2006, p. 1.

total of $15 million, of which two thirds for civil penalties and the other third for consumer redress. The settlement became the largest to date.

Choicepoint, among other cases, has led to an onset of a significant number of breach notification acts at the state level. At present, 42 states have some form of breach notification law in place, which differ slightly based on applicable parties, type of data 'lost' and type of notification required. The differences, however subtle, do cause or could cause confusion among the various organizations and as such perhaps federal legislation is a need which has yet to be attended to due to the controversial nature of the idea itself.

In her conclusion, Lilia Rode writes "Security breach notification statutes like California's ensure that consumers are protected from identity thieves." While perhaps in the long run security breach notification manages to provide sufficient protection, with regard to its short-term results she is incorrect. Security breach notification's strongest asset is the way in which it forces corporations to provide the highest form of security for the customer's personal data, so in and of itself breach notification laws do not protect the consumer. Furthermore, notifying consumers that their information has been compromised helps them to become more aware and cautious of potential irregularities but perpetrators can still commit identity theft with the information they obtained through the data security breach. Consequently, data security breach notification is valuable due to its ability to influence the incentives of corporations to provide better security but as a countermeasure alone it fails to provide complete protection for consumers.

Additionally, in 2003, Congress passed, and the President signed into law, the Fair and Accurate Credit Transactions Act (FACTA).[254] FACTA is another initiative which increases organizational responsibility. FACTA provides a number of provisions to fight identity theft, among these are "compulsory credit card number truncation on receipts, mandates to card issuers to investigate change of address and new card requests, fraud alert requirements by credit reporting agencies, mandatory blocking of identity theft-related information on credit reports, and free annual credit reports."[255] The Act, therefore, serves a number of purposes. First, the truncation of credit numbers on receipts is an effort to prevent identity theft from occurring. Second, the mandate to investigate requests for new cards and address changes tries to aid in the detection of identity theft attempts. Third, placing a fraud alert on someone's credit card is an instrument to stop repeat identity theft.[256] Fourth, the mandatory blocking of identity-theft related information is a means for the victim to return to his or her original credit rating and therefore reduce the devastating damage of the crime. The annual credit reports are certainly a valid tool for individuals to discover any irregularity within their credit

---

[254] Fair and Accurate Credit Transactions Act 2003, Public Law 108-159.

[255] Linnhoff, S. & Jeff Langenderfer (2005), 'The Emergence of Biometrics and Its Effect on Consumers', *39 Journal of Consumer Affairs* (2), p. 205.

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

history as a result of identity theft.[257] Especially, with the relatively short statute of limitations, the annual credit reports can help citizens to actually have a legitimate claim in court in case they fall victim to an identity thief. As to the effectiveness of these measures, some appear skeptic. The ITRC indicates on its website how a fraud alert on a credit report is not necessarily a guarantee a company or financial institution is not going to extend credit to the perpetrator, because they can simply ignore the alert.[258] A more effective means to prevent any further acts of identity theft is the credit freeze which a number of states introduced. The credit freeze allows residents to prevent anyone from viewing their credit reports and opening up a new line of credit. Even individuals who have never been victims of identity theft can request credit agencies to place a credit freeze on their account for a fee. In California, for example, residents pay $10 to each Credit Reporting Agency (CRAs)[259] (three in total) to freeze their credit. Due to the fact that the credit freeze is an initiative taken at the state level by only a restricted number of states, not everyone in the US can take advantage of this option. The inability of some victims to take advantage of the credit freeze provides a significant strain on their opportunity to prevent identity theft from occurring or reoccurring.

Another significant element of FACTA was the request made by Congress to the Department of Treasury to undertake a study on "the use of biometrics and other similar technologies to reduce the incidence and costs to society of identity theft by providing convincing evidence of who actually performed a given financial transaction."[260] The Department of Treasury concluded in its study how biometric technology is not a 'silver bullet' to reduce identity theft and "Biometrics are not likely in the near term to be very useful to confirm the true identity of an individual at the initial point of opening an account or submitting an application to a financial institution if the person has no prior relationship with the institutions."[261] Additionally, the Department notes the major obstacles which make biometrics at this point in time a sub-optimal solution. These obstacles include consumer concerns, costs, lack of accuracy and reliability of technology, and the absence of interoperability of biometric systems.

Legislative action continues to expand with regard to identity theft. Predominantly at the state level, various bills are introduced on a yearly basis. As noted by the National Conference of State Legislatures, "[i]n the 2007 legislative session, states continue to strengthen laws to protect consumers from identity theft. From increasing penalties to expanding the definition of identity theft and law enforcement role in investigating cases, states enacted several bills to help fight identity theft. States went further to assist identity theft victims after the

---

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

[258] Identity Theft Resource Center (2005). 'Victim Resources: Victim Guide.' The ITRC specifically notes how "there is no law that requires issuers to honor this request. We find that it works about 50-70% of the time."

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

[260] Quoted in United States Department of Treasury (2005). 'The Use of Technology to Combat Identity Theft.' Report on the Study Conducted Pursuant to Section 157 of the Fair and Accurate Credit Transactions Act of 2003', p. 69.

[261] *Ibid.*, p. 70.

victimization, by enacting laws that prohibit discrimination against an identity theft victim, allow expungement of the records related to the underlying theft and created Identity Theft Passport programs to help victims in clearing their name and financial records."[262]

6.6 Conclusion

Identity theft is clearly a contested issue within the United States. By some considered a big problem whereas by others merely an exaggerated media item. A large majority of policy makers, consumer advocates, law enforcement agents and even business officials understand how identity theft generally causes both individual victims and society in general a lot of damage. Whether the problem is increasing or decreasing is, however, murky and contested territory. Despite all of its experience, the United States remains in search of both an accurate picture of the prevalence of identity theft as well as a system of countermeasures which can be effective enough to reduce the problem.

[262] See http://www.ncsl.org/programs/lis/privacy/idt-legis.htm.

7 Conclusion

In the United States, the debate about identity theft took on such proportions in the past decade that it came close to a hype. Although there was, and is, sufficient empirical evidence that financial identity theft in particular is indeed a problem in the US, media reports and movies, as well as many research reports and articles outdid each other in calling it the fastest growing crime or the biggest crime of the information age. Such epithets were, and are still, hard to underpin with data about real-life occurrences of identity crime, not the least because of conflicting assessments of available data. Slowly but surely, and true to the nature of a hype cycle,[263] the US debate seems to get back to more realistic proportions.

In the wake of US reports, hyperboles for identity theft like 'the fastest growing crime' also start showing up in Europe, and reports and articles about identity crimes are mushrooming. The debate is not at a 'peak of inflated fears', to paraphrase the hype cycle: with relatively low-key attention in the general mass media or in discussions in the pub, it is not a big hype in Europe – yet. Nevertheless, the attention to identity theft is growing fast. Is this warranted by reality, and is it becoming a true problem in Europe as well as in the United States?

This report has tried to sketch a picture of the actual European prevalence of identity crimes, in order to help put our concerns over identity-related crime, in particular identity theft, in perspective. The result is, unfortunately, only a piecemeal picture: studies appear scarce, and most authors of the country chapters point out how the lack of a separate criminal provision makes it more complicated to gather information on the problem, since crimes are not being specifically reported or registered as identity-related crime.

Alongside the lack of specific provisions in criminal law, terminology and concepts are far from clear in most countries. The terms 'identity theft' and 'identity fraud' are often used, but with potentially differing interpretations. The FIDIS network has tried to develop a clear and consistent typology and terminology of identity-related crime,[264] but this is as yet one of many definitional studies that have not yet yielded an authoritative, generally accepted definition.[265] In fact, uncertainty and unclarity are dominating themes in many discussions with regard to identity theft. The unclarity about definitions and about the actual prevalence of identity theft prevent many officials within both the public and the private sector, or so they claim, to take action.

Nevertheless, the contours of our picture of the European prevalence of identity-related crime shimmer through the available data and reports. Document fraud is an on-going concern, with tens of thousands of cases yearly in countries like Belgium and France. The traditional forms of document forgery have, perhaps because of better security features in documents, been supplemented more recently with look-alike fraud, which is a major concern in several countries.

---

[263] See http://en.wikipedia.org/wiki/Hype_cycle.

[264] Leenes, R. (ed.) (2006), *D5.2b: ID-related Crime: Towards a Common Ground for Interdisciplinary Research*, FIDIS deliverable, available at http://www.fidis.net/; Koops, Bert-Jaap, Ronald Leenes, Martin Meints, Nicole van der Meulen & David-Olivier Jaquet-Chiffelle (2008), 'A Typology of Identity-related Crime: Conceptual, Technical, and Legal Issues', *Information, Communication & Society* (forthcoming).

[265] For an interesting other attempt, based on a wide, worldwide overview of definitions, see (in Dutch, with English summary) De Vries et al. 2007. They define identity fraud as 'obtaining, taking, possessing or creating false means of identification intentionally (and) (unlawfully or without permission) and to commit with them unlawful behaviour, or: to have the intention to commit unlawful behaviour.'

However, in the past few years, a shift is occurring – at least in policy debates if not also in practice – from document and look-alike fraud to online forms of fraud, in particular financial identity fraud or identity theft. In Belgium, for example, Nigerian scams and phishing, although yet limited in numbers, are mushrooming, and Germany appears to be the major host in Europe of phishing websites. Moreover, phishing – which traditionally relies on luring ICT users by deceptive email messages to false websites – seems to be increasingly replaced by covert forms of fraud, in particular by botnets that assemble identity and personal data from infected computers. In Germany, Trojan-infected computers already seem to account for 90% of phishing attacks.

Altogether, identity-related crime, particularly document forgery and look-alike fraud as well as computer-related financial identity theft, are significant forms of crime that, particularly for the latter, are on the rise. There is insufficient empirical evidence to call it a big problem yet, but the upward trend that is perceptible warrant taking expeditious measures to prevent it becoming a big problem in the first place.

Like the US, European countries are indeed taking countermeasures to combat identity-related crimes. This part of the picture is fairly clear, and it is largely similar for the European countries studied in this report.

Rather surprisingly in view of regulatory traditions, in Europe, legal measures are much less prominent than in the United States. Criminal law has not been adapted to accommodate identity crimes specifically; existing provisions – both traditional ones like theft, fraud, and forgery, and newer ones relating to cybercrimes – are considered an adequate basis to prosecute identity-related crimes. Only in very few cases, when no fraud or damage has occurred, does an identity-related crime not seem to be punishable. The main exception is the United Kingdom, which introduced its notable Fraud Act of 2006. The Act does not literally mention or introduce identity theft or identity fraud as a separate crime category, but it does introduce provisions which are extremely applicable to incidents of identity-related crime. Furthermore, at the European level, the European Commission has been discussing the potential for an overarching criminal provision identifying identity theft as a separate crime for quite some time. Whether such a provision will actually be introduced at the European level remains unclear and rather speculative.

Apart from criminal law, other areas of law may also serve to prevent or address identity crimes, such as data-protection law where data controllers can sometimes be held liable for data breaches, and tort on the basis of abusing someone's name. The European Union is perhaps also following the American lead with regard to this type of countermeasures. On a more national level, the United Kingdom is certainly considering similar provisions as a result of several data losses within both the public and the private sector.

What is more, the US have taken other legislative measures, including the Gramm-Leach-Bliley Act that imposes security measures, laws such as FACTA, which increase organizational responsibility, and security breach notification laws. These seem rather specific for the US situation. Security measures for personal data, since the Data Protection Directive of 1995, have been imposed in Europe generally, unrelated to identity crimes, on data processors. The FACTA type of measures, like free credit reports, seem particularly relevant in the US context, where credit cards are very easy to get and where credit reports are vital for people's long-term financial abilities; in the European market, such measures may not be necessary. However, the mandatory truncation of credit card numbers on receipts, included in

FACTA, has also been recommended in France and may be a valuable measure in Europe as well.

Compulsory security breach notification has only very recently become an issue in Europe. Such a system requires organizations to provide their customers with notification whenever they have lost personal information. In Germany, a Bill to that effect has been proposed in parliament, although it is unlikely to be adopted. In a thorough information security study from economic and empirical perspectives, 'a comprehensive security-breach notification law' was recommended for Europe.[266] Peter Hustinx, European Data Protection Supervisor, wants such legislation to go beyond telecoms and ISPs. As he states, "providers of public electronic communication services in public networks but also to other actors, especially to providers of information society services which process sensitive personal data (e.g. online banks and insurers, on-line providers on health services, etc.)."[267] The strong support for a breach notification is quite similar to the arguments offered by advocates in the US. Breach notification provisions, according to the advocates, hold organizations accountable and also 'force' them to implement better security standards which subsequently will provide better protection for personal information and will also prevent breaches from occurring. Whether the legislation will actually work like this in practice remains a question which only time can answer. A danger, however, remains that individuals become immune to the notifications and as such to do not place any value on the incident itself, which means the need for organizations to alter their ways becomes less apparent.

Despite the US-specificity of the legal measures discussed, the picture emerging from our survey suggests that measures like those imposed in the US by legislation, are often taken by the financial sector itself, or by public-private partnerships, in Europe; a notable exception is the United Kingdom, even though the private sector is rather active in that territory as well. Financial institutions are acutely aware of the threat of identity theft, also in view of the reliability of the entire financial system, and hence they take the lead in enhanced technical and organizational security measures. Unlike in the US, these do not necessarily have to be backed up by legislation. A wide panorama of measures is visible, consisting of awareness raising campaigns and organizational measures like consultation platforms and complaint centers, as well as technical measures such as enhanced information security standards and innovative techniques like virtual dynamic cards (in France), homebanking computer interface (HBCI) and its follower FinTS, and enhanced transaction authentication numbers, eTAN and TANplus (in Germany). Some potential solutions, however, like the 3D secure system, are opposed in France by merchants and banks for economic reasons, suggesting that market failure – one of the reasons for the US to impose legal obligations – may not altogether be absent in Europe.

Welcome as all these countermeasures are, there is a snag. One countermeasure consistently showing up is to introduce general-purpose electronic identity cards and numbers, often backed up by biometrics, aimed at preventing document or look-alike fraud. The downside of

---

[266] Anderson, Ross, Rainer Böhme, Richard Clayton & Tyler Moore (2008), *Security Economics and the Internal Market*, report for ENISA, January 2008, available at http://www.enisa.europa.eu/doc/pdf/report_sec_econ_&_int_mark_20080131.pdf, p. 3.

[267] European Data Protection Supervisor (2008), 'EDPS Opinion on ePrivacy Directive review: overall positive, but further improvements should be considered', Press Release available at http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/PressNews/Press/2008/EDPS-2008-03-EN_ePrivacy.pdf.

such measures is that they introduce considerable vulnerabilities: as the resulting identification infrastructure comes to rely heavily on the unique eID method, the risk of identity theft actually rises. If someone is able to appropriate someone's eID, the damage for the victim is all the larger as the system is used for ever more government services, and perhaps for commercial purposes as well as the private sector is ready to embrace secured government-introduced identification mechanisms. Moreover, the burden of proving being a victim of identity theft becomes heavier as the system is supposed to be more secure. The incidence of identity theft in countries with all-purpose identification infrastructures may be limited, but the potential damage for victims is huge. Thus, large-scale secured eID cards and similar measures to curb document fraud are a two-edged sword, and governments need to carefully consider and monitor emerging side-effects. Sectoral identification infrastructures with sector-border control might turn out to be a more prudent balance between preventing document fraud and preventing identity theft.[268]

Perhaps the most important lesson of this report's survey is that, although it seems evident that countermeasures to combat identity-related crime should be targeted at relevant vulnerabilities in the identification infrastructures, this is not always the case. Europe has wisely chosen not to follow the United States too closely in choosing countermeasures, since the prevalence of identity theft in the US most likely stems from vulnerabilities in the US financial system and market orientation that are specific to the US situation, with its epidemic data brokers and lack of verification in the private sector. However, a closer look is needed at vulnerabilities in the European situation itself. The current policy debate sometimes, for example in France, focuses perhaps still too much on document fraud and too little on online financial identity theft, and a comprehensive plan of attack to combat phishing by botnets rather than by fake websites has yet to be developed.

Therefore, rather than continue to harp on about generally accepted definitions, the lack of data, and whether or not to start registering identity-related crime incidence before countermeasures can be taken, a better approach to address the threat of identity-related crime may well be to start conducting more in-depth studies of the strengths and weaknesses of European financial and identification infrastructures in the information society. Now that identity theft is past the stage of big hype in the US, there is yet time to prevent it becoming a big problem in Europe.

[268] Compare also Buitelaar, Hans (ed.) (2007), *D13.3: Study on ID Number Policies*, FIDIS deliverable, available at http://www.fidis.net, on various possible identification number policies.

Selected Bibliography

Anderson, K. B. (2005), 'Identity Theft: Does the Risk Vary With Demographics?', Federal Trade Commission, Bureau of Economics Working Paper No. 279, available at http://www.ftc.gov/be/workpapers/wp279.pdf.

Anderson, Ross, Rainer Böhme, Richard Clayton & Tyler Moore (2008), *Security Economics and the Internal Market*, report for ENISA, January 2008, available at http://www.enisa.europa.eu/doc/pdf/report_sec_econ_&_int_mark_20080131.pdf.

Buitelaar, Hans (ed.) (2007), *D13.3: Study on ID Number Policies*, FIDIS deliverable, available at http://www.fidis.net.

De Bot, D. (2005), Privacybescherming bij e-government in België, Vanden Broele, Brugge, n°249.

De Cock, D. Ch. Wolf & B. Preneel, The Belgian Electronic Identity Card, (Overview), available at http://www.cosic.esat.kuleuven.be/publications/article-769.pdf.

Denolf, J. (ed.), *Identiteitsfraude. Misdrijf van de toekomst? Fraude d'identité. Le crime du future?* Politeia, Brussels, 2005.

Draps, K. (2007). Identiteitsfraude. Een routineactiviteitenbenadering, Leuvense Universiteitsbibliotheek, Leuven.

Government Accountability Office (2002), "Identity Theft: Prevalence and Cost appear to be growing", Report to the Congressional Requesters.

Home Office Statistical Bulletin (2007), 'Mobile phone theft, plastic card and identity fraud: Findings from the 2005/06 British Crime Survey', available at http://www.homeoffice.gov.uk/rds/pdfs07/hosb1007.pdf.

Hoofnagle, C.J. (2007), "Identity Theft: Making the Known Unknowns Known", 21 *Harvard Journal of Law & Technology* (1).

Koops, Bert-Jaap & Ronald Leenes (2006), 'ID Theft, ID Fraud and/or ID-related Crime. Definitions matter', *Datenschutz und Datensicherheit* 2006 (9), p. 553-556.

Koops, Bert-Jaap, Ronald Leenes, Martin Meints, Nicole van der Meulen & David-Olivier Jacquet-Chiffelle (2008), 'A Typology of Identity-related Crime: Conceptual, Technical, and Legal Issues', *Information, Communication & Society* (forthcoming).

Leenes, R. (ed.) (2006), *D5.2b: ID-related Crime: Towards a Common Ground for Interdisciplinary Research*, FIDIS deliverable, available at http://www.fidis.net/.

Moore, T. and Clayton, R. 'An Empirical Analysis of the Current State of Phishing Attack and Defense'. Available at http://www.cl.cam.ac.uk/~rnc1/weis07-phishing.pdf.

Pintér, Róbert (ed.) (2007), *D5.2c: Identity related crime in the world of films*, FIDIS deliverable, available at http://www.fidis.net/.

Savirimuthu, A. & Joseph Savirimuthu (2007), 'Identity Theft and Systems Theory: The Fraud Act 2006 in Perspective', *4 Script-ed* (4).

United Kingdom Cabinet Office (2002), *Identity Fraud: A Study*, United Kingdom: Cabinet Office Publications.

De Vries, U.R.M.Th., H. Tigchelaar, M. van der Linden & A.M. Hol (2007), *Identiteitsfraude: een afbakening. Een internationale begripsvergelijking en analyse van nationale strafbepalingen*, Utrecht: WODC, http://www.wodc.nl/images/1496_%20volledige_tekst_tcm44-86343.pdf (English summary available at http://www.wodc.nl/images/1496_summary_tcm44-86342.pdf).