eCrime
ICT, law & criminology

01

eCRIME RESEARCH REPORTS

Andrea Di Nicola
Andrea Cauduro
Alberto Cordioli
Vincenzo Falletta
Fabiano Francesconi
Elisa Martini
Mara Mignone

WEB PRO ID

DEVELOPING WEB-BASED DATA COLLECTION MODULES TO UNDERSTAND, PREVENT AND COMBAT ID RELATED CRIMES AND FACILITATE THEIR INVESTIGATION AND PROSECUTION

Beneficiaries
eCrime, Faculty of Law, University of Trento (Coordinator)
RiSSC - Centro Ricerche e Studi su Sicurezza e Criminalità (Co-beneficiary)

Associate partners

Technological partners
Telecom Italia, Vodafone Omnitel, Wind Telecomunicazioni
Consorzio per la Tutela del Credito – CTC

Institutional partners
Ministero dell'Economia e delle Finanze – UCAMP
(Ufficio Centrale Antifrode dei Mezzi di Pagamento)

With financial support of the Prevention of and Fight against Crime Programme
European Commission - Directorate-General Home Affairs

eCrime Research Reports

No. 01

WEB PRO ID
Developing web-based data collection modules to understand, prevent and combat ID related crimes and facilitate their investigation and prosecution

Andrea Di Nicola (scientific coordinator)
Andrea Cauduro (project manager)
Alberto Cordioli
Vincenzo Falletta
Fabiano Francesconi
Elisa Martini
Mara Mignone

ISSN 2284-3302
ISBN 978-88-8443-529-3

eCrime - ICT, Law & Criminology
Faculty of Law
University of Trento
Via G. Verdi, 53
38122 Trento, Italy
+39 0461 282336
www.ecrime.unitn.it

Trento, March 2014

Table of contents

01

Acknowledgements 3

02

Executive summary 5

03

Identity-related crimes and the need for innovative tools to understand, prevent and combat them 9

3.1 Identity-related crimes: an overview 9
3.2 The need for innovative web and ICT solutions 11

04

Aim, objectives and activities of the project 13

05

Organization of this report 17

06

ID crimes against natural persons: the web victimization survey and its results 19

6.1 Research methodology 20
6.2 The questionnaire 21
6.3 Survey results 22
6.4 Legal remedies and policies to prevent identity crimes 33
6.5 Summary of the results of the victimization survey 34

07

ID crimes against companies: the web data collection module to collect case studies on IDRC against businesses and related results 37

7.1 Foreword 37
7.2 Qualitative analysis of case studies in the mobile communication sector 38
7.3 Legal remedies 42
7.4 Summary of the results of the qualitative analysis 50

08

WASP: an alert system to prevent and tackle ID crimes against companies 53

8.1 Problem statement 53
8.2 Methodology 54
8.3 WASP 57
8.4 Remarks on WASP 65
8.5 Summary of the results of WASP 66

bi

Bibliography 69

a

Annex A: Guidelines for exporting the web modules to carry out a victimization survey on identity-related crimes in EU Member States 71

Annex B: Guidelines for exporting the web modules for the collection of business case studies on identity-related crimes 73

Annex C: Guidelines to export WASP 75

Annex D: Notes on the algorithms employed 77

Annex E: An example of a WASP Graphical User Interface (GUI) 79

Annex F: Questionnaire of the victimization survey 81

01

Acknowledgements

This report presents the results of project “WEB PRO ID - Developing web-based data collection modules to understand, prevent and combat ID related crimes and facilitate their investigation and prosecution”, financed by the European Commission under ISEC programme (project no. HOME/2010/ISEC/AG/FINEC-018), coordinated by eCrime, the research Group on ICT, law and criminology of the Faculty of Law of the University of Trento and carried out together with RiSSC-Centro Ricerche e Studi su Sicurezza e Criminalità (co-beneficiary) and the assistance of the following associate partners: Telecom Italia, Vodafone Omnitel, Wind Telecomunicazioni, Consorzio per la Tutela del Credito – CTC (technological partners) and Ministero dell’Economia e delle Finanze – UCAMP (Ufficio Centrale Antifrode dei Mezzi di Pagamento) (institutional partner).

The research project has been coordinated by Andrea Di Nicola, assistant professor in criminology at the Faculty of Law of the University of Trento and scientific coordinator of eCrime. Andrea Cauduro, senior researcher at eCrime, Faculty of Law, University of Trento, acted as project manager. Themistoklis Palpanas, associate professor of Massive Data Analytics at the Department of Information Engineering and Computer Science of the University of Trento and member of eCrime, supervised the ICT component of the project. Other researchers at eCrime contributed to the research activities (in alphabetical order): Alberto Cordioli, researcher at eCrime, Faculty of Law, University of Trento; Giuseppe Espa, full professor of Data Analysis and Statistics at the Department of Economics and Management of the University of Trento and eCrime member; Vincenzo Falletta, senior researcher at eCrime, Faculty of Law, University of Trento; Fabiano Francesconi, researcher at eCrime, Faculty of Law, University of Trento; Fausto Giunchiglia, full professor of Research Methodology and Logic for data representation and knowledge at the Department of Information Engineering and Computer Science of the University of Trento and eCrime member; Elisa Martini, senior researcher at eCrime, Faculty of Law, University of Trento; Barbara Vettori, assistant professor in Sociology of Deviance at the Catholic University of Milan and eCrime member; Ilya Zaihrayeu, post-doctorate student in Computer Science at the Department of Information Engineering and Computer Science of the University of Trento and eCrime member.

The research group also included RiSSC researchers. The group was coordinated by Mara Mignone, PhD and Criminologist, co-founder and President of RiSSC, with the support of Lorenzo Segato, PhD and Criminologist, co-founder and Director of RiSSC, and included Valentina Scioneri, Project Manager at RiSSC, Sinuè Bisello and Fabio Negro, junior researchers at RiSSC. The group was supported by two external experts, Fabio Carli, Contract Professor at Milano Bicocca University - Faculty of Economics and Francesca Bosco, Project Manager at UNICRI. Cristina Gallina assisted with the proof reading of the final text.

This research work would not have been feasible without the help and assistance of a number of persons. First of all, we would like to thank for their help our associate partners for their support (above all for the data provided) and their valuable suggestions and comments, webmaster, the administrative staff at eCrime and at the Faculty of Law of the University of Trento, together with all the many other persons impossible to list here without whom this research would not have been accomplished. Second, we would like to express our gratitude to the Directorate-General Home Affairs of the European Commission which, under the ISEC Programme, has supported both the project and the realisation of this publication. Adrian Belton kindly assisted with the proof reading of the final text.

02

Andrea Di Nicola

Executive summary

This report sets out some of the final results of Project *WEB PRO ID - Developing web-based data collection modules to understand, prevent and combat ID related crimes and facilitate their investigation and prosecution*, financed by the European Commission under ISEC programme (project no. HOME/2010/ISEC/AG/FINEC-018). WEB PRO ID was coordinated by eCrime, the research Group on ICT, law and criminology of the Faculty of Law of the University of Trento and carried out together with RiSSC-Centro Ricerche e Studi su Sicurezza e Criminalità (co-beneficiary) and the assistance of the following associate partners: Telecom Italia, Vodafone Omnitel, Wind Telecomunicazioni, Consorzio per la Tutela del Credito – CTC (technological partners) and Ministero dell'Economia e delle Finanze – UCAMP (Ufficio Centrale Antifrode dei Mezzi di Pagamento) (institutional partner).

For the purpose of the report *identity theft (or impersonification)* is defined as the theft or assumption of the identity of an existing or "existed" person for criminal purposes, and *identity frau*d as the creation of a completely or partially false identity (so-called 'synthetic identity') for criminal purposes. *Identity-related crime*s (or identity crimes) as both the abovementioned criminal conducts.

More specifically, project WEB PRO addressed the issues of the prevention and fight against ID-related crime (ID theft/ID fraud) by focusing on the need for:

- advanced horizontal solutions and tools, especially technology-based, which enhance the collection, exchange, and processing of information, data, and fraud-cases related to the victimisation of both persons and businesses;
- an innovative and information-based ID management system, including shared and sound procedures, to monitor the phenomenon and to prevent ID-related crimes by means of alert systems;
- enhanced public and private cooperation;
- better mutual understanding and coordination among law enforcement agencies, national authorities, private companies and citizens.

All these strategies should be adopted to prevent and fight against ID-related crimes.

Given this research need, project WEB PRO ID aimed at preventing/combating ID-related crimes (IDRC) against citizens and businesses by promoting ID management and facilitating the investigation and prosecution of IDRC with the development of innovative data collection modules and ICT tools.
To achieve these aims, the project set itself the following general objectives:

1) develop web-based data collection modules on identity-related crimes against both citizens and businesses;
2) promote and implement ID ICT management solutions based on processed information, innovative preventative tools and alert-systems;

3) foster mutual understanding and training between Law Enforcement Agencies (LEAs) and private companies.

Project WEB PRO ID had broad and multidisciplinary objectives, with many activities that led to the following results: a website, web modules, a prototype software, training activities, dissemination. This report refers only to some of the activities carried out and to some of the results achieved during the project. More specifically, this report:

- delineates the features of the victimization web-survey module on IDRC against persons in terms of methodology and presents the analysis of the results of the web survey administered to a sample of Italian citizens;
- describes the characteristics of the web data collection module on IDRC against businesses and presents the findings of the analysis carried out on a number of case studies of ID crimes suffered by some of the companies partners of the project and retrieved through the module;
- describes the results of the analysis of the data provided by companies partners of the project, which included activation requests by customers for services/devices, and presents the features of *WASP* (*Webproid Alert System Prototype*), the computerized alert system (prototype software) for the prevention of IDRC and correlated crimes against businesses that was developed also on the basis of this analysis.

The results from the above three areas were as follows.

Victimization survey

Through the development of a web module, it was possible to administer a questionnaire to Italian citizens to gather data on victimization and perception on the risk of suffering identity theft. As regards the general figures, 15% of the sample had suffered at least one ID theft in their lives, 25% of them had been multi-victimized. As regards the profile of the typical victim, there were some recurrent features: in detail, male, 35-54 years old, single, resident in Northern - Central Italy, high education level, employed, low income (< 20,000 euros), owner of a number of electronic devices, frequent user of the Internet for e-commerce/in-banking.

Victims' data were usually obtained through "phishing" emails, Facebook/social networks, wallet theft, malicious software, and they were used to create false documents, request loans, mortgages, etc., buy goods, sign a contract.

As for the consequences, 35% of the victims surveyed had discovered the ID theft after at least one week, 79.5% took a few days to resolve the problem, 56% experienced severe emotional distress. Only 47.4% of ID thefts were reported to the police, and the motivations for doing so were: track down the thief, a sense of moral/social duty, to obtain more control by police, to avoid paying for unrequested goods/services, to recover goods/money loss. As for the remaining 52.6%, they were not reported to the police because of: fear of retaliation, no monetary loss, nothing was stolen, no insurance, police discouraged the victim from reporting.

Identity thieves were in 83.4% of cases unknown to the victim. In the only 50 cases in which the thief was known, s/he was a single criminal, Italian, stranger to the victim.

As for the perception of and social insecurity about ID thefts, 93.1% of the respondents thought citizens should be concerned about the risk of suffering an ID theft, but only 37% of them were worried about the possibility of suffering an ID theft. Respondents who most feared being victimized were elderly, married, with a low education level, resident in Southern Italy. All of them were actually less victimized compared to other categories. By contrast, respondents who least feared being victimized were young people, single, with a high education level, resident in Northern and Central Italy. All of them were actually more victimized compared to other categories.

As regards the risk factors that favour the commission of an identity theft, the interviewees stressed people's carelessness in protecting their personal data, inadequate data protection by companies, too mild penalties, and lack of control by LEAs.

Finally, the interviewees also requested a series of public measures: information and awareness campaigns for citizens, a free toll number to report ID crimes and/or advise citizens, specific laws against ID theft, more severe penalties, and the creation of a public authority for the prevention and fight against ID theft.

Business case studies

Through the development of a web module dedicated to gathering business case studies, it was possible to obtain data from December 2010 and August 2013. The general results were a high vulnerability to ID crimes related to signing a contract that can take the form of identity thefts (or impersonation, which is the use of an identity related to natural or legal existing or existed persons) or of identity frauds (i.e. the use of a fictitious or real identity with alteration of some relevant sensitive data). The purpose of ID crime was to misappropriate devices (e.g. smartphones, tablets, PCs), more than the phone-related frauds concerning the call traffic. Also found was the key importance of document falsification

(e.g. use of the stolen original documents with alteration of pictures and/or data, or use of entirely counterfeit documents), and fraudsters' ability to adjust criminal fraud schemes related to signing up contracts on the basis of the specific vulnerabilities of the victimized company (e.g. type of commercial offers, users and equipment, control systems).

Similarly to what happens in the case of frauds against natural persons, also when frauds are committed against companies there is a high likelihood of impunity for the perpetrators. Furthermore, the police shows a marginal role both in the process of verification/investigation of suspected fraud and in the case of a confirmed fraud. The report to Police concerned only 5% of cases of identity theft and 18.6% of cases of identity fraud.

The data showed a predominance of identity theft over identity fraud. Identity theft represented 75% of the cases analyzed; 87% of cases were crimes committed against a legal person (company ID theft). In 89% of cases, the perpetrators requested to sign a new contract, usually with personal data related to a new customer (85.9%), in 65% of cases, the average duration of fraud by signing up was limited, being no more than 30 days. The channels most frequently used for signing a contract were the "physical" ones of a store/dealer (31%) and of an agency (26%).

As mentioned above, the purpose of fraud by signing up related to the identity theft is the misappropriation of the cutting-edge smartphones (40.8%), mobile phones and tablets and on average, for each case at least 5 devices are stolen, while the phone-related frauds associated with the abuse or the resale of call traffic are marginal (17%).

Considering the documents provided when requesting a contract, in 47.3% of cases totally counterfeit documents were used: in particular, identity card, fiscal code number, health insurance card, and VAT registration certificate.

Finally, the average loss per case was between 2000 and 3000 euros, but sometimes fluctuated between 20 thousand and 35 thousand euros per case

By contrast, ID frauds represented less than a quarter of the sample of cases analyzed (24.7%) and included new activations (96%) made by new customers (95%). As regards *modi operandi*, they seemed to show more precise borders than those of identity theft. Because ID frauds are aimed almost exclusively at the misappropriation of cutting-edge mobile phones, they require a lower level of expertise and may be committed serially, also considering the fact that their average duration does not exceed 30 days. The most frequently used channel for frauds by signing up related to the identity fraud was the agency (41.2%).

The response to such crimes by companies varied: in the case of identity theft, the detection took place thanks to the alerts generated by the control systems (53%), but also to the analysts' activities (37.9%). In the case of identity fraud, the analysts' work was the essential factor (72%).

WASP - Webproid Alert System Prototype

The third area of research carried out for WEB PRO ID concerned analysis of activation datasets provided by telecommunication and credit companies in order to apply data mining techniques to identify those typical patterns that characterize a fraudulent identity. From this knowledge, researchers then developed a software prototype WASP (Webproid Alert System Prototype) able to exploit data mining techniques to rank the identities most at risk of an ID crime and provide them to company analysts for further preventative/tackling actions. In addition, researchers developed a common database able to merge and share anonymized fraudulent identities previously identified by project partners so as to allow cross-checks and tackle serial identity fraudsters.

Specifically, the results of the analysis showed that, in the partners' datasets, fraudulent identities varied from 1% to 1‰ of the total number of instances; 4% of fraudulent identities were in common between partners; and 75% of frauds lasted less than one month (25% lasted 1-7 days, 22% lasted 8-15 days, 28% lasted 16-30 days).

The software that was developed relied on the following algorithms: CART, Random Forests, RIPPER and SVM and is three-tier based:

1) *Presentation tier* made up of a web Application to enable the final user to access WASP via a browser;
2) *Logic tier* made up of: a) Ranking System (RS), a component that ranks identities according their risk of being fraudulent; b) Shared Identity Engine (SIE), a database in which fraudulent identities (encrypted) are stored and shared among project partners; Data Mining Engine (DME), a component in which several data mining algorithms are used to produce predictions about the risk of an identity being fraudulent;
3) *Data integration tier* made up of: a) Database layer for the implementation of a set of databases containing partners' data; b) Integration layer for the integration and interoperability of the various (and different) partners' datasets.

03

Andrea Cauduro

Identity-related crimes and the need for innovative tools to understand, prevent and combat them

3.1 Identity-related crimes: an overview

3.1.1 Definitions. Identity has become an increasingly crucial asset for citizens and companies. In the present-day information society, digital and "real-life" identities often overlap to create, on the one hand, great opportunities for economic and personal development, but on the other, opportunities for the easy commission of (serious) crimes. By way of example, *phishing* is a technique used to steal the access codes of bank accounts and transfer money from them (Wall, 2007). Beside this "classic" crime aimed at obtaining personal data for illicit gain, in the past few years identity crimes[1] have been developed and refined to extend their range of action:

for example, to obtain undue funding, or to avoid sanctions (e.g. the use of a stolen identity to obtain welfare benefits, or to charge an unaware victim with a fine for a driving offence). Furthermore, crimes facilitated by stealing/altering an identity can have purposes other than illegal gain. This is the case of e.g. cyberbullying or stalking committed through the identity of an unaware person by using instant messaging programmes (Patchin & Hinduja, 2006; Smith et al., 2008). Finally, identity misuse can be a key factor in crimes against the state or public order: as exemplified by the 9/11 attacks, when "*several of the hijackers had used fraudulent documents to obtain Virginia driver's licenses, which were then easier to obtain because of a loophole that allowed proof of identity and residence with an affidavit rather than an official document*" (Elston & Stein, 2002, p. 4).

There is a common factor In all cases: the theft of Identity is a preliminary offence committed to enable the commission of another crime (e.g. fraud, libel).

In this regard, and before illustrating international trends, it is necessary to give definitions to the various criminal offences concerned. The task is not easy, because the debate is still open and experts/researchers do not completely agree on an ultimate classification.[2] However, the most accepted ones follow:

[1] Henceforth also referred to as "ID crimes".

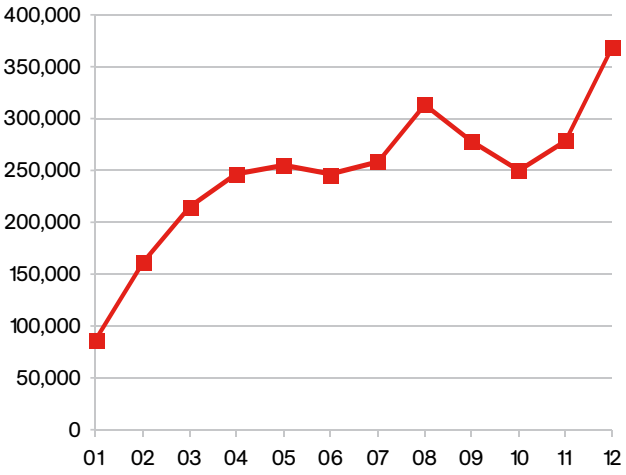
[2] Some researchers (mainly in the USA) prefer the term 'identity theft' to 'identity fraud', since they maintain that the fraud affects the person victim of the abuse rather than the identity itself (Acoca, 2008; McNally & Newman, 2008, p. 2). Other researchers dispute the concept of identity theft, arguing that one should only refer to "identity abuse" since identity cannot be stolen (Acoca, 2008, p. 74). Finally also some international bodies have recently contributed to the debate on the definition of identity crimes: see Europol (2006) and United Nations (2007). Although interesting, these questions will not be discussed further since do not pertain to the aim of this report.

1) *Identity theft (or impersonification)*: the theft or assumption of the identity of an existing or "existed" person for criminal purposes;
2) *Identity fraud*: the creation of a completely or partially false identity (so-called 'synthetic identity') for criminal purposes (Acoca, 2008; Fraud Prevention Expert Group, 2007; UNODC, 2011, p. 26).
3) *Identity-related crimes (or identity crimes)*: both the above-mentioned criminal offences.

3.1.2 Identity-related crimes: international and EU trends

Identity abuses are not new in the criminal scenario. However, the spread of the Internet and new technologies (e.g. smart phones, tablets) has generated a rocketing growth of such criminal actions. In this regard, studies have been conducted in several countries in the past few years to monitor and quantify the phenomenon. A very recent study conducted in the USA reveals that "*approximately 16.6 million persons or 7% of all U.S. residents aged 16 or older, were victims of one or more incidents of identity theft in 2012*" and that the misused information mainly concerned bank or credit card accounts (Harrell & Langton, 2013). These data are in line with those reported by the US Federal Trade Commission (FTC), which has been collecting information on ID thefts since 2001. According to the last available data (Federal Trade Commission, 2013), complaints about ID thefts have more than quadrupled in this period (see Figure 1 below). This finding is likely to be affected by the increased awareness among US citizens of ID crimes that may make them more prone to report such offences. Nonetheless these figures highlight the rapid growth of such crimes in recent years.

Figure 1 - Trend of ID thefts reported to the US Federal Trade Commission. 2001-2012.



Source: eCrime elaboration on FTC 2013 data

As well as the trend in reported ID crimes, the FTC also indicates the main purposes of such crimes, stressing that the victims are the state, citizens and companies: "*Government documents/benefits fraud (46%) was the most common form of reported identity theft, followed by credit card fraud (13%), phone or utilities fraud (10%), and bank fraud (6%). Other significant categories of identity theft reported by victims were employment-related fraud (5%) and loan fraud (2%)*" (Federal Trade Commission, 2013, p. 3).

As regards the victims, the majority (68%) report the crime to the police, although this percentage has decreased in the past three years (2013, p. 13). Finally, as regards the age profile of the victims, the FTC study highlights that the victims are mainly aged under 50 (64%) with a peak in the 20–to-29 age range (21%).

Besides these official data, which concern reports to the FTC and the police, a series of studies on ID thefts have sought to determine their frequency, their aims, and the damage suffered by victims by taking a different approach: that of the victimization survey. For example, the results of a victimization survey conducted on a random sample in 2009 by the Identity Theft Resource Centre (ITRC) are in line with the official data (2010, p. 6): 68% of victims were aged under 49, and were mainly concentrated between the ages of 20 and 29 (25%). Another victimization survey carried out in the USA is the one by Synovate for the FTC (2007, pp. 3–4). The study estimated that in 2005, 3.7% of the US population (8.3 million persons) suffered an ID theft for fraud purposes. In detail, the report stated that 1.5% of the population had incurred damage relative to bank cheques/accounts, or phone contracts; while 1.4% of citizens discovered that illicit use had been made of their credit cards; and 0.8% found that their ID had been abused to activate contracts, bank accounts, etc. with the purpose of committing further frauds concealed behind the stolen identity.

Compared to official data, the added value of victimization surveys is that they make it possible to collect a large amount of information on the crime suffered, on its dynamics, on the reasons for reporting/not reporting it; and also on the perception of security relative to specific offences. For example, the Synovate survey found that the majority of victims detected the ID theft in less than one week, although a number of persons discovered the abuse after longer periods, sometimes even more than six months after the theft (2007, p. 23). This trend was confirmed by the ITRC, which stressed that 45% of the abuses were detected within three months, although "*the percentage of those discovering the first incident of identity theft more than 24 months after its occurrence remains alarmingly high*" (2010, p. 19).

Another aspect explored by victimization surveys is the perpetrator/victim relationship. According to Synovate, in 84% of cases the victims did not know the perpetrators of the ID crime; and in 56% of the episodes victims did not know how their data had been stolen (2007, pp. 27–28). Similar evidence is provided by ITRC data: 63% of the citizens interviewed did not know the imposters who had abused their identity; while of those known to them,13% were relatives, 6% ex-spouses or significant others, 5% friends/roommates (2010, p. 16).

Finally, studies based on victim interviews yield better information on the timing of the problem's solution and the economic damage suffered. As regards the former aspect, the solution required some days to up to three months (Synovate, 2007, pp. 25–26) or an average of 141 hours according to the ITRC, but in this case it should be noted that "*it is important to remember that these hours may be over a period of weeks, months or even years. Victims must wait for answers to letters or reports to be completed before proceeding*" (2010, p. 20).

What about the "average" economic damage? Synovate (2007, pp. 35–36) estimated the median value of the losses at $ 500. On the same topic, ITRC used different calculation methods (mainly linked to quantification of the hours taken to solve the problem) and estimated that the average cost of repairing the damage due to the takeover of existing financial accounts was $ 527, while it increased to $ 2,104 in the case of "*new financial accounts, criminal, governmental issues or a combination of several situations*" (2010, p. 20). Furthermore, the ITRC also focused on the financial losses to companies targeted by ID crimes to obtain e.g. financial benefits, phone credit, on devices. In this case, a non-representative sample of US companies stated their losses, and from these data the ITRC calculated an average loss of $ 29,162, with peaks of more than $ 100,000 (2010, p. 23). In this regard, since the sample used for the estimation did not reflect the entire universe of US firms, the estimate cannot be considered fully reliable, as correctly stated by the authors.

The situation illustrated above for the USA is similar in the European area, although the number of studies is more limited. For example, a survey conducted for Eurobarometer reports that "*on average across the EU, 8% of internet users say they have experienced or been a victim of identity theft. This figure is similar in most EU countries, but is highest in Romania, where 16% of internet users say they have experienced identity theft, including 5% who say it has happened to them often. Respondents in Hungary (12%), UK (12%) and Austria (11%) are also more likely than average to say they have experienced identify theft. The lowest levels are in Slovenia (2%), Lithuania (2%), Greece (3%) and Denmark (3%)*" (TNS Opinion & Social, 2012, p. 48).

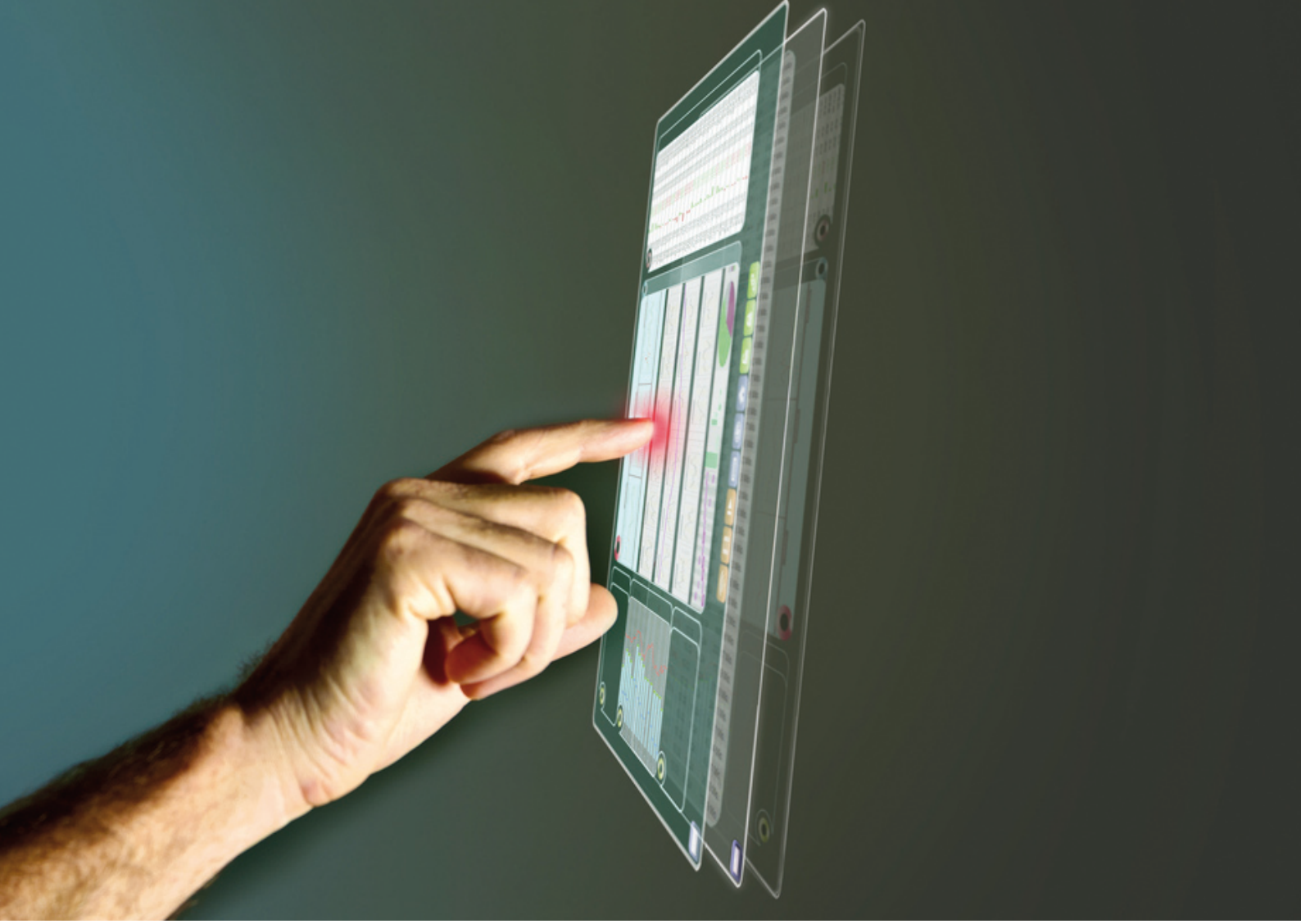
3.2 The need for innovative web and ICT solutions

It is clear from the data illustrated above that identity-related crimes are proliferating. Their steep rise should be monitored since they enable the commission of a variety of offences against property, persons and/or the state security. Unfortunately, identity misuse has to date been investigated in a scattered manner. There have been some valuable pieces of research (above all in the USA), but much has still to be explored: from a final definition of ID crimes, through a clearer picture of their amount, frequency, and development, to the drafting and deployment of more effective counter-strategies. In particular, further studies are essential to improve overall knowledge on IDRC so as to provide citizens and companies with stronger tools to defend themselves and/or to prevent the serious economic/reputational damage that they may incur in the case of identity-related crimes.

More specifically, project WEB PRO addresses the issues concerning the fight against ID-related crime (ID theft/ID fraud) by focusing on the need for:

- advanced horizontal solutions and tools, especially technology-based, which enhance the collection, exchange and processing of information, data and fraud cases related to both citizen and business victimisation;
- innovative and information-based ID management systems, including shared and sound procedures to monitor the phenomenon and prevent ID-related crimes by means of alert systems;
- enhanced public and private cooperation;
- better mutual understanding and coordination among law enforcement agencies, national authorities, private companies and citizens.

All these strategies should adopted to prevent and fight against ID-related crimes.



04

Andrea Di Nicola

Aim, objectives and activities of the project

In front of this research need, the aim of Project WEB PRO ID[3] is to prevent/combat ID-related crimes (IDRC) against citizens and businesses by promoting ID management, and facilitating the investigation and prosecution of IDRC by developing innovative data collection modules and ICT tools.

To achieve these aims, the project set itself the following general objectives:

1) develop web-based data collection modules on identity-related crimes against both citizens and businesses;
2) promote and implement ID ICT management solutions based on processed information, innovative preventative tools and alert systems;
3) foster mutual understanding and training between Law Enforcement Agencies (LEAs) and private companies.

Under objective 1, the following activities were conducted:

- Activity 1.1. Creation of a victimization web-survey module on IDRC against persons consisting of an online questionnaire administered to collect information about a) if/when in the last year a person had undergone IDRC; b) correlated crimes and (un)safety concerns about these offences. The web-survey was designed for a) periodic repetitions; b) replication in other Member States.
- Activity 1.2. Creation of a web data collection module on IDRC against businesses developed in collaboration with associate partners to a) collect case studies on IDRC undergone by businesses; b) collect information for comprehension of the cases; c) guarantee transferability of the module to other Member States.
- Activity 1.3. Creation of a website dedicated to data collection (www.webproid.eu). This was the input point for the data connected to the two modules under activities 1.1 and 1.2. Dedicated sections allowed surfers to report IDRC cases, to obtain information and legal aid, to consult and comment on Project's outputs.
- Activity 1.4. Implementation of the victimization web-survey module on IDRC against persons, population of the related database (db) and drafting of guidelines for its replication in other MSs. Web surfers would use the victimization web-survey module to input data and populate a db (victimization db). Guidelines for the use of the module will be drafted to favour its exportation.
- Activity 1.5. Implementation of the web data collection module on IDRC against businesses, population of the related db and drafting of guidelines for its replication in other Member States. Associate

[3] Henceforth also referred to as 'WPI'.

partners employed the module to input data on IDRC case studies suffered by their corporations and populate a db (case studies db). More specifically, a number case studies by two of the telecommunication companies partners of the project (Vodafone and Wind) were collected through the web module developed under activity 1.2. These data made it possible to populate a database. Guidelines for the use of the module were drafted to favour its exportation.

Under objective 2, the following activities were conducted:

- Activities 2.1. Based on data collected under activities 1.4 and 1.5, development of qualitative and quantitative analyses of the dynamics and trends of IDRC and identification of legal remedies.

- Activities 2.2. Definition of a protocol enabling LEAs and businesses to access the database under activity 1.5.

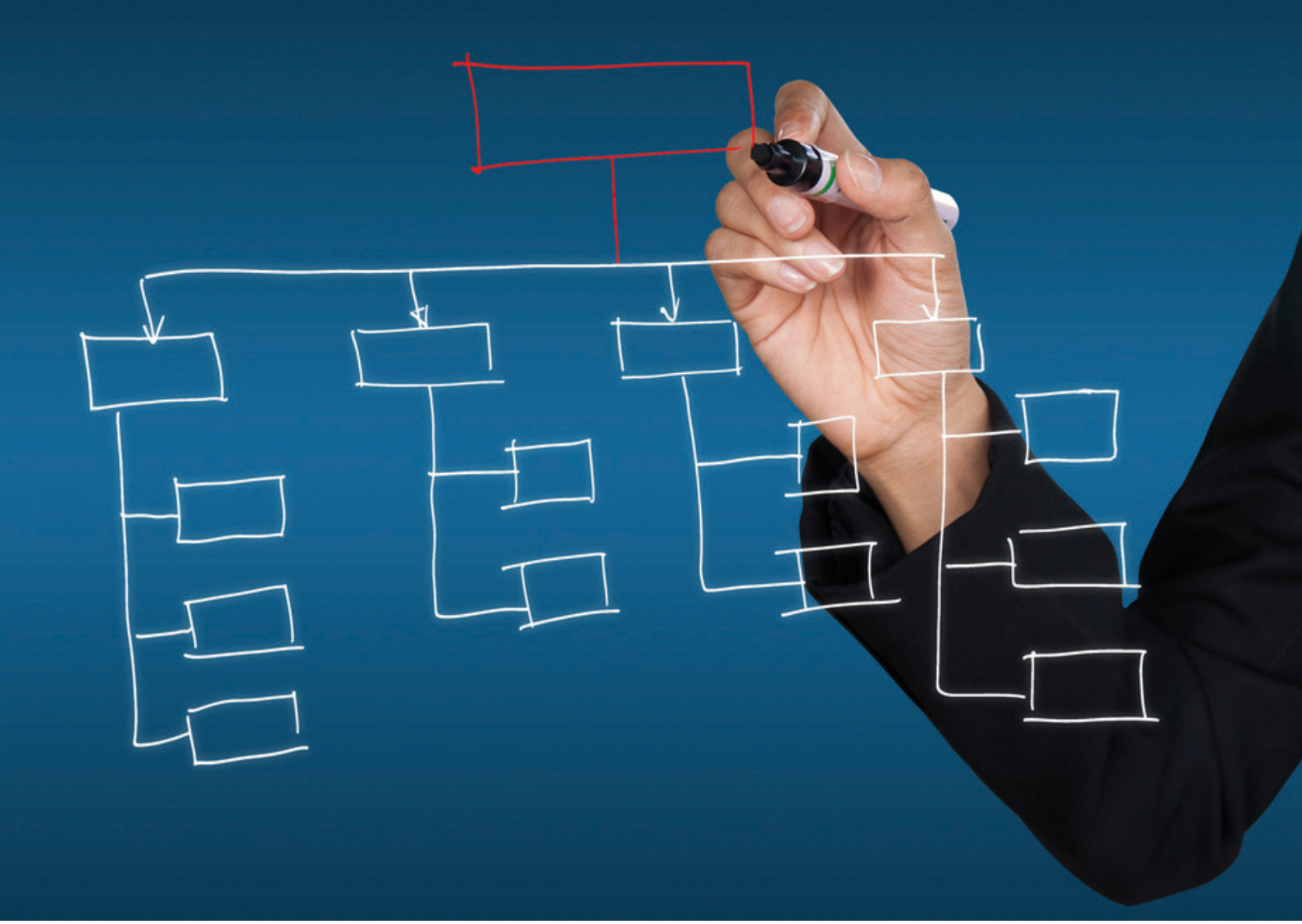
- Activities 2.3. Development of a computerized alert system (prototype software) for the prevention of IDRC and correlated crimes against businesses. Some telecommunication[4] and credit companies[5] involved in WEB PRO ID provided the researchers with databases containing various months of activation requests (services, new mobile phones, loans, etc.) that represented a crucial dataset for the research (see below general objective 2). Also in this case guidelines for exportation have been drafted.

Under objective 3, the following activities were conducted:

- Activity 3.1. Drafting and delivery of a joint training program between public (LEAs, universities) and private sector actors made up of working tables/ seminars and backed by the databases created in the project. In detail, two training seminars were carried out in Trento and Rome to illustrate the results of the research and the potentialities of the alert system developed. In addition, a final conference was held in Trento to disseminate the findings and foster dialogue between LEAs and private companies in the fight against and prevention of identity-related crimes.

[4] Vodafone Omnitel B.V. and Wind Telecomunicazioni s.p.a.

[5] Compass s.p.a., member of CTC.



05

Andrea Di Nicola

Organization of this report

As stated above in Chapter 4, project WEB PRO ID had broad and multidisciplinary objectives, with many activities that led to the following results: a website, web modules, a prototype software, training activities, dissemination. This report refers only to some of the activities carried out and some of the results achieved during the project, as follows.

After Chapters 1 to 5, which are introductory, **Chapter 6** delineates the features of the victimization web-survey module on IDRC against persons in terms of methodology (activities 1.1 and 1.4 on the web-based data collection modules on identity-related crimes against citizens); and it presents the analysis of the results of the web survey administered to a sample of Italian citizens (activity 2.1). The aim of this analysis was to:

a) determine how many Italian citizens have suffered one or more identity-related crimes;
b) trace a profile of persons at risk of offences;
c) draw a picture of the security perceptions of the interviewees as regards identity-related crimes;
d) outline possible legal measures that could help in preventing/tackling identity-related crimes.

Additional information on the victimization survey is provided at **Annex A:** *Guidelines for exporting the web modules to carry out a victimization survey on identity-related crimes in EU Member States* and at **Annex F:** *Questionnaire of the victimization survey*.

Chapter 7 describes the characteristics of the web data collection module on IDRC against businesses (activities 1.2 and 1.5 concerning the web-based data collection modules on identity-related crimes against businesses), and it presents the findings of the analysis carried out on a number of case studies on ID crimes suffered by some of the companies partners of the project and retrieved through the module (activity 2.1). In detail, these cases were examined in order to understand the dynamics of such offences: e.g. recurrent patterns, techniques employed, normative weaknesses and/or prevention systems adopted by companies. At the end of the analysis, some legal measures to tackle and prevent IDRC are outlined.

Additional information on this issue is provided at **Annex B:** *Guidelines for exporting the web modules for the collection of business case studies on identity-related crimes*.

Chapter 8 describes the features of *WASP* (*Webproid Alert System Prototype*), the computerized alert system (prototype software) for the prevention of IDRC and correlated crimes against businesses. Additional information regarding the *WASP* is provided at **Annex C:** *Guidelines to export WASP*, **Annex D:** *Notes on the algorithms* employed *employed*, **Annex E:** *An example of a WASP Graphical User Interface (*GUI).

Other information and documentation (e.g. training seminars and final conference materials) related to the project, but not included in this report, are available at the project website: webproid.unitn.it, or can be requested at this email address: ecrime@unitn.it.

06

Andrea Cauduro
(6.2, 6.3.1, 6.4)

Andrea Di Nicola
(6.3.2, 6.3.5)

Elisa Martini,
(6.1, 6.3.3, 6.3.4)

ID crimes against natural persons: the web victimization survey and its results

One of the major research problems regarding ID crimes (as highlighted in Chapter 3) is the scattered nature of knowledge about the victims of and trends in such offences. Assistance in remedying this shortcoming is provided by the criminological research that, over the years, has developed a series of qualitative and quantitative methodologies and tools. In particular, one of them has become a research standard: the victimization survey, which has been spreading since the 1960s (Vettori, 2010) and whose main purpose is to gain detailed knowledge on the dynamics of a crime and, specifically:

a) to determine the 'dark figure' (the crimes not reported to the police and the reasons for not reporting them); b) to investigate the perception of insecurity, correlating it to the socio-demographic characteristics of the respondents (for instance, age, education, occupation, gender); c) to understand whether there is a relationship between victims and their daily routines (see Groves et al., 2013; and Linch & Addington, 2007).

Drawing on this research background, one of the aims of project WEB PRO ID[6] was to develop a web-based data collection module on identity-related crimes against citizens, and innovative methods and tools (i.e. based on the web) to facilitate the data collection on ID crimes suffered by natural persons. This aim was achieved through the devising and conduct of a web victimization survey (*WPIvs – WEB PRO ID victimization survey*) to estimate the number of victims of identity theft in Italy, to outline their socio-demographic characteristics, as well as the ID theft dynamics, to study the victims' perception of the risk of suffering such crimes, and to understand whether there is a relationship among victims and their daily use of PCs, online trade, and online banking.

The chapter is organised as follows: a) a brief presentation of the research methodology (section 6.1); b) the questionnaire[7] administered (section 6.2); c) survey results on victim profiles (subsection 6.3.1), ID theft[8] characteristics (subsection 6.3.2), perception of and social insecurity concerning ID thefts (subsection 6.3.3), risk factors (subsection 6.3.4), public interventions to be deployed to tackle/prevent ID theft (subsec-

[6] Specifically, objectives 1.1, 1.4 and 2.1 of the project.

[7] For the text of the questionnaire, see Annex E below.

[8] Since in the case of an ID fraud, the personal data are invented or fake, no direct 'victim' exists. Therefore the survey carried out for WEB PRO ID focused on ID theft.

tion 6.3.5); d) possible legal measures to be enacted against ID theft (section 6.4). The chapter concludes with summary of the results (section 6.5).

6.1 Research methodology

Project WEB PRO ID defined identity theft as the assumption of the identity of an existing or "existed" person for criminal purposes.

In order to exploit the potentialities of victimization surveys and reduce their shortcomings, it was decided to conduct a web victimization survey (using the CAWI method: *Computer Assisted Web Interviewing*) for two main reasons. Firstly, this approach makes it possible reach a high number of persons in a short time and with costs lower than those of traditional surveys (e.g. CATI/CAMI methods). Secondly, it is possible to administer the survey through an online questionnaire hosted on a publicly accessible website in order to gain the highest visibility possible. The idea is to rely on a post sampling strategy. Consequently, for WEB PRO ID the questionnaire was published online and advertised so as to attract as many respondents as possible. This approach led to a self-selected sample that was then weighted.

A questionnaire was developed using *Limesurvey* software and hosted on the WPI website for about two months (from 25 September to 1 December 2013). *Limesurvey* is an open source platform for the creation of online questionnaires. It is extremely flexible software able to contain the most complex questions of a survey. It is possible to use filters between variables or sections, and the questionnaire is closed at the invitation via email. Compilation is anonymous, and the researcher can collect parameters – such as IP address, start time and end time of compilation – useful for improving the analysis of the data. Data can be exported to Excel, SPSS and R.

There are advantages and disadvantages to using the CAWI approach. One advantage is that it provides access to groups and individuals who would be difficult, if not impossible, to reach through other channels. Project WPI aimed to estimate the number of victims of identity thefts, crimes that are strictly correlated to Internet use. Hence this method reached the correct population to whom to administer the survey. A second advantage is that Internet-based surveys make it possible to save time. In fact, online surveys enable researchers to reach thousands of people with shared characteristics in a brief amount of time, even though they may be separated by great geographic distances. In addition, responses to online surveys can be immediately transmitted to the researchers through a database file. This permits preliminary analyses to be conducted on collected data while waiting for the desired number of responses to accumulate. The *WPIvs* used email-based surveys, inviting the population to fill in the questionnaire hosted on the WPI website. After the administration period, data were exported to statistical software packages (SPSS) in order to analyse the answers. The use of an online survey also eliminated the need for paper and other costs, such as those of postage, printing, and data entry. Similarly, conducting online interviews offers cost savings advantages: costs of recording equipment, travel, and the telephone can be eliminated. Finally, transcription costs can be avoided since online answers are automatically documented.

However, there are also disadvantages that should be considered by researchers contemplating the use of online survey methodology. When conducting online surveys, researchers may encounter problems as regards sampling. For instance, relatively little may be known about the characteristics of people in online communities, aside from some basic demographic variables, and even this information may be questionable. In order to avoid this problem, *WPIvs* used membership email lists (about 1,200,000 emails) provided by a company leader in Internet advertising and marketing, in which socio-demographic characteristics were validated by the business company. Once the email list had been obtained, researchers emailed an online survey invitation to every member on the list. Theoretically, this could give a sampling frame. However, problems such as multiple email addresses for the same person, multiple responses from participants, and invalid/inactive email addresses make random sampling online a problematic method in many circumstances. The *WPIvs* solution was to associate a unique code number with each email in order to avoid multiple responses; and in order to mitigate sample distortion, the *WPIvs* used a post-stratification approach by creating a weight variable.

On conclusion of the administration, the final *WPIvs* sample consisted of 2,176 cases, and it was made proportional to certain characteristics (gender, age, area of residence) of the Italian population by means of a post-stratification technique (weighting).[9]

For the purpose of *WPIvs*, the researchers used information acquired in the AVQ ISTAT Survey – (multipurpose survey on daily life) provides information on the

[9] The weighting of data is a way to vary how much a case counts (weights) in the dataset in order to make it comparable to a reliable sample or universe. For more details, see Levy and Leme (2008).

Table 1 – Calculation of weight variable

		AVQ Relative frequency		SAMPLE Relative frequency		Weight	
		Male	*Female*	*Male*	*Female*	*Male*	*Female*
Centre-North	18-24 years	0.13	0.12	0.04	0.08	0.13/0.04	0.12/0.08
	25-34 years	0.18	0.21	0.13	0.18	0.18/0.13	0.21/0.18
	35-44 years	0.25	0.28	0.18	0.22	0.25/0.18	0.28/0.22
	45-54 years	0.23	0.23	0.25	0.28	0.23/0.25	0.23/0.28
	55-64 years	0.14	0.12	0.24	0.16	0.14/0.24	0.12/0.16
	>65 years	0.08	0.04	0.16	0.06	0.08/0.16	0.04/0.06
	Total	1.00	1.00	1.00	1.00		
South and Islands	18-24 years	0.18	0.20	0.04	0.07	0.18/0.04	0.20/0.07
	25-34 years	0.23	0.27	0.13	0.23	0.23/0.13	0.27/0.23
	35-44 years	0.23	0.25	0.21	0.27	0.23/0.21	0.25/0.27
	45-54 years	0.19	0.18	0.30	0.27	0.19/0.30	0.18/0.27
	55-64 years	0.12	0.08	0.19	0.11	0.12/0.19	0.08/0.11
	>65 years	0.05	0.02	0.13	0.04	0.05/0.13	0.02/0.04
	Total	1.00	1.00	1.00	1.00		

socio-demographic composition of the people using the Internet (ISTAT, 2013). To calculate the weight, researchers combined data on age, gender and area of residence, and they estimated the relative frequency for each cell, both for the AVQ survey and *WPIvs*. Finally in order to obtain the weight variable, they compared the frequencies calculated in the AVQ survey and *WPIvs* sample, as shown above (Table 1).

6.2 The questionnaire

The questionnaire was structured into three main sections: a) socio-demographic characteristics of the respondents, with a part on the frequency and kind of their Internet use; b) ID theft victimization; c) perception of security and social insecurity about identity crimes.

Specifically, in the first section the questions focused on standard demographic information, such as: gender, marital status, age, area of residence, occupational status, educational level, income class. Moreover, some information was gathered about Internet use, such as: e-commerce frequency, in-banking frequency, type and number of electronic devices owned.

The second section of the questionnaire asked whether the respondents had been a victim of identity theft in their lives. If so, they were asked to answer a series of questions regarding their experience with identity theft. In particular:

- number of previous experiences of victimization;
- knowledge about the use of both personal data and stolen data (creating false documents, requests for loans, financing or mortgages, purchasing goods, signing contracts, filling in a tax return, obtaining medical care, obtaining employment, defamation, stalking);
- features of the identity theft (how the data were obtained, when the theft was identified, whether or not the crime was reported to the police, and the reasons);
- features of the offender/s (number of people involved, proximity to the victim, perpetrator/s nationality);
- consequences of the theft (economic and social quantification of the loss, time taken to restore the situation).

Finally, if the respondent had never been a victim of identity theft, she/he was automatically moved to the third section, which asked about social and personal insecurity, specifically:

- level of concern about suffering an identity theft and motivation (social indicator);[10]
- level of concern about personally suffering an identity theft (individual indicator);[11]
- risk factors;
- suggestions for public measures to protect citizens.

6.3 Survey results

6.3.1 The victims

Identity theft is a dual crime since it usually affects two victims: the person whose identity was misused and the business whose service was stolen. This subsection provides an overview of the results regarding the respondents, correlating their socio-demographics data to the probability of suffering an identity theft in order to outline a potential victim profile. Specifically, this subsection details the number, percentage, and demographic characteristics of victims who reported one or more incidents of identity theft. Later, it focuses on the most recent incident experienced in order to describe victim responses to identity theft. It describes how the victim discovered the crime, financial losses and other consequences of identity theft (including the amount of time victims spent on solving related problems), reporting of the incident to law enforcement agencies and the motivation, the level of distress that the identity theft victims experienced.

In *WPIvs* 15 per cent of the sample (n=345) reported having been a victim of some form of an identity theft in their lives. About 75 per cent of the respondents that had experienced identity theft reported that they had experienced one episode. 25 per cent of respondents (about 4 per cent of the total sample) had experienced more than one episode during their lives. Subsequent findings in this report are based on the characteristics of the most recent episode of identity crime.

The percentage of respondents suffering an identity theft is in line with the results of similar victimization surveys in Europe; or, in some cases, the situation in Italy is better than in other European countries. For instance, according to research commissioned for UK Fraud Prevention Month almost a quarter of UK residents have been victims of identity fraud compared to a 17 per cent average across Europe. Even in Russia, only 20 per cent of the population has been affected by identity theft (National Fraud Authority, 2013).

Personal characteristics may influence the risks of identity theft inasmuch as these characteristics are linked to patterns of Internet use. In this regard, males had a higher probability of being victims of an identity theft; and this result is in line with those of other research studies underlining that more males than females report that someone had obtained their credit card information or forged a credit card in their name (Figure 2). Persons aged between 18 and 24 (less than 15 per cent) were the least likely to experience identity theft, followed by persons aged over 55 (15.8 per cent). The 35-54 age group was most at risk, with the highest significant impact being for persons aged 35-44 (Figure 3). The majority of the persons affected by identity theft lived in the north-centre of Italy (66.6 per cent) (Figure 4). They usually had a high education level (45.1 per cent had degrees) as other research had already underlined (Figure 6): victims with postgraduate degrees reported having been victimized more frequently than did graduates or victims with a high school diploma or less. Victims, usually, are employed (52.7 per cent, Figure 7) and unmarried (45 per cent, Figure 5). Persons in the lowest income category (those with an annual household income of 20,000 euros or less) had a higher prevalence of identity theft than persons in other income brackets (Figure 8).

Recent studies (Bradford, 2013) report that individuals who use the Internet for banking, and/or e-mailing/instant messaging are more likely to be victims of identity theft than others. Similarly, online shopping and downloading increases victimization risk. The results of *WPIvs* show that the victimization risk increases with the number of electronic devices owned and prolonged Internet use (Figure 9).

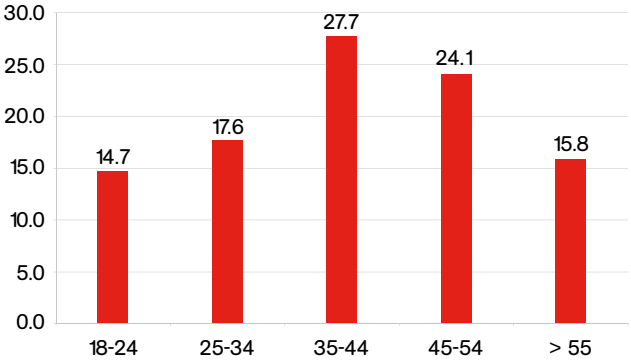
[10] 'Social risk perception' refers to what respondents think is the likelihood of citizens suffering an ID theft. In order to measure the social risk perception, the survey posed the following question: "Do you think that people should be worried about the risk of suffering an identity crime?".

[11] 'Individual risk perception' refers to what respondents think is the likelihood of themselves suffering an ID theft. In order to measure the individual risk perception, the survey posed the following question: "In the past 12 months how much have you thought about possibly being the victim of an identity theft?".

Figure 2 – Percentage distribution of respondents who reported having been victims of identity theft during their lives by gender (n=345)

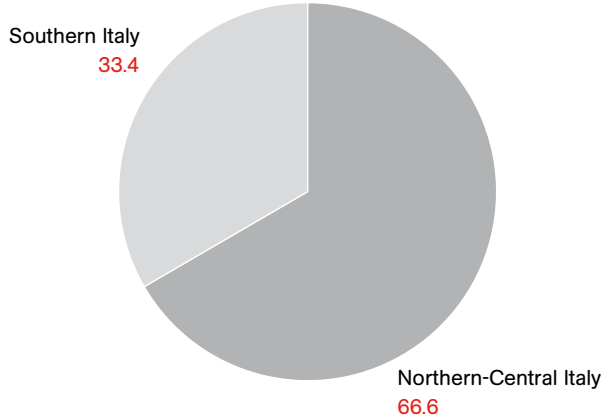
Source: WEB PRO ID victimization survey 2013

Figure 3 – Percentage distribution of respondents who reported having been victims of identity theft during their lives by age class (n=345)



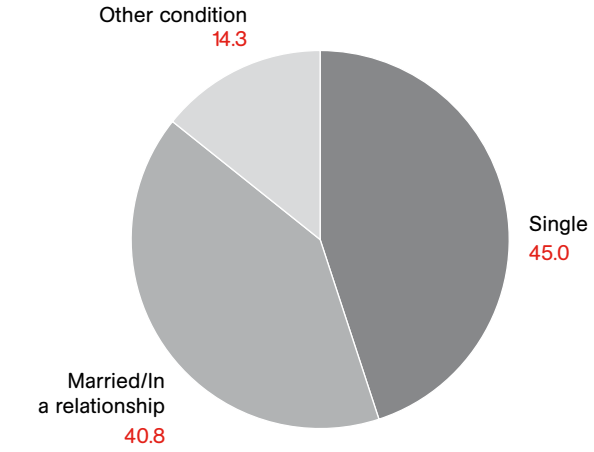
Source: WEB PRO ID victimization survey 2013

Figure 4 – Percentage distribution of respondents who reported having been victims of identity theft during their lives by area of residence (n=345)



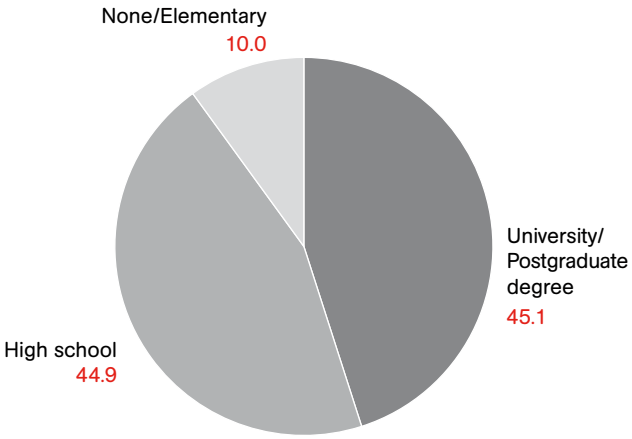
Source: WEB PRO ID victimization survey 2013

Figure 5 – Percentage distribution of respondents who reported having been victims of identity theft during their lives by marital status (n=345)



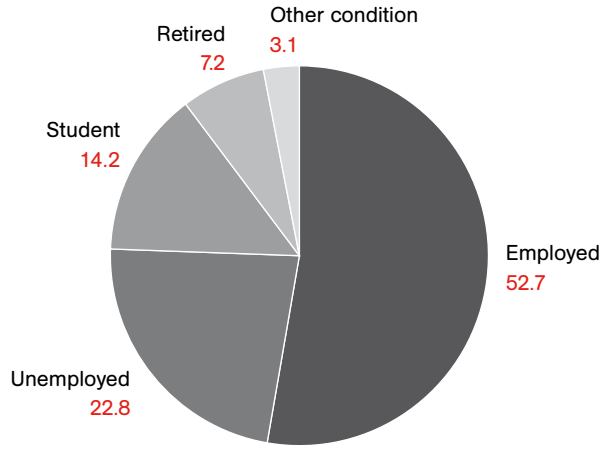
Source: WEB PRO ID victimization survey 2013

Figure 6 – Percentage distribution of respondents who reported having been victims of identity theft during their lives by educational level (n=345)



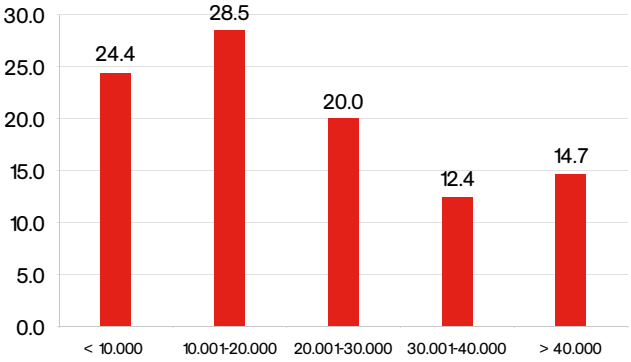
Source: WEB PRO ID victimization survey 2013

Figure 7 – Percentage distribution of respondents who reported having been victims of identity theft during their lives by occupation (n=345)



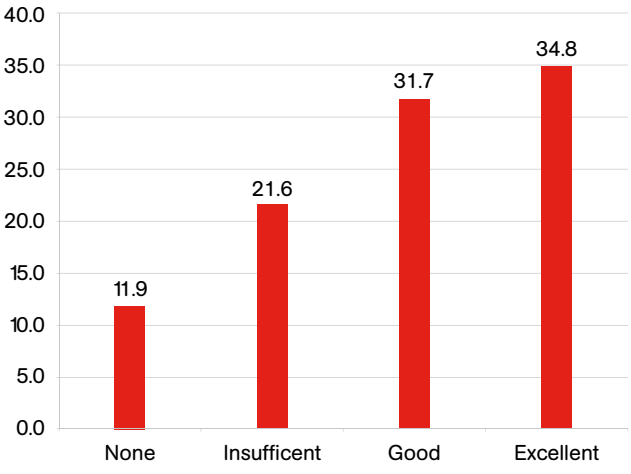
Source: WEB PRO ID victimization survey 2013

Figure 8 – Percentage distribution of respondents who reported having been victims of identity theft during their lives by income bracket (n=345)



Source: WEB PRO ID victimization survey 2013

Figure 9 – Percentage distribution of respondents who reported having been victims of identity theft during their lives by use of Internet (n=345)



Source: WEB PRO ID victimization survey 2013

A victim profile, as emerged from *WPIvs*, is presented below at Table 2.

Table 2 – The victim profile that emerged from the WEB PRO ID victimization survey

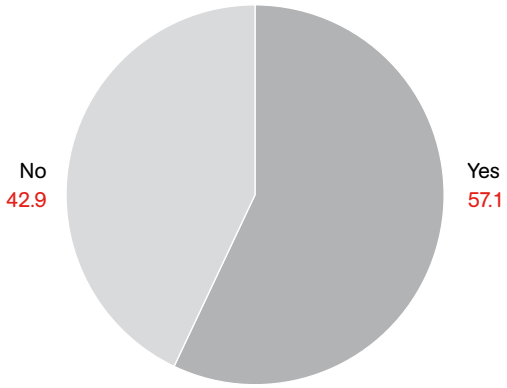
Feature	% among victims of ID theft
Male	60.8
35-54 years	51.8
Lives in the north-centre of Italy	66.6
Unmarried	45.0
Graduate	45.1
Employed	52.7
Frequent use of Internet for e-commerce/e-banking + possession of many electronic devices	34.8

Source: WEB PRO ID victimization survey 2013

6.3.2 Characteristics of ID theft

Identity thieves steal victim's information by various methods and for a variety of reasons, but primarily to facilitate a number of types of financial fraud. 57.1 per cent (191 cases) of the victims who responded to the questionnaire knew for what activities/crimes their personal data had been used (Figure 10).

Figure 10 – As regards the last identity theft that you suffered, do you know for what criminal purpose your personal data were used? Percentage distribution (n=334)



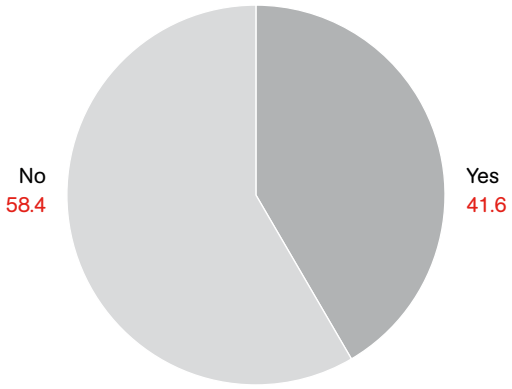
Source: WEB PRO ID victimization survey 2013

Identity theft is not only the assumption of someone else's identity, it is also the fraudulent use of her/his credentials and financial information. Fraudulent use of someone else's payment card is a very common type of identity theft. Once someone has the ability to use another person's identity, the most likely things that they will do are:

- create false documents (identity card, health insurance card / tax code) – 32 cases
- request one or more personal loans, financing or mortgage – 28 cases
- buy one or more goods (cars, electronic / computer goods) – 23 cases
- sign one or more contracts (e.g. telephony, rental) – 23 cases

Identity theft can be committed using a wide variety of techniques. Whilst it is not a new phenomenon, the development of technology, particularly the Internet, has enabled the development of many new techniques and made identity theft more prevalent. Establishing one's real identity for online transactions is more complex than it is in a face-to-face transaction, so that fraud becomes easier. This subsection describes some of the main ways in which identity theft is committed. About 42 per cent of identity theft victims (128 cases) knew how the offender had obtained their information (Figure 11).

Figure 11 – As regards the last identity theft that you suffered, do you know how your personal data were obtained? Percentage distribution (n=308)



Source: WEB PRO ID victimization survey 2013

The most common online scam is phishing: the sending of a fake email supposedly from a person's bank requesting a return email with personal information to update security details (28 cases). Phishing involves the use of deceptive emails or mirror websites, which look like the websites of legitimate businesses, intended to obtain users' personal information. A common example is an email pretending to be from a bank, asking customers to give their account details.

Nevertheless, identity data are frequently stolen from Facebook (or other social networks) profiles (27 cases). Offenders make increasing use of social networking sites to commit identity theft. Owing to the amount of personal information posted on social networking sites, identity thieves often gather details about victims which they use, for instance, to hack into bank accounts. Furthermore, Facebook users are duped into surrendering personal information through fake posts that solicit "likes", votes, or link clicks. Messages have been found which lead to a page that asks users for contact details (like a phone number), and since these links are believed to be sent by a "friend", the receivers trust them and end up becoming victims.

Two other techniques commonly used to obtain personal data are the theft of wallets (26 cases) and malicious software (22 cases) installed on the victim's computer without his/her knowledge or consent. The programs that collect personal information are typically spyware or keyloggers. This type of software is specifically designed to search for personal information.

More than 35 per cent of the victims reported that they had discovered the crime after at least one week. And about one in five detected the crime after more than a month (Figure 12). Nevertheless, in the United States, for instance, the situation is worse: some studies report that the average amount of time that elapses before discovery of identity misuse is 14 months (Federal Trade Commission, 2001). One study found that 24 per cent of its surveyed victims did not discover the crime until more than two years after the original misuse of their information (Foley, 2003). Some victims had been unaware of the misuse for as long as five years (Federal Trade Commission, 2001).

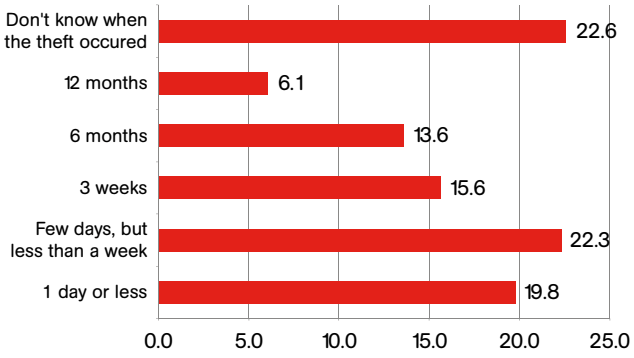
At the time of the survey, 79.5 per cent of the identity theft victims interviewed had resolved all problems associated with the incident. The majority of the identity theft victims had spent a few days but less than one week in dealing with associated problems, while about 11 percent had spent more than a month. Finally, a fifth of the victimized respondents reported that at the time of the interview they were still experiencing problems associated with the identity theft. Victims who spent more time solving problems related to ID theft were more likely to experience difficulties with work or personal relationships and severe emotional distress than were victims who solved their problems quickly. Among the identity theft victims who spent 1 month or more solving financial and credit problems due to the theft, more than 56 percent of them experienced severe emotional distress, compared to 21 percent who spent a day or less.

A victimization survey can be used to estimate the 'dark figure' of crimes. This expression refers to the amount of offences that occur but are not reported by the victims to the law enforcement agencies. This indicator assumes great importance because it makes it possible to gain a more accurate and comprehensive representation of the crime. 47.4% of the ID crime victims surveyed had reported the crime to the police, while the majority of them (52.6%) had decided for various reasons not to report the crime suffered (Figure 13).

The most common reason why identity theft victims report an incident to the police is so that the criminal can be caught (55.9 per cent). The next two most common reasons related to the LEAs: 53.1 per cent reported out of a sense of moral/social duty; 40 per cent to obtain closer control by the police. The next two reasons related to the goods stolen: about 37 per cent of victims reported in order to avoid payment of goods/services not requested, and about one in four to recover the goods/money stolen (Figure 14).

52.6 per cent of the identity theft victims surveyed had not reported the incident to the police and they cited a variety of reasons for not doing so. The most common reason was that the victim was afraid of some kind of retaliation (33.3 per cent). About one third (30.9 per cent) of the non-reporting victims had not contacted the police because they had suffered no monetary loss or no goods had been stolen. One in five non-reporting victims did not an insurance, and 17.3 per cent were discouraged by the police from reporting the crime (Figure 15).

Figure 12 – How much time passed until you discovered the theft? Percentage distribution (n=306)

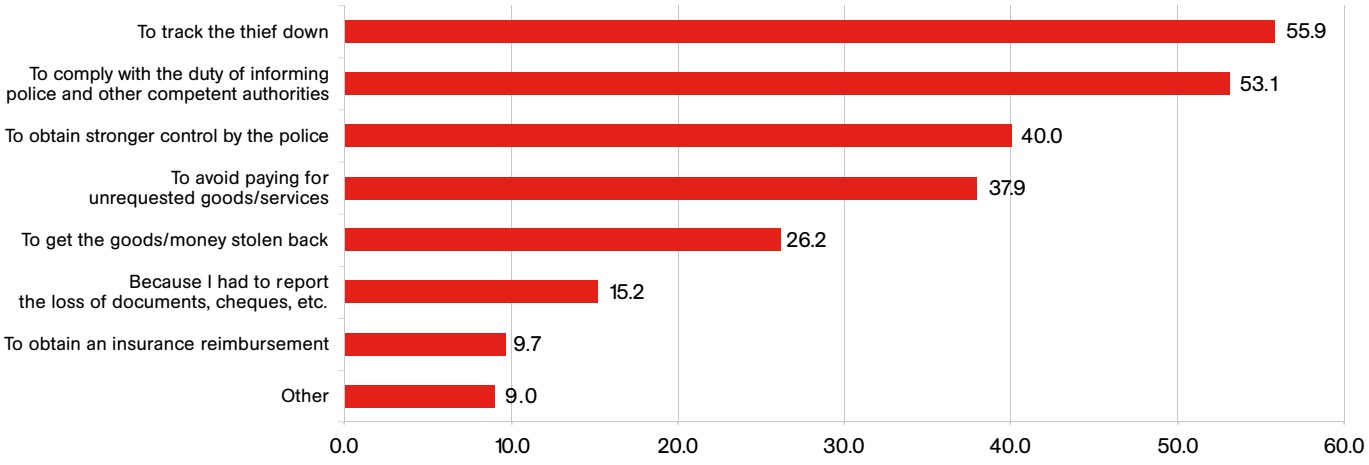


Source: WEB PRO ID victimization survey 2013

Figure 13 – Did you report the theft to the police? Percentage distribution (n=307)

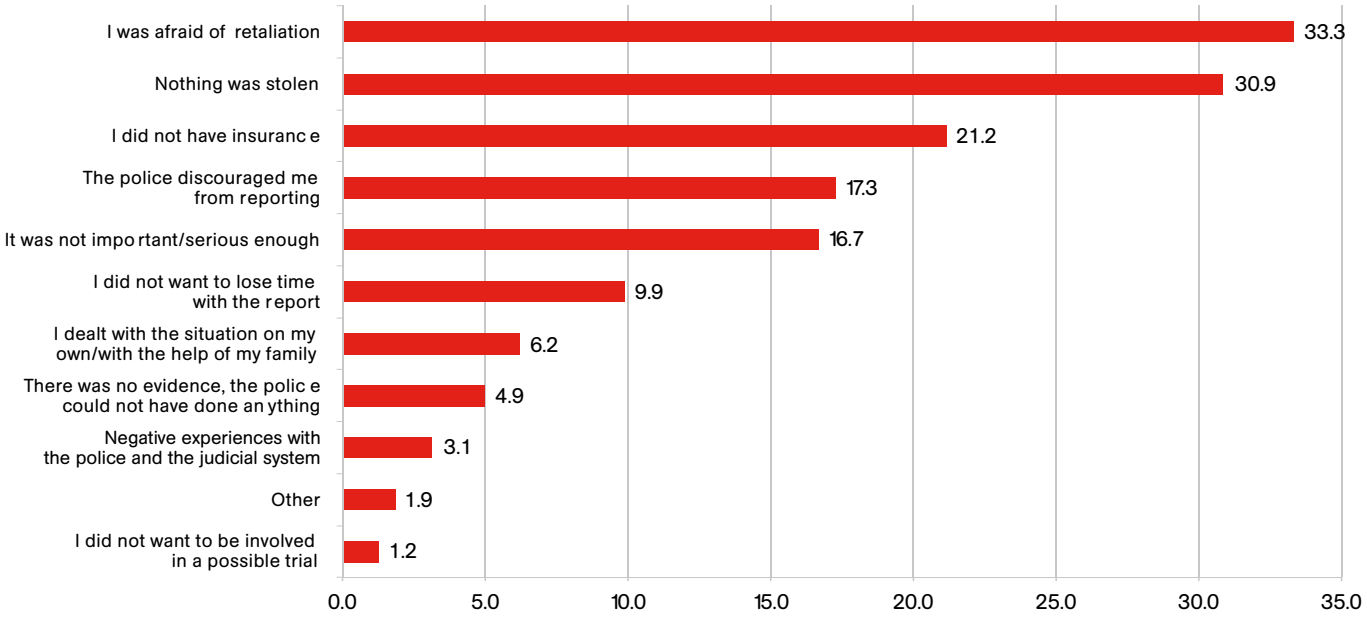
Source: WEB PRO ID victimization survey 2013

Figure 14 – For what reason(s) did you report the theft to the police? Percentage distribution (n=145). Multiple response



Source: WEB PRO ID victimization survey 2013

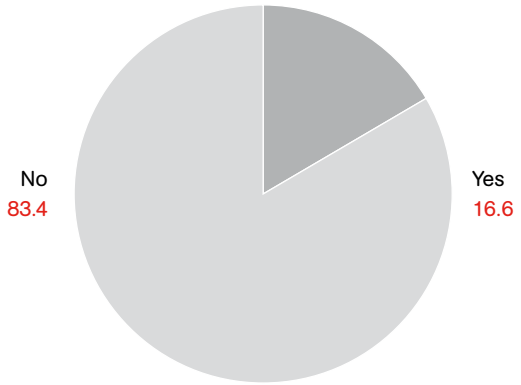
Figure 15 – For which reason(s) did you not report the fact to the Police? Percentage distribution (n=162). Multiple response



Source: WEB PRO ID victimization survey 2013

Not surprisingly, given the nature of ID theft, many victims know nothing about the offenders, and what they known may be inaccurate or misleading. Even when information is available, there is no indication of the basic socio-demographic characteristics of offenders. In detail, the vast majority of the identity theft victims interviewed (83.4 per cent) knew nothing about the identity of the offender (Figure 16). Only in 50 cases was the criminal's identity known, and the crime involved a single perpetrator, Italian, and unknown to the victim. Owing to the limited number of cases, this result cannot be generalized and should be considered as purely indicative.

Figure 16 – As regards the last identity theft that you suffered, were the perpetrators discovered? Percentage distribution (n=300)



Source: WEB PRO ID victimization survey 2013

6.3.3 Perception of and social insecurity about ID thefts

While criminal activities can have direct impacts on victims, they also have a wider indirect impact on individuals and society through the "fear of crime". This is a concept that has been defined and measured in a variety of ways including concern about crime, perceived risk of victimization, perceived threat and behavioural responses to fear (Roberts, Indermaur, & Spiranovic, 2013). The *WPIvs* measures fear of crime mainly through two indicators:

- Do you think that people should be worried about the risk of suffering an identity crime? (social risk)
- In the past 12 months how much have you thought about possibly being the victim of an identity theft? (individual risk)

Table 3 shows the comparison between the two indicators. Almost all of the respondents stated that citizens should be concerned about the risk of identity theft, while at individual level, the risk was much more mitigated. In fact, 37 per cent of the sample had thought frequently about the possibility of being victim of an identity theft over the past 12 months.

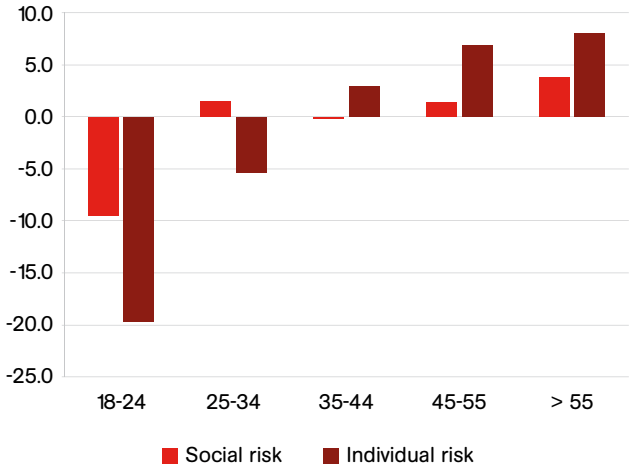
Table 3 – Comparison between social and individual perceived risk. Do you think that people should be worried about the risk of suffering an identity crime? (social risk); In the past 12 months how much have you thought about possibly being the victim of an identity theft? (individual risk). Percentage distribution

	Social risk	Individual risk
Yes[12]	93.1	37.0
No[13]	6.9	63.0
Total	100.0	100.0
N	2,096	2,094

Source: WEB PRO ID victimization survey 2013

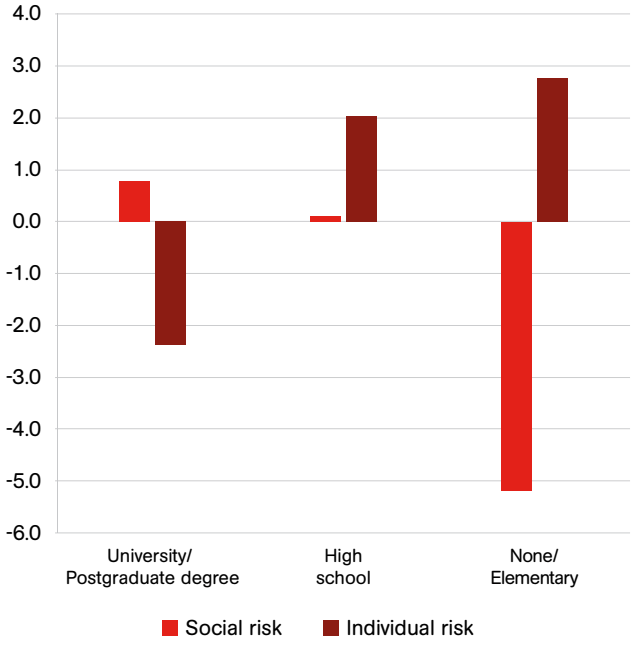
In terms of both social and individual risk, there was no significant difference between men and women. However, in regard to age classes, seniors more frequently feared being victims of identity theft, especially on a personal level, and they expressed less fear with regard to the perceived social risk. Young respondents (18-24 years) had a different attitude: they were less concerned in general and even less involved at the individual level of perceived risk (Figure 17). This was confirmed when taking occupational status into account: students, in fact, showed a level of perceived social and individual risk lower than the average, while retired people seemed more worried about suffering an identity theft, and they considered it a major social problem. In regard to educational level, significant differences are apparent, especially for respondents with a low level of education: they perceived a higher individual risk level than did respondents with a higher level of education, even though they were less victimized (Figure 18). Different results are observed in terms of marital status: single persons were the most victimized, but as far as perceived individual risk is concerned, they presented a level lower than the average value. Conversely, married/in a relationship persons and those in other conditions (divorced/widowed) seemed more insecure (Figure 19).

Figure 17 – Comparison between social and individual perceived risk. Do you think that people should be worried about the risk of suffering an identity crime? (social risk) (n=2,096); In the past 12 months how much have you thought about possibly being the victim of an identity theft? (individual risk) (n=2,097). Differences in percentages compared to the average value by age class



Source: WEB PRO ID victimization survey 2013

Figure 18 – Comparison between social and individual perceived risk. Do you think that people should be worried about the risk of suffering an identity crime? (social risk) (n=2,096); In the past 12 months how much have you thought about possibly being the victim of an identity theft? (individual risk) (n=2,094). Differences in percentages compared to the average value by educational level

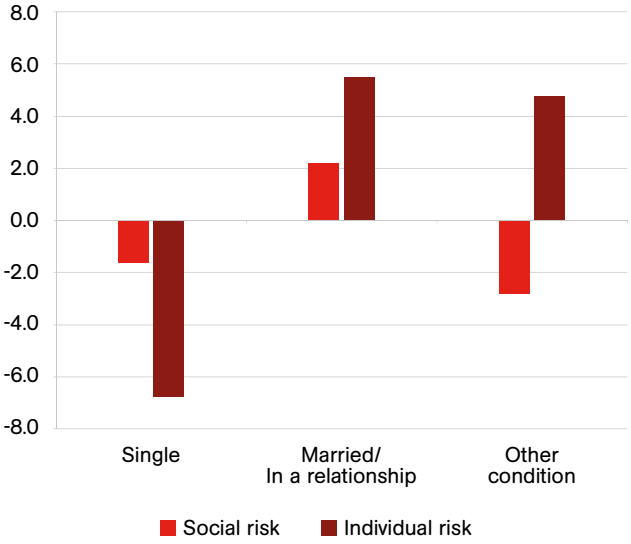


Source: WEB PRO ID victimization survey 2013

[12] Category "Yes" aggregates the answers "a great deal" and "somewhat" to the question: "In the past 12 months how much have you thought about possibly being the victim of an identity theft?".

[13] Category "No" aggregates the answers "little" and "nothing" to the question: "In the past 12 months how much have you thought about possibly being the victim of an identity theft?".

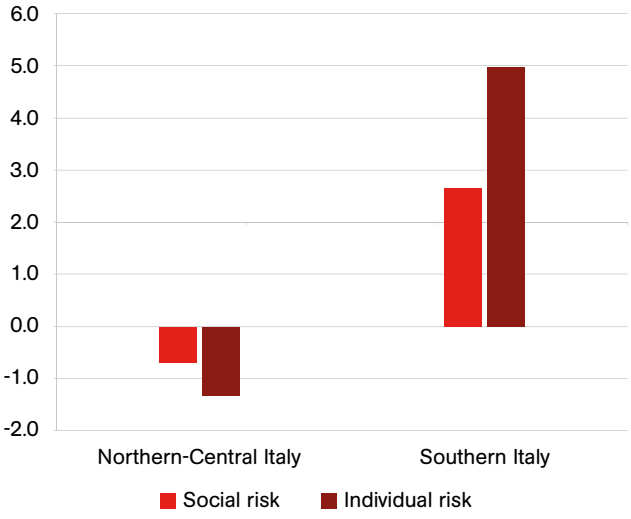
Figure 19 – Comparison between social and individual perceived risk. Do you think that people should be worried about the risk of suffering an identity crime? (social risk) (n=2,095); In the past 12 months how much have you thought about possibly being the victim of an identity theft? (individual risk) (n=2,095). Differences in percentages compared to the average value by marital status



Source: WEB PRO ID victimization survey 2013

With regard to the area of residence, respondents living in Southern Italy were the most worried, and they presented a greater sense of insecurity at both individual and social level (Figure 20). This result does not correspond to a higher probability of being a victim of an identity theft, since respondents living in Central and Northern Italy were the most victimized.

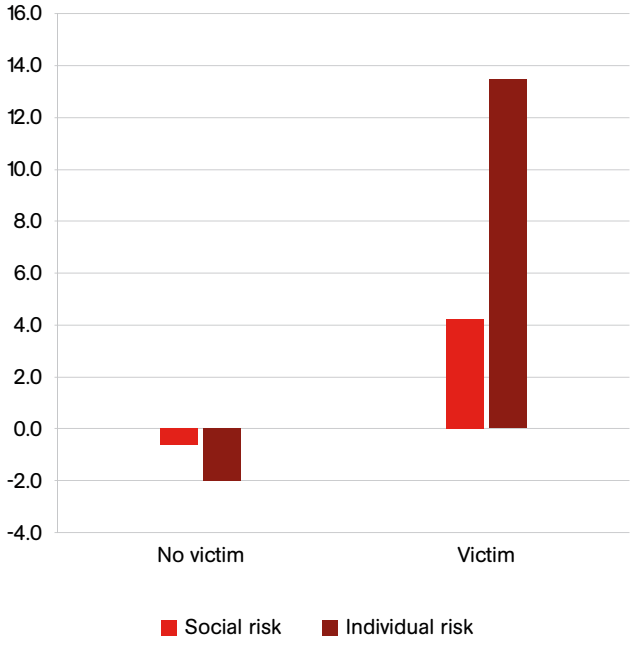
Figure 20 – Comparison between social and individual perceived risk. Do you think that people should be worried about the risk of suffering an identity crime? (social risk) (n=2,094); In the past 12 months how much have you thought about possibly being the victim of an identity theft? (individual risk) (n=2,095). Differences in percentages compared to the average value by area of residence



Source: WEB PRO ID victimization survey 2013

As confirmed by other surveys (Hasselm, 2011), victimization heightens the fear of crime and the perception of insecurity: as Figure 21 shows, those respondents who had suffered an ID theft presented a level of insecurity, at both individual and social level, greater than the average values recorded.

Figure 21 – Comparison between social and individual perceived risk. Do you think that people should be worried about the risk of suffering an identity crime? (social risk) (n=2,095); In the past 12 months how much have you thought about possibly being the victim of an identity theft? (individual risk) (n=2,095). Differences in percentages compared to the average value by victimization



Source: WEB PRO ID victimization survey 2013

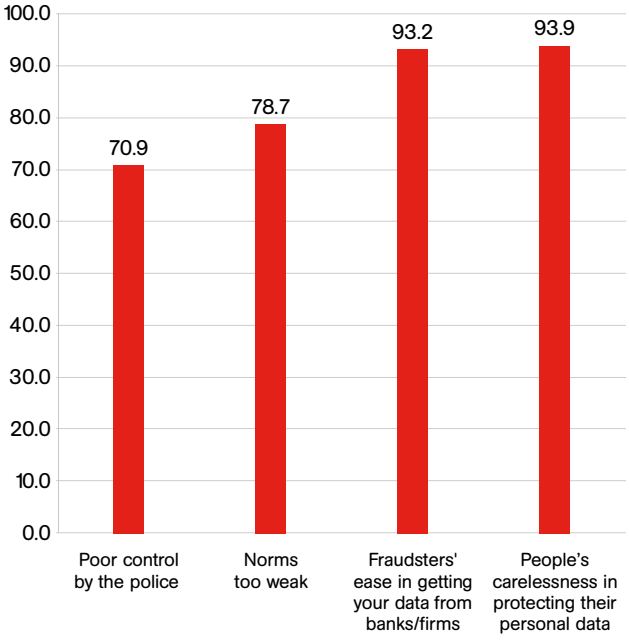
6.3.4 Risk factors

This subsection presents the results relative to the respondents' perception of victimization risk factors. This perception has no relationship with the socio-demographic characteristics of the respondents, but it is strictly related to victimization/non-victimization.

According to the results, the vast majority of the interviewees indicated as risk factors both carelessness in protecting personal data by citizens and inadequate data protection by companies. Besides this aspect, the respondents also highlighted the inadequacy of institutional measures. In detail, 78.8 per cent of the sample claimed that penalties are too moderate and 70.9 per cent cited insufficient control by LEAs (Figure 22). As a consequence, a preventive approach aimed at protecting people and businesses from identity thefts is crucial. However, it should be borne in mind that the

perception of the risk factors varied greatly according to the victimization/non-victimization status of the respondents (see below).

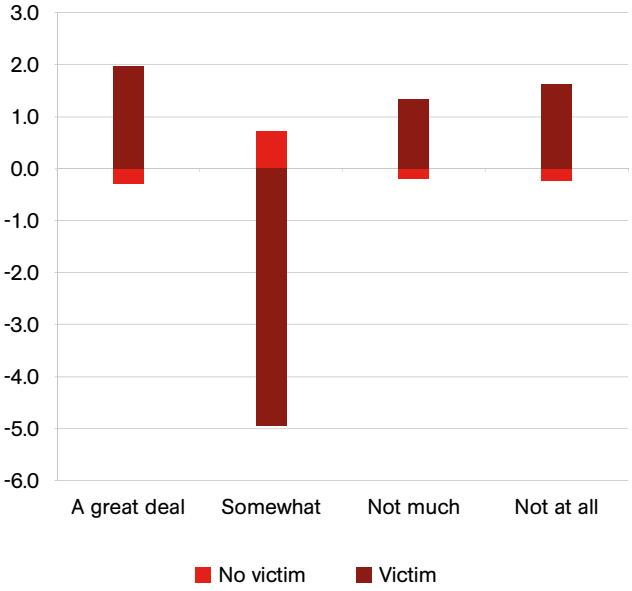
Figure 22 – To what extent do you think that the following factors increase the risk of identity theft? (Answers: A great deal/Somewhat). Percentage distribution (n=2,272). Multiple response



Source: WEB PRO ID victimization survey 2013

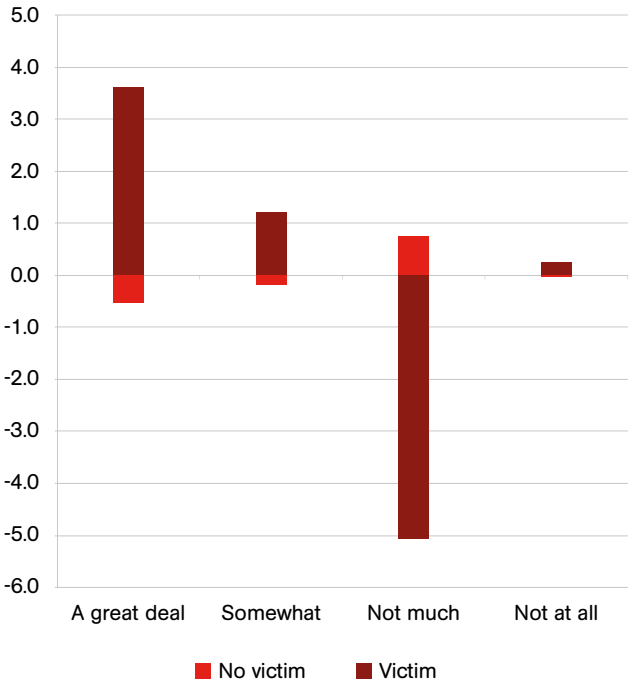
The *WPIvs* shows that victimized and non-victimized persons have quite different risk perceptions. In fact, respondents who had suffered an identity theft at least once in their lives considered as much more significant external social factors such as lack of control by law enforcement, moderate law/penalties, and inadequate protection of personal data by companies. By contrast, compared with the average value, they considered the people's carelessness in protection of their personal data as less risky (Figures 23-26).

Figure 23 – To what extent do you think that lack of control by law enforcement increase the risk of identity theft? Differences in percentages compared to the average value by victimization (n=2,079)



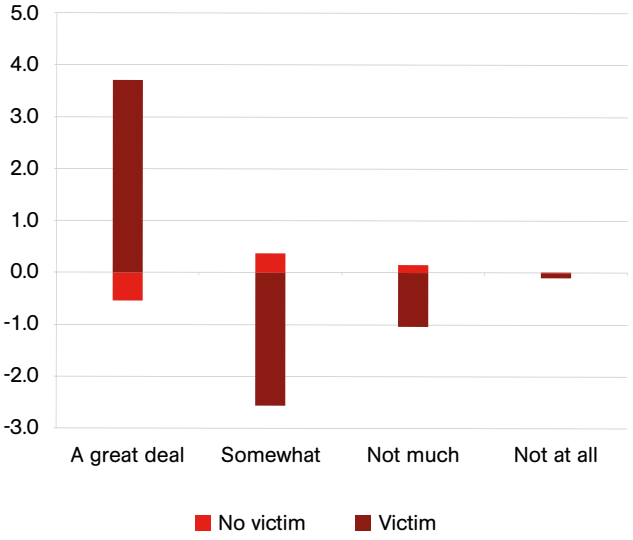
Source: WEB PRO ID victimization survey 2013

Figure 24 – To what extent do you think that too moderate law/penalties increase the risk of identity theft? Differences in percentages compared to the average value by victimization (n=2,078)



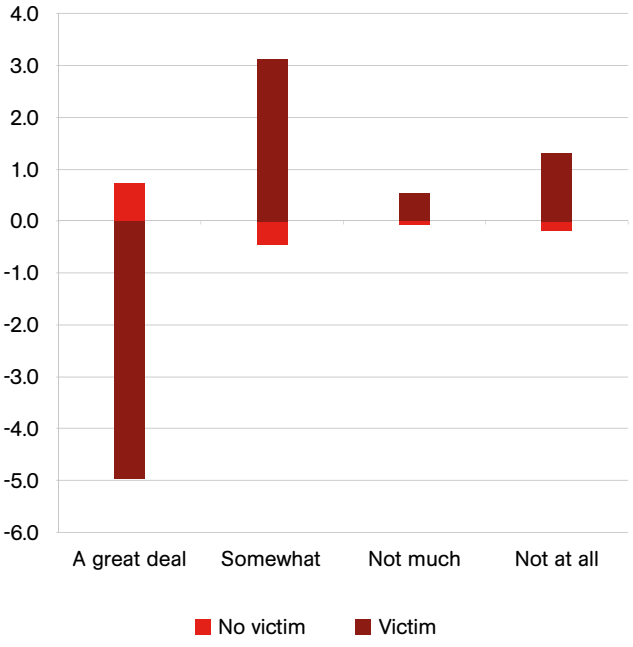
Source: WEB PRO ID victimization survey 2013

Figure 25 – To what extent do you think that the inadequate protection of sensitive data by banks/agencies, etc. increase the risk of identity theft? Differences in percentages compared to the average value by victimization (n=2,086)



Source: WEB PRO ID victimization survey 2013

Figure 26 – To what extent do you think that people's carelessness in protecting their personal data increase the risk of identity theft? Differences in percentages compared to the average value by victimization (n=2,078)



Source: WEB PRO ID victimization survey 20133.6 Survey results: public intervention

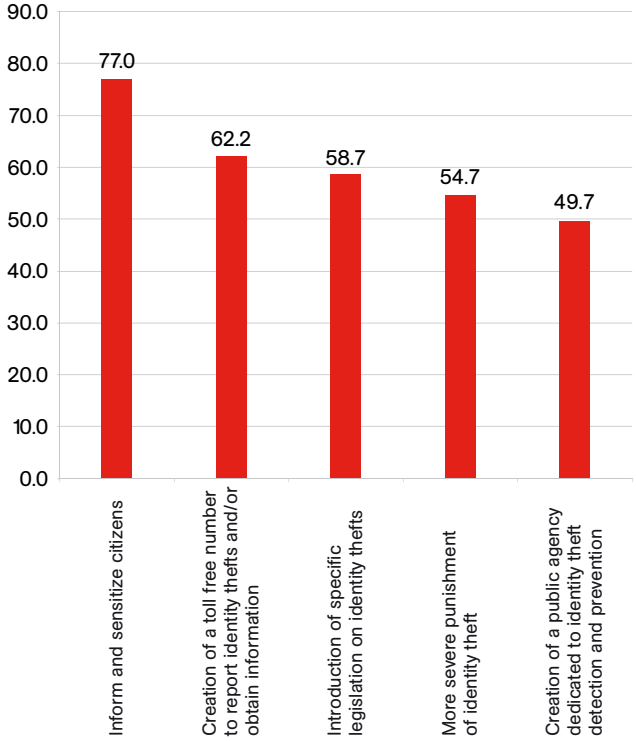
6.3.5 Public measures

Among the most significant risk factors, respondents indicated the inadequate protection of personal data by citizens. In this regard, not surprisingly, they also wanted public measures aimed at fostering prevention, above all through information and awareness campaigns, as detailed in Figure 27 and here below:

- create information and awareness campaigns for citizens (77.0 per cent);
- create a free number to report ID crimes and/or to advise citizens (62.2 per cent);
- create specific norms against the ID theft (58.7 per cent);
- increase the penalties for ID theft (54.7 per cent);
- create a public authority for the prevention and fight against ID theft (49.7 per cent).

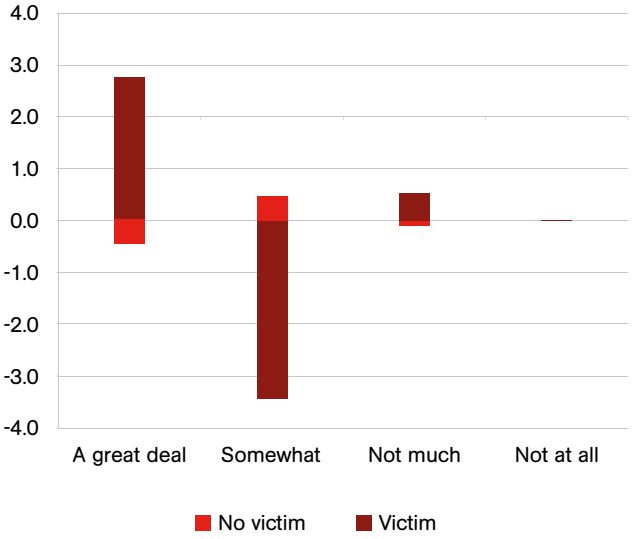
Public interventions varied between the victimized and non-victimized respondents. Compared to the average value, the latter indicated as priorities the creation of a toll free number to report identity crimes and/or to advise citizens; the creation of a public authority for the prevention and fight against identity theft, and the creation of specific norms against ID theft aimed at increasing citizens' protection (Figures 28-31).

Figure 27 – To what extent do you think the following measures should be a priority in protecting citizens? Percentage distribution (n=2,272). Multiple response



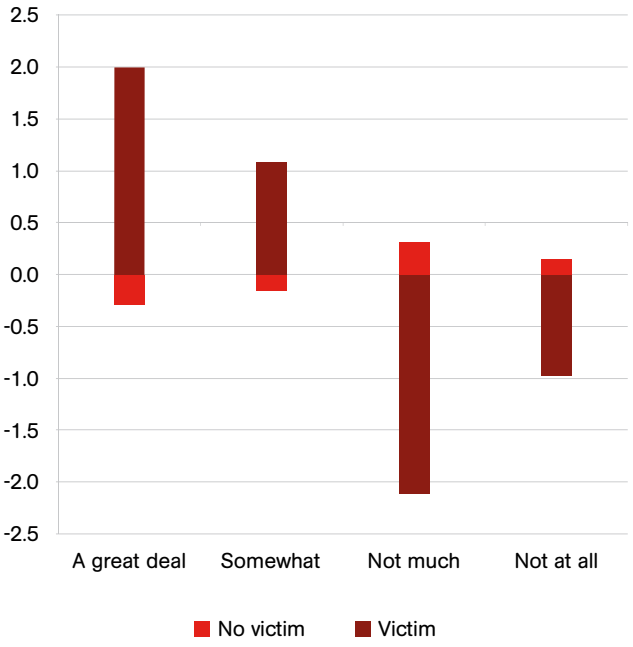
Source: WEB PRO ID victimization survey 2013

Figure 28 – To what extent do you think the creation of a public authority for the prevention and fight against identity theft should be a priority in protecting citizens? Differences in percentages compared to the average value by victimization (n=2,077)



Source: WEB PRO ID victimization survey 2013

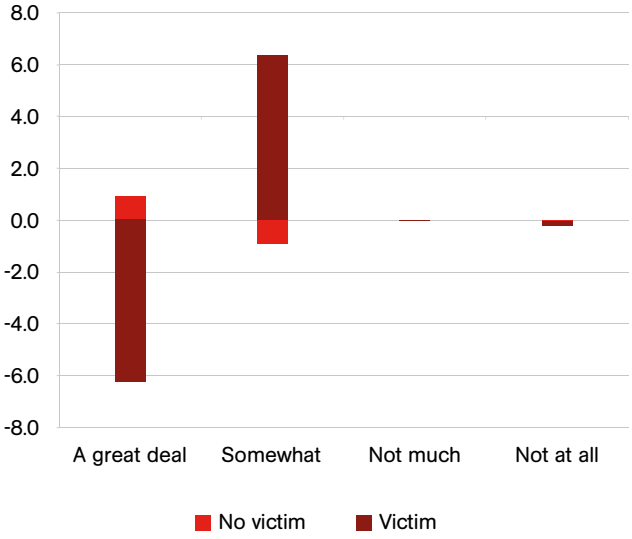
Figure 29 – To what extent do you think the creation of specific norms against identity theft should be a priority in protecting citizens? Differences in percentages compared to the average value by victimization (n=2,078)



Source: WEB PRO ID victimization survey 2013

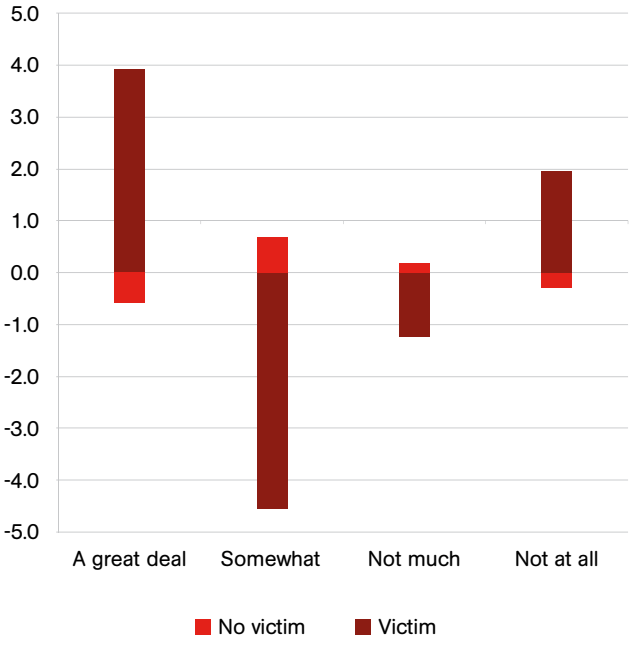
Somewhat surprisingly, those respondents who had suffered an identity theft considered interventions aimed at informing citizens to be less urgent (Figure 30). This result seems to indicate a certain distancing from the phenomenon of victimization: public actions seem to be perceived as extraneous to the victim, thus not causing any kind of protective behaviour to avoid identity crimes.

Figure 30 – To what extent do you think people's information and awareness on identity theft should be a priority in protecting citizens? Differences in percentages compared to the average value by victimization (n=2,078)



Source: WEB PRO ID victimization survey 2013

Figure 31 – To what extent do you think the creation of a toll free number to report ID theft/to advise people should be a priority in protecting citizens? Differences in percentages compared to the average value by victimization (n=2,077)



Source: WEB PRO ID victimization survey 2013

6.4 Legal remedies and policies to prevent identity crimes

According to the results of the *WPIvs* and backing upon measures taken by a number of countries against ID crimes (McNally & Newman, 2008), some suggestions for legal remedies and policies can be made. Some general rules that could/should be followed to create a first set of counter-measures pertain to situational crime prevention techniques (D. Cornish & Clarke, 2003) to reduce the opportunities for ID crimes. Specifically, the results of *WPIvs* suggest possible measures that could be adopted for each of the five categories envisaged by Cornish and Clarke (2003, p. 90), as listed below.

1) Increase the effort required to commit an ID crime. For example, increasing citizens' awareness about ID thefts, so as to make such crimes more difficult/expensive to commit and therefore less appealing to offenders.

2) Increase the risks of getting caught. For example, introducing specific norms on ID thefts (when not present), as well as improving police knowledge and efforts to deploy effective counter-strategies.

3) Reduce the rewards that result from the crime. For example, introducing and/or increasing protection-of-sensitive-data techniques in companies (banks, agencies, etc.) in order to conceal final targets such as credit card numbers.

4) Reduce behaviour that may encourage or otherwise tempt offenders. For example, deploying systems and awareness-raising campaigns to foster the protection of personal data by citizens and by companies so as to avoid an undue exposure of personal data that can "tempt" ID fraudsters to commit their offences.

5) Remove excuses that offenders may use to justify their crime. For example, reminders that certain types of behaviours are illegal, campaigns to raise citizens' awareness of ID crimes in order to spread the idea that identity is a valuable asset that should not be abused.

In addition, public measures should also have strong educational and awareness aspects. They should target broad audiences including consumers, key employees in the public and private sectors, as well as LEAs. An analysis of the challenges being faced suggests that efforts to combat ID crimes have three key aspects:

- *prevention*, i.e. actions that stakeholders can take to reduce the risk of identities being stolen (e.g. ways to enhance identity security, ways to identify attempts and instances of identity theft, and ways to limit the magnitude and scope of incidents);

- *deterrence*, i.e. actions that stakeholders can take to discourage criminals from committing an ID crime (e.g. legal sanctions).

- *recovery and redress*, i.e. actions that stakeholders can take to facilitate recovery and redress of such harms as financial detriment, injury to reputation, and other non-monetary harms (OECD, 2008a).

Finally, given the strict connection between ID crimes and the Internet, some specific policies should be deployed to prevent online ID crimes. More in detail:

- collecting more reliable data on online ID crimes, their trends, their *modi operandi*, their damage;

- creating specific information/awareness programmes and disseminating the related materials;

- strengthening the tools intended to protect personal data (e.g. data integrity rules);

- developing new tools to detect ID crimes automatically and share information about them.

6.5 Summary of the results of the victimization survey

General figures
15% of the sample had suffered at least one ID theft in their lives, 25% were multivictimized
Victim profile
Male, 35-54 years old, unmarried, resident in Northern - Central Italy, high education level, employed, low income (< 20,000 euros, owner of a number of electronic devices, frequent user of the Internet for e-commerce/in-banking
Characteristics of the ID theft
Data are obtained through: "phishing" emails, Facebook/social networks, wallet theft, malicious software
Stolen data used to: create false documents, request loans, mortgages, etc., buy goods, sign a contract
Consequences of ID theft: 35% of victims discovered the ID theft after at least one week, 79.5% took a few days to resolve the problem, 56% experienced severe emotional distress
Reporting to the police: 47.4% of ID thefts were reported to the police to track down the perpetrator, out of a sense of moral/social duty, to obtain more control by police, to avoid paying for unrequested goods/services, to recover goods/money loss
Not reporting to the police: 52.6% of ID thefts were *not* reported to the police because of fear of retaliation, no monetary loss, nothing was stolen, no insurance, police discouraged the victim from reporting
Perpetrators of ID theft
83.4% unknown
When the perpetrator was known (only 50 cases): single perpetrator, Italian, stranger to the victim
Perceptionof and social insecurity about ID thefts
93.1% of the respondents thought people should be concerned about the risk of suffering an ID theft
37% of the respondents thought "much" or "somewhat" about the possibility of suffering an ID theft
Respondents who most feared being victimized: elderly, married, low education level, resident in Southern Italy. All of them were actually **less** victimized compared to other categories
Respondents who least feared being victimized: young, single, high education level, resident in Northern and Central Italy. All of them were actually **more** victimized compared to other categories
Risk factors according to respondents
People's carelessness in their protecting personal data
Inadequate data protection by companies
Penalties too mild
Lack of control by LEAs
Victimized respondents considered as most the significant risk factors: lack of control by LEAs, penalties too mild, inadequate data protection by companies
Non-victimized respondents considered as the most significant risk factors: people's carelessness in protecting their personal data
Necessary public actions according to respondents
Information and awareness campaigns for citizens
Free toll number to report ID crimes and/or advise citizens
Specific laws against ID theft
More severe penalties
Creation of a public authority for prevention and fight against ID theft

07

Mara Mignone

ID crimes against companies: the web data collection module to collect case studies on IDRC against businesses and related results

Similarly to the situation detailed above (Chapter 6), also the knowledge about ID crimes suffered by companies is fragmented and largely superficial.

In order to fill this gap, one of the aims of project WEB PRO ID[14] was to develop a web-based data collection module on identity-related crimes against businesses, innovative methods and tools (i.e. based on the web) to facilitate data collection on ID crimes suffered by businesses, and its application. This aim was achieved through the creation and implementation of web modules allowing the collection of information on case studies from some of the companies partner of the project to outline the structure, prevalence, and features of such offences committed against companies.

The chapter is organised as follows: a foreword (section 7.1), the presentation of the results of the qualitative analysis of case studies in the mobile communication sector (section 7.2), the analysis of legal framework and remedies at International and EU level (section 7.3). The chapter concludes with a summary of the results (section 7.4).

7.1 Foreword

Although ID crimes against service-providing companies have been around for a long time and have become a significant phenomenon, their real dynamics and tendencies are still not yet well-known.

Recently, at international level, more and more attention has been focused on the economic-financial crimes and the internal and external frauds. Studies have been carried out and periodically updated, allowing to assess, supervise and deeply analyse in quantitative and qualitative terms the companies' exposure to criminal risk.[15] Regardless of individual data and potential methodological objections, these initiatives took credit for having contributed to focus the attention on the company as a crime victim, in contrast to the general perception of the company as a crime perpetrator.

However, the types of crimes connected to the violation of identity – real or fictitious – still remain in a cognitive limbo affected by issues of definition that have never been solved (both on the criminology and regulatory level), due to the complexity of drawing a clear line

[14] Specifically, objectives 1.2, 1.5 and 2.1 of the project.

[15] Among the others: PWC, Global Economic Crime Survey 2011; KROLL, Global Fraud Report 2012/2013 and Global Fraud Report 2013/14; KPMG, Who is the typical fraudster?, 2012; Home Office, 2012 Commercial Victimisation Survey, 2013; Javelin Strategy, Javelin Strategy Report 2013, 2013.

between traditional crimes and IT crimes, but also of assessing the real exposure to the victimization of each company and of different economic sectors.

The study activities carried out within the Project WEB PRO ID on a case sample provided by mobile phone companies allowed to collect some central structured information needed to develop the main features of the current scenario from a criminology point of view.

In phenomenological terms, the clear predominance of identity theft over identity fraud, the centrality of document falsification, and the ease and speed in committing fraudulent schemes are just some of the common features that clearly emerged in both of the analysed companies.

Along with the development of an initial knowledge base, it was possible to identify limitations and problems related to the type and relevance of the collected data on the one hand, and to the internal and external factors affecting prevention and fight against criminal risk on the other hand. These aspects are extremely interdependent and crucial in reducing crime chances.

7.2 Qualitative analysis of case studies in the mobile communication sector

The ID crimes against the mobile phone companies can be briefly described as "simple" in their *modus operandi*, but pervasive in terms of effect and damage since they are repetitive and restricted within a very limited time frame. In other words, they manifest themselves as serial crimes, committed in a continuous time, exploiting the vulnerabilities related to the business needs of companies (in particular to the speed required for the service activation in order to meet the market needs) and, at the same time, the inevitably longer timetable of fraud prevention and control activities.

This time dilation does not depend only on procedures and tools used in preventing subscription fraud and more in general in preventing criminal and operational risks, but it is also a direct consequence of the limitations imposed on phone company operators by the Italian Privacy Law. In fact, the prohibition of accessing and using some of the data related to natural and legal persons represents an obstacle in adopting countermeasures able to promptly protect from any ID crimes not only the company but, indirectly, also the citizens who could be unaware victims of identity theft in a phone contract transaction.

The potential relevance of ID crimes and their upward trend, as well as the vulnerability of the mobile communication sector, had already emerged in the first Italian Victimisation Survey about ID crimes, a study carried out by the ALIAS[16] Project, coordinated by UCAMP (Central Office for Payment Instrument Fraud Prevention of the Ministry of Economy) and undertaken in collaboration with RiSSC.

The results of that research showed an ID crime impact of 2.66%, where 0.56% was related to credit frauds and 2.10% to payment cards frauds. Considering the credit frauds, 86% of the ID thefts concerned the signing of a contract using the victim's name, while only 14% was related to the purchase of goods in instalments. However, none of the victims had indicated the illicit use of their personal data in order to obtain a mortgage or a loan/financing.

Those data pointed out a displacement from banking and financial field towards economic sectors like the phone companies and others providing services with deferred payment, which in those days were less ready to manage the criminal risk than the credit institutions.

7.2.1 Criminal dynamics: the predominance of ID theft

As emerged from the qualitative analysis[17], the updated picture of the current situation confirms the continuing vulnerability of the mobile communication sector to ID crimes and poses even more clearly the problem of protecting phone companies but also citizens.

In fact, the cases provided by two mobile companies have confirmed the prevalence of *impersonation* and, therefore, the predominance of the ID thefts against natural or legal persons (existing or existed) over the ID frauds, which use fictitious or real identities, but altering them. The identity theft was represented by the

[16] ALIAS Project. Enhancing public-private cooperation on ID theft and payment card fraud. Co-financed by the European Commission under the Prevention of and Fight Against Crime Programme of DG Freedom, Security and Justice (JLS/2007/ISEC/533). The victimization analysis was carried out on a representative sample of 2,519 people, submitting a questionnaire with CATI methodology. The survey investigated on ID theft with the purpose of credit frauds and payment card frauds.

[17] The sample was composed of 413 cases equally provided by two project partners (here on also referred as "Company 1" and "Company 2"). Due to the sensitivity of the information provided, the name of the companies are not indicated. The cases were related to period from December 2010 to August 2013. The collection of information was carried out using an online form available on the website of this Project with restricted access. Data are aggregated and reported anonymously in order to safeguard confidential information.

75% of the cases analyzed by the survey and the most part of them did not involve a natural person as victim, but a legal one (87%).

This finding focuses the attention on the *company ID theft* phenomenon, which has been marginally described in recent literature compared to the victimization of citizens. Moreover, not only does it highlight how one can easily access business information, but more over how one can so straightforwardly use them to commit subscription frauds.

Furthermore, the fact that the victimized companies are mostly corporations (40%) suggests a rational choice by fraudsters, who are aware of the longer time used by these organizations in identifying the crime suffered because of their complex structure and consequently in reconstructing facts and reacting to protect themselves. And in many cases, the understanding of a crime like the company ID theft can be slowed down by the lack of awareness and knowledge of this phenomenon.

However, a significant difference does exist between the two companies analyzed in the survey in terms of exposure to the risk of an ID theft and especially the one concerning the legal person: this difference can be related to many factors, such as target users, business policies, offers and promotions of products, but also to the systems used to detect and prevent fraud during the activation stage. This confirms that the opportunities for crime are often pertaining to the choices of the company itself. In fact, in the case of Company 1, the ID theft and fraud values are, respectively, 67% and 33%. Considering the ID theft, in 95% of cases the victims are legal persons and, only marginally, natural persons. In the case of Company 2, the ID theft and fraud values are, respectively, 84% and 16%, while the ID theft values affecting companies and natural persons are respectively 80% and 20%.
In other words, Company 1 may find more difficult, at least in an initial stage, to classify the different types of ID crime, but it can focus on preventing its business customers, who are the most suffering victims of identity theft.
Company 2 is helped in classifying identity-related crimes by the clear predominance of ID thefts over frauds, but it must invest its efforts on monitoring activation services concerning to both legal and natural persons.

The two companies find even more complex to detect victimization because of the speed of criminal schemes due to *impersonation.* In fact, in 65% of cases the duration of the criminal act did not go over the calendar month. To further confirm the speed that characterizes the *modus operandi*, there is the fact that the longer the cases last, the more drastically they reduce: only 2 cases showed a duration of between 6 and 12 months.

The main purpose of the identity theft is the misappropriation of the cutting-edge terminals, especially smartphones (40.8%), but also mobile phones (13.3%), tablets (10.6%). On average, for each case 4.7 devices were stolen. These are assets with a strong social attraction, easily resalable and highly gainful, which will inevitably attract criminal attention.

However, the phone frauds in the strict sense represent a small number of cases, equal to 17% of the analyzed sample, also because they are more complex and require a higher expertise. This category includes, among others, the ability to make phone calls without bearing their cost, the possibility of taking advantage from the sale of call traffic, especially to premium rate numbers at the international level (the so-called International Revenue Share Fraud), and the opportunity to obtain SIM cards for the resale of call traffic.

Considering the perpetrators' profile, the analyzed cases did not reveal the presence of a real risk of internal frauds, committed with the connivance of one or more employees. Even the criminal risk related to the connivance of the dealers appears to be marginal in fraud cases (3.1%). Therefore, it is possible to assume that some individuals or organised groups are able to find by themselves information about identity and/or income of natural and legal persons, and to proceed with the signing of contracts. However, the specific environment of perpetrators isn't yet so well-known because, in 63.3% of the analyzed cases, the phone company operators have failed to say whether or not they have identified fraudsters. In addition, a further 9% represents the cases where it is certain that the perpetrator hasn't been identified.

In terms of *modus operandi*, identity theft is associated with the falsification of documents, which is instrumental and crucial for committing contract frauds. The documents used by fraudsters are totally counterfeit (47.3%), stolen (36.3%) and, less often, the original ones that have been altered (14.1%). For altering the original documents, online sensitive data are used too. Because of the lack of detailed information, knowledge on the types of document is still limited. Where it has been pointed out, the most vulnerable documents are identity card, fiscal code number/health insurance card and VAT certificate. While the first two are official documents that have security features designed to protect the originals, making the falsification more complex and recognizable, the VAT registration certificate is a paper document with any security protection. There-

fore, it can be easily reproduced in a very accurate way and used for fraudulent purposes.

Knowledge of the falsification of documents related to identity theft is still incomplete, concerning not only the types of documents, but – as a consequence – the quality of them.

Usually, in contractual arrangements the perpetrators ask for the activation of a new contract (89%) instead of changing an existing and effective one. Generally, this request is made by a new customer (85.9%), and therefore assigned to some records "unknown" to the company. It is a technique that, from the fraudster's point of view, allows to limit the risk to be identified, because identity data are not recorded in business systems and the phone company operators still have a very few possibilities to check personal information in real time and with certainty.

The channels used for signing contracts are mainly physical, in store or with dealer (31%) and in agency (26%). Internet has a marginal role because it is not yet used by mobile phone companies for all types of contracts.

7.2.2 Criminal dynamics: the main features of ID frauds

Identity frauds represent almost a quarter of the analyzed sample (24.7%), where the use of a false identity is predominant (63.7%) compared to the use of an identity that is real but altered in some of its main features[18] (35,3%).

Considering the *modus operandi*, identity fraud differs from identity theft and seems to have better defined boundaries.

First of all, it consists almost entirely of requests made by new customers (95%), with the purpose of signing a new contract (96%). In addition, these cases focused exclusively on the misappropriation of devices and not on the potential profits of the phone fraud related to the national and/or international call traffic. On average, 5 devices are stolen for each case and they are mostly smartphones or Iphones and tablets.

Therefore, this is about circumscribed and basically simple criminal offenses that require a rather low level of criminal expertise and may be committed serially.[19] They are based mainly on a good reliability of the information and personal documents provided during the signing of the contract. In fact, in those cases where a feedback has been given, the quality of documents was considered high. Moreover, in most cases the fraudulent episodes are fast, lasting less than a month, and focused on specific targets. Unlike the identity theft, the most used channels are the agencies.

With regard to the perpetrators, the case studies showed that they are mainly outside the companies (85.3%), excluding the possibility of a collusion between employees/agents/dealers and professional criminals. Apart from this figure, the missed identification of perpetrators still remains significant (41.2%), as well as the lack of knowledge about their personal information (31.4%).

7.2.3 The company's perspective: investigation and prevention activities and challenges for the future

The companies suffering identity-related crimes are especially affected by the economic point of view. For the mobile phone operators, the analysis of case studies has assessed the average loss due to ID theft as being between 2,000 and 3,000 Euros, except for some individual cases that even reach a value between 20 and 35 thousand Euros. The same dynamic can be seen in identity fraud, albeit with smaller amounts. In fact, the maximum loss, connected to individual cases, ranges between 10 and 15 thousand Euros.

However, these crimes can also have a strong reputational impact, mostly related to the media exposure that such a case may have. For instance, this could happen when the phone fraud is used against a bank or an insurance agency, or is related to a more complex situation like the economic organised crime and the terrorism. The World Bank (2008) itself highlighted the risks that the cutting-edge phone services may determine, acting as "facilitators" in the money transfer for illegal purposes.

Therefore, it is essential that the response of mobile phone operators to the risk of identity-related crimes, in terms of prevention, investigation and contrast, will be based on the promptness, efficiency and predic-

[18] The personal data that are more vulnerable to alteration and change are the first and/or last name, the VAT number, the fiscal code number and, less often, the residence address and the last figures of the identity card.

[19] That is the case of an Egyptian 22-year-old boy, who was proven to be involved in at least 15 cases of ID fraud.

tion ability criteria. These elements are crucial in order to compete in the market and, at the same time, to protect oneself from a complex phenomenon, characterized by several constant attempts that often occur simultaneously in various geographic sites and in fast-fading cases.

However, there are significant obstacles, both internal and external, that affect the companies' performance. Concerning the outer limits on the one hand, the above-mentioned Privacy Law caused a considerable setback in determining the self-protection policies. The inner limits, on the other hand, are represented by both human and procedural/instrumental factors. Some of the issues related to the fraud prevention are the predominance of marketing and promotion policies over the fraud prevention ones, the difficulties in managing territorial networks, the constant inability to check in an effective way, the documents provided by people signing a new contract or changing a previous one, the unawareness of one's own vulnerability and the lack of a preventive knowledge of the previous cases' main features. Moreover, in many cases the economic/business and legal logics predominate over the safety needs, because the safety itself is often perceived – even by the top management – not as an essential added value, but as a limit to the business development.

Currently, the activities carried out by companies to deal with the risks related to ID crimes do not differ significantly depending on whether they are thefts or frauds. However, these two phenomena have some distinctive features that should orientate the prevention choices.

In the case of identity theft, for example, the crime detection takes place both through the control systems (53.1%) and the analysts' activities (37.9%). The report from the dealer or the victim, who is the legitimate identity holder, only occurs in 4.5% and 1.6% of cases, respectively. In 1% of cases, the ID crime is detected thanks to the Police Force or bank reports.

In the case of identity fraud, however, the analysts' work is crucial, as shown by approximately 72% of cases. The general alarms of control systems detect the ID frauds in the 23% of cases, while the remaining 5% represents the detection by dealers.

In terms of business criticality, which turns into criminal opportunities, the identity theft seems to be related mainly to the human factor. In more detail, the failure to carefully examine the documents provided during a request of a contract is crucial (71%).[20] The 18% of cases has proved a suspected fraudulence or an intentional responsibility of the dealer. However, the intrinsic vulnerability of the channels or promotions used for contract signing/activation is marginal (9%). A very limited number of cases has also shown the carelessness of institutions or individuals affecting by ID theft (2%).

However, the identity fraud has a different scenario, which is more fragmented and has coexisting problems concerning the documentation analysis (51%) and criminogenic factors inherent to both the commercial offers (16%) and the Internet channel (12%). Furthermore, the 21% of cases has also shown a suspected fraudulence of the dealer. The resulting consideration is, therefore, that identity fraud is much more related to the opportunities that, directly or indirectly, are determined by company itself through its choices. The ID fraud definitely has a marginal size compared to the decision-taking centres and the fraud prevention activities themselves. The correlation among the intermediary (e.g. dealer or agent), the vulnerable offer and the failure to check the personal documents is a extremely strong chain that can easily turn into serial frauds, very well planned and therefore difficult to be promptly detected.

In operational terms, the response of companies to the detection of ID theft or fraud cases is divided into a number of actions, which are complementary to each other.

In the case of identity theft, the first and the most common response is the suspension of the contract and, if possible, the recovery of goods associated with the verification of the customer's information (84%). Very often, after this stage there is a unilateral dissolution (60%). The personal records are then included in a black-list (43%) and the IMEI number is blocked or even included in a black-list (27%). The decision to proceed with a complaint to the Police Force, however, is marginal (5%), as well as the application of disciplinary measures for the dealers involved in the fraud scheme (8%).

In the case of identity fraud, the procedure includes, once again, the suspension of the contract and the verification of the customer's information (83%), often followed by a unilateral dissolution (52%). In 65% of cases, the personal records are included in a black-

[20] It includes the following options: "failure to check the documents" (66%), "failure to check the documents with a nonstandard signature" (4%) and "failure to check the documents that are not in accordance with the procedures" (1%).

list and in 60% of them the same happens to the IMEI number. The distinguishing element is the complaint to the Police Force, which occurs in 18.6% of cases. The explanation may be connected to both the lack of the injured party (unlike the case of identity theft, which involves a natural or legal person) and the more detailed information collected by analysts while checking the data. The greater knowledge of the criminal dynamics could justify the choice of more disciplinary measures for the involved dealers (16.7%).

At last, as a result of almost all cases of both ID theft and fraud, the companies said they had taken further and specific preventive measures, based on the analysis of risks and *modi operandi*.

According to the survey's results, the most critical features, which seem to have a radical impact on the companies' response to the threat of identity-related crimes, may be:

- the failure to take a clear position against the frauds - not just the identity ones - that damage the company, from the inside as from the outside. A zero-tolerance policy, turning into initiatives for the exposure and into choices for the risk reduction, is a discouraging tool that should not be underestimated. In fact, a company that "aligns" itself against the criminal risk is perceived as more dangerous by a potential fraudster, who is rationally led to choose other "safer" alternatives;
- the actual difficulties in identifying customers with certainty, with respect to the information provided and the identity and income documents. In particular, this critical aspect is related to the previously-mentioned laws, but also to the inaccessibility of public sources. In this sense, the Public system for the prevention on an administrative basis of frauds in the credit sector, with specific reference to ID theft (Legislative Decree of April 11, 2011, No. 64) should fill this gap, contributing to a drastic reduction of identity-related crimes;
- the still superficial knowledge of criminal dynamics and *modi operandi*, but also of the opportunities exploited to defraud the company. The information collected - or made available – allow to delineate the phenomenon only at a superficial level. There are insufficient details about the victims of ID theft, the perpetrators, the chain of behaviours supporting the criminal act and the correlation between cases, just to name a few. A general knowledge does not allow more extensive analysis and forecast of potential changes in the short or medium term, but above all it does not allow to convert the knowledge itself into targeted and organized proposals and initiatives to reduce the criminal risk.

7.3 Legal remedies

7.3.1 International and European legislation[21]

Despite the lack of globally-applicable criminal law standards, international and regional organizations have intensified their efforts to create a basis for international conventions aimed at improving international cooperation in preventing and/or prosecuting cases of identity theft. This topic has an important place in the crime prevention activity of the UN, and this issue has gained major importance, particularly in relation to organized crime and terrorism. The purpose of the UN in this field is to support its MS in preventing and prosecuting ID-related crimes, in adopting appropriate national legislation, and in improving MS' security systems and promoting international cooperation. Based on ECOSOC Resolution 2004/26[22] and ECOSOC Resolution 2007/20[23], the UN set up a group of experts working on ID-related crimes, and they published multiple studies on this topic (UNODC, 2013). Moreover, the importance of preventing ID-related crime is also emphasized in some UN resolutions, for example in the "Resolution on Strengthening the United Nations Crime Prevention" (UNODC, 2006), which recognizes identity crime as a major emerging threat.

There are also other international organizations working on this issue. One example is the Organization for Economic Co-operation and Development (OECD), which recognizes the importance of addressing identity theft because of the great damage this type of crime causes to the economy. In 1999, the OECD approved the "Guidelines for Consumer Protection in the Context of Electronic Commerce". The measures of those guidelines can be used mainly to prevent identity crime. However, they do not criminalize identity theft because they take the form of soft-law. The purpose of the Guidelines is to provide a framework and a set of principles to assist: i) governments in formulating and implementing consumer and law enforcement policies; ii) business associations, consumer groups and self-regulatory bodies by providing guidance to the

[21] Section in collaboration with Francesca Bosco, UNICRI.

[22] *ECOSOC Resolution 2004/26* on "International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes" quoted in: *UNODC*, Handbook on Identity-related Crime (2011), p. 38-41.

[23] *ECOSOC Resolution 2007/20* on "International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime", quoted in: *UNODC*, Handbook on Identity-related Crime (2011), p. 38-41.

core characteristics of effective consumer protection; iii) individual businesses and consumers engaged in electronic commerce (OECD, 1999). In 2003, the OECD developed the "Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders" (OECD, 2003), and similar to the 1999 Guidelines, they do not criminalize identity theft. They are intended as support for national agencies to help them improve their security system against fraudulent commerce. In 2008, the OECD published a "Scoping Paper on Online Identity Theft", which provides an analysis of different types of online identity theft. Moreover, it also deals with aspects related to the victims and to law enforcement schemes. This paper was an in-depth study requested by the Committee on Consumer Policy (CCP) in order to better understand the concept and the extent to which identity theft may affect consumers and users (OECD, 2008b). In 2008, the OECD also published "Policy Guidance on Online Identity Theft", which provides an overview of different strategies to combat online identity theft (e.g. education, collection of important data, data security, and electronic authentication) (OECD, 2008a).

The Council of Europe (CoE) is another international organization working on security issues. As a part of its "action against economic crime" agenda, the CoE recognizes the importance of preventing and fighting identity crime. However, it is important to mention the fact that the CoE categorizes identity crime in the more general category of cybercrime, due to the fact that ID-related crimes are increasingly committed by using new communication technologies.

In 2001, the CoE produced the "Convention on Cybercrime", also known as the Budapest Convention, which was initially signed by 30 countries. It serves as a guideline for any country developing comprehensive national legislation against Cybercrime and as a framework for international cooperation between State Parties to this treaty".[24] By 2014, 52 states had signed and 41 states had ratified the Convention.[25] The Budapest Convention is a very important document because it provides a global framework to fight cybercrime. Contrary to the soft-law character of the OECD Guidelines, the Budapest Convention criminalizes behaviour such as gaining illegal access to a computer system, illegal interception, data interference, system interference, misuse of devices, computer-related forgery and fraud, and other crimes committed online (child pornography, infringement of copyright and related rights). Moreover, the Budapest Convention provides tools for conducting efficient investigations, with the scope to apply them by means of a computer system and utilize any evidence in electronic form. Some examples of investigative tools provided by the Budapest Convention include: procedural safeguards, preservation of stored computer data and partial disclosure of traffic data, production order, search and seizure of stored computer data, real-time collection of traffic data, and the interception of traffic data. The Budapest Convention is very important because it provides a framework for efficient international cooperation and because it coordinates legislation with other countries. The Convention provides for mutual legal assistance and other provisions for international cooperation on cybercrime. Particularly, the Convention introduces specific provisions for the expedited preservation of stored computer data, the expedited disclosure of preserved computer data, mutual assistance regarding accessing stored computer data and mutual assistance in the interception of traffic and content data.

In the EU, there is a general divergence of opinions about the political-criminal discourse regarding the issue of ID-related crime, and there is still the need for a clear definition of this phenomenon. In fact, there are still some MS in which there is no agreement on a legal definition of identity theft. However, there is a strong influence from the US and from international organizations pushing towards the criminalization of this identity theft. The EU itself, as supranational entity, is trying to make uniform the criminal legislation of MS on this topic (De Morales & Muñoz, 2009, p. 1f).

It seems that identity crime has become politically relevant since the beginning of 2000. The causes for this change of attitude towards ID-related crime were on the one hand the increase in the use of new technologies, and on the other hand the terrorist attacks of September 11, 2001. The terrorist attacks and the large-scale global economic loss for financial entities and losses for citizens, led the EU to deal more seriously with the problem. At the beginning, the phenomenon of identity theft was mainly analyzed in relation to the financial sector and to new technology. Another focal point of these first approaches was studying the link between identity crime and organized crime. It should be noted that in this first phase the EU did not recognize the need to criminalize identity theft as a separate form of crime; it rather supported the adoption of preventive measures to avoid fraud, in particular in the financial sector. In 2001 this legislative proposal was approved under the Treaty of Amsterdam in the form of a frame-

[24] Council of Europe, Action Against Economic Crime - Cybercrime: http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp (13.02.2014).

[25] Council of Europe, Convention on Cybercrime: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG (12.02.2014)

work decision (De Morales & Muñoz, 2009, p. 2ff). This framework decision did not make any mention of identity theft or identity fraud. Along with the definition of falsification of non-cash means of payment, the fight against computer crime was also introduced as a major priority. Until 2003-2004 there had been a dominant view that considered identity theft as an issue linked to other forms of crime, and because of this, it did not need separate attention. The "New EU Action Plan 2004-2007 to Prevent Fraud on Non-Cash Means of Payment" (Commission of the European Communities, 2004) changed this view, and identified this phenomenon as a separate form of crime. With this plan, the European Commission showed its willingness to analyze the problem in depth (De Morales & Muñoz, 2009, p. 2ff).

The Joint Research Centre[26] published in 2003[27] and in 2004 (De Morales & Muñoz, 2009, p. 2ff) two reports on identity theft, which referred to an increase of identity theft cases in the real and virtual worlds and claimed that there was an absence of appropriate legislation to deal with the problem. Moreover, these reports highlighted some of the most important questions related to identity crime, such as those concerning the damage done to the victim and the connections between identity crime and organized crime (terrorist attacks, trafficking of drugs, arms and human beings). In 2004 there was a change of leadership in the research and the Internal Market and Services Directorate General (DG)[28] assumed the direction of the research programs and worked together with the EU Fraud Prevention Expert Group (FPEG),[29] which consists of representatives of national banking systems and law enforcement agencies. As a result of the engagement of the FPEG, a "New Action Plan 2004-2007 to Prevent Fraud on Non-Cash Means of Payment" was adopted, which recognized the necessity in the EU to create comprehensive measures to deal with this problem (De Morales & Muñoz, 2009, pp. 4–7).

The idea of harmonizing criminal legislation amongst MS, of urging them to define identity theft as a crime and to adopt sanctions against it, was proposed for the first time at the "High Level Conference on maintaining the integrity of identity and payments"[30] held in Brussels in 2006 in the framework of the Action Plan 2004-2007. However, not all parties agreed with this idea of harmonizing criminal legislation regarding identity crime. Some participants (Germany) believed that the national legislation of MS was enough to deal with identity theft and other related crime. Subsequently, the Commission published the communication "Towards a general policy on the fight against cybercrime".[31] This is an important document because here identity crimes are defined for the first time as separate offences, and in addition, document calls for the explicit harmonization of MS legislation on identity crime. To this purpose, the Commission tried to lead all MS to criminalize identity-related crimes. However, a prior impact assessment showed that this harmonization would not be easy because of the different legal traditions and practices of MS. Therefore, the report initially suggested the use, by MS, of non-legislative measures. Criminal legislation would be harmonized only in the scenario that the previously adopted, non-legislative measures failed (De Morales & Muñoz, 2009, pp. 7–11).

Before the entry into force of the Treaty of Lisbon, the competences over the issue of identity crime were split, and they were not very clear: they were placed either under the First Pillar - former art. 95 TEC (actual art. 114 TFEU) - responsible for the good functioning of the internal market, or under the Third Pillar - former art. 31.1 e TEU - responsible for establishing basic rules against organized crime and terrorism. A decision for one of these two options would have made a great difference, not only in legal but also in procedural terms. The latest modification of the Treaty simplified the division of the competences, so that now the only possible legal basis would be art. 83 TFEU[32] (De Morales & Muñoz, 2009, p. 11f).

[26] For more information see: *Joint Research Centre*: http://ec.europa.eu/dgs/jrc/ (21.01.2014).

[27] Security and Privacy for the citizen in the post-September 11 digital age (2003), quoted in: *De Morales Romero*, From Nothing to Having It All? (2009), p. 2ff.

[28] For more information see: *DG Internal Market and Services*: http://ec.europa.eu/dgs/internal_market/index_en.htm (21.01.2014).

[29] For more information see: *EU Fraud Prevention Expert Group*: http://ec.europa.eu/internal_market/fpeg/index_en.htm (21.01.2014).

[30] *High Level Conference* on maintaining the integrity of identity and payments: http://www.google.it/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CDQQFjAA&url=http%3A%2F%2Feuropa.eu%2Frapid%2Fpress-release_SPEECH-06-730_en.pdf&ei=aIPeUtTeL0i6yAPd2IDQDg&usg=AFQjCNEfBqJvoSOcm0pBM4kJT0ofTAU4EQ&bvm=bv.59568121,d.bGQ (21.01.2014).

[31] Towards a general policy on the fight against cybercrime: http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/l14560_en.htm (21.01.2014).

[32] Article 83 (ex Article 31 TEU):
1. The European Parliament and the Council may, by means of directives adopted in accordance with the ordinary legislative procedure, establish minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension resulting from the nature or impact of such offences or from a special need to combat them on a common basis. These areas of crime are the following: terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime and organized

Actually, the most important instruments in Europe to prevent and to fight identity crime are the "Framework Decision on Attacks against Information Systems"[33] and the "Council of Europe Convention on Cybercrime" (Budapest Convention).[34] However, the conclusions of the European Council on the "Action Plan to Implement the Concerted Strategy to Combat Cyber-Crime" in 2010 also made an important contribution to the implementation of the cybercrime strategy. On the institutional level there have also been some improvements in harmonizing and coordinating amongst MS' international investigations against ID-related crime. A new centre has been established to deal with cybercrime and also with crimes related to identity theft. This centre is Europol's European Cybercrime Platform (ECCP), with the purpose to "facilitate the collection, exchange and analysis of information." On an operational level, the High Tech Crime Centre of the European Police Office (Europol) has been playing a key role in supporting on-going investigations. This Centre enables online crime specialists to provide more targeted and effective countermeasures in the areas of child sexual exploitation, payment card fraud and cybercrime – crime areas in which the internet plays a key role.[35] In 2010, Europol's Cybercrime Task Force was created with the aim to study operational and strategic issues on cybercrime investigations, prosecutions and cross-border cooperation to fight against different forms of cybercrime. The creation of all those departments should be regarded as a step toward a more effective and consistent approach to fight against identity theft and cybercrime in general at the EU level (Robinson, Graux, Parrilli, Klautzer, & Valeri, 2011, p. 34f).

Moving to the national sphere it is clear that states adopt different approaches to confront the problem of identity theft and ID-related crimes in general. However, most experts believe that the solution to this problem should combine legislative with non-legislative approaches, across both the public and the private sector. Legislative tools that can be implemented on the national level include: identity theft legislation criminalizing different types of misuse of personal data (France); legislation for the protection of personal data; regulations related to identity documents and numbers; general penal provisions with respect to fraud, forgery and usurpation of titles; regulations particular to a specific sector (organized crime, terrorism); and non-criminal regulations (administrative infractions). Non-legal measures include the use of public-private partnerships; hotlines and reporting centres; the collection of statistics; user awareness and reporting mechanisms; and technology to improve the security of identity infrastructure (Robinson et al., 2011, p. 35f).

Usually, states combine legislative and non-legislative measures. Contrary to the US and Canada, in the EU there are just few states that have adopted a specific law on identity theft or ID-related crime. The majority of EU MS use more general provisions in criminal law to prosecute this kind of crime. Some examples of countries with a specific provision for identity theft are Estonia, France, Portugal and Slovenia. However, even if these countries have a strong legislative approach to prosecute ID-related crimes, they often have weak enforcement mechanisms and a lack of reporting centres.

Non-legislative measures are used in many EU MS. Some countries like Ireland, the Netherlands and the UK have good reporting mechanisms, which on the one hand provide citizens with advice and support on internet-based crimes, and on the other hand, work as contact points to report online incidents. Romania also created a reporting mechanism in 2004, but it is no

crime. On the basis of developments in crime, the Council may adopt a decision identifying other areas of crime that meet the criteria specified in this paragraph. It shall act unanimously after obtaining the consent of the European Parliament. 2. If the approximation of criminal laws and regulations of the Member States proves essential to ensure the effective implementation of a Union policy in an area which has been subject to harmonization measures, directives may establish minimum rules with regard to the definition of criminal offences and sanctions in the area concerned. Such directives shall be adopted by the same ordinary or special legislative procedure as was followed for the adoption of the harmonization measures in question, without prejudice to Article 76. 3. Where a member of the Council considers that a draft directive as referred to in paragraph 1 or 2 would affect fundamental aspects of its criminal justice system, it may request that the draft directive be referred to the European Council. In that case, the ordinary legislative procedure shall be suspended. After discussion, and in case of a consensus, the European Council shall, within four months of this suspension, refer the draft back to the Council, which shall terminate the suspension of the ordinary legislative procedure. Within the same timeframe, in case of disagreement, and if at least nine Member States wish to establish enhanced cooperation on the basis of the draft directive concerned, they shall notify the European Parliament, the Council and the Commission accordingly. In such a case, the authorization to proceed with enhanced cooperation referred to in Article 20(2) of the Treaty on European Union and Article 329(1) of this
Treaty shall be deemed to be granted and the provisions on enhanced cooperation shall apply.
Consolidated version of the Treaty on the Functioning of the European Union. (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:115:0047:0199:en:PDF) (23.01.2014).

[33] *Framework Decision* on Attacks against Information Systems: http://europa.eu/legislation_summaries/information_society/internet/l33193_en.htm (21.01.2014).

[34] *Council of Europe* Convention on Cybercrime (Budapest Convention): http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (21.01.2014).

[35] For more information see: *High Tech Crime Centre of Europol*: https://www.europol.europa.eu/content/page/mandate-119 (21.01.2014).

longer in use. Finally, some EU MS have other forms of non-legislative measures; Belgium, Germany, Greece, Luxembourg, the Netherlands, Sweden, and the UK use public awareness campaigns to warn citizens against ID crime on the internet (Robinson et al., 2011, pp. 40–80).

7.3.2 Priority issues for EU and national institutions[36]

ID-related crimes and cybercrimes in general have been exploiting new information and communication technologies in order to find more efficient methods to steal identities and personal information of consumers. ID-related crimes have become a major concern for national governments and also for international organizations due to the large amount of damage and losses that they have caused the economy, particularly the banking/financial sector.

A first challenge for global policymakers concerns creating definition of ID-related crimes. In fact, there are many possible definitions that have been provided by governments and international organizations, but this is not a good starting point to create a legal provision. The lack of an agreement on the definition of ID-related crimes is responsible for two problems: it's difficult to estimate the true extent of the problem; and, this is also an obstacle to the international cooperation.

There are many different forms of identity crime, which operate in different sectors and with different purposes. Criminals may use different techniques to commit their crimes. There are traditional methods – like the theft of a wallet or of a laptop – and new methods which use internet technologies – like spamming, phishing, or sniffing.

The socio-economic profiles of both victims and offenders are very diverse. Regarding the victims, there is usually discrimination in terms of age and wealth. The offenders are usually young men coming from all socio-economic backgrounds; they don't need to have particular technical skills to commit ID-related crimes.

At the international level there are many approaches to prevent and prosecute this phenomenon. The UN has adopted many resolutions with the aim to lead states to improve their national legislation, their security systems and their level of international cooperation. The CoE has also made an important contribution by creating a convention with criminal laws provisions, while other organizations like the OECD have adopted soft-law guidelines.

The EU started dealing seriously with this topic after September 11, 2001, but in the early stages of the research, identity theft and fraud were not considered separate crimes and were studied only in relation to the financial sector. This situation changed in 2003 and 2004 when the Joint Research Institute published two reports on the increase in identity theft cases. These reports noted the lack of adequate legislation and addressed some important questions related to the damages incurred by victims and the link between identity crime and organized crime. The New EU Action Plan 2004-2007 identified identity theft and fraud as new, separate forms of crime. The standardization of legislation on cybercrime among all MS is not easy due to the different legal traditions and practices of each MS. In effect, the EU decided to initially adopt non-legislative measures to prevent cybercrime. On the institutional level, there has been some major progress: the creation of Europol's European Cybercrime Platform and Europol's Cybercrime Task Force was important in improving cross-border cooperation and coordinating international investigations.

The growing number of internet users and the spread of new technologies provide new opportunities for criminal activities, and traditional forms of crime (like identity theft, child pornography, drug trafficking, etc.) are increasingly moving to cyberspace, assuming a new dimension. There is also a need for employing more effective preventative measures, which include using both legislative and non-legislative tools. In this regard, it is important to reach an agreement on a common legal definition of ID-related crimes, and to set common standards and practices to coordinate international investigations. The prevention of and fight against ID-related crime should not only involve actors from government and international organizations, but also representatives from civil society. This public-private partnership should play more of a role in the prevention of identity theft and in the establishment of new channels of risk communication. This is essential in order to inform the public of the need to protect personal information and about the risks related to identity theft.

[36] Section in collaboration with Francesca Bosco, UNICRI.

7.3.3 The Italian case. The new Public system to prevent ID theft

At the national level, the focus of the institutions on the criminal risks related to ID crimes has resulted in two main initiatives, connected respectively to the payment cards and to the services that allow deferred payments.

Concerning the payment cards, the Law 166 of 2005 was a very important step in fight against fraud as it has instituted the *SIPAF – Electronic Payment Card Administrative Fraud Prevention System,* a structured prevention model whose implementation and management have been entrusted to UCAMP - Central Office for Payment Instrument Fraud Prevention of the Ministry of Economy and Finance.

The law was issued with the intent[37] to act with effective tools to strengthen the prevention and thus limit the extent and the level of danger of this phenomenon. In particular, the measure's aim was to establish a protection system able to operate at the national level, in terms of payment card fraud prevention and, at the same time, to help at European level the operating contact points concerning the transnational unlawful acts, according to the Council Framework Decision 2001/413/JHA, adopted on May 28, 2001, about the fight against fraud and counterfeiting of non-cash means of payment.

More in detail, the administrative prevention[38] has the task of:

- identifying the critical points in the security systems of the companies issuing payment cards;
- designing solutions, also through legislative acts, to eliminate them gradually, through a strong cooperation between public and private sector;
- establishing the minimum safety standards that the issuing companies must respect.

The reasons for the regulatory choice can be recognized especially in:

- the need to contain the phenomenon of payment card cloning;
- the need to ensure the confidence of citizens in the non-cash means of payment;
- the urgency to monitor the fraud phenomenon in order to assess its impact on the economic and financial system.

The choice to address the initiative not only to credit cards but also to debit cards was determined by the knowledge that the fraud prevention must be able to embrace both the payment instruments, since the fraudulent techniques used by organized crime to reproduce or clone debit cards are quite similar to those used for counterfeit credit cards; there are also similar inconveniences that may arise for cardholders and operators.

In accordance with the law, the element that has been considered crucial for prevention activities related to payment card fraud was the ability to promptly identify the potential risk factors, in order to limit as much as possible the fraud opportunities, protect citizens and market, and ensure the development of a cashless society.

There are two main instruments through which the above-mentioned Act tried to achieve this result: the so-called "Electronic Archive" and the "Working Group".

The Electronic Archive receives data from the companies that issue cards and from those that regulate the conventional points of sale (referred to as "reporting entities"), and consists of two information sections called respectively "DATA" and "INFORMATION".

The DATA include:

a) data identifying the points of sale and the legal representatives of merchants in relation to which the right to revoke the agreement governing the acceptance of payments cards has been exercised;
b) data relating to any counterclaim contract signed with the points of sale whose merchant agreement has been revoked;
c) data identifying transactions not recognized by the holders of the payment cards or reported by them to the judicial authorities;[39]
d) data relating to ATMs subject to fraudulent tampering.

INFORMATION include:

e) information related to the dealers and transactions vulnerable to the risk of fraud, involving both operators

[37] What stated here is illustrated in the annexed Report of the Government Bill, introduced on 14th July 2004 at the Chamber of Deputies.

[38] What stated here is explained on the website of Ministry of Economy and Finance-Department of Treasury, in the section called "Prevention of Payment Instrument Fraud" (http://www.dt.tesoro.it/it/antifrode_mezzi_pagamento/prevenzione_frodi_mezzi_pagamento/).

[39] In accordance to the principle of territoriality, the Archive also receives data of disputed transactions related to cards issued by foreign companies. In this case, the payment dispute is notified thanks to Visa and Mastercard worldwide networks.

and payment cards monitored by the reporting entity. The measure highlights the significant role of the data mentioned in a) and c), because they include both the merchant agreement revocation by reporting companies towards the dealers involved in irregular transactions, and the payment dispute notifications made by cardholders.

From the prevention point of view, these two types of information are closely related; in fact, thanks to the payment dispute notifications, points of sale where the operation was carried out irregularly can be identified. The intersection of these data with those concerning the merchant agreement revocation allows to achieve the goal of strengthening the security of the card accepting circuit. In fact, the companies accepting payment cards cloned or counterfeit or the companies representing a "point of compromise" in which the data of the card magnetic tape are captured, are removed from the circuit.

The consultation of the Electronic Archive data must allow to the individual reporting companies that provide its information to know all the transactions that occurred in a specific point of sale and have not been recognized by the cardholders.

A complete knowledge of these transactions allows to overcome a critical step in prevention activity, which is carried out individually by private entities such as the reporting companies; this criticality is due to the fact that each company can only detect an irregular transaction in relation to its payment cards, but it's unaware of the irregular transactions that took place in the same financial cycle with cards of other corporate issuers.

Considering that the law is based on the principle of liberalism (basically, except for the obligation to communicate the above-mentioned information and data, the reporting companies have no other restrictions), each company has still the option of keeping a merchant agreement contract with an operator that has already had its contract revoked by other companies; however, it being understood that the ability of the system to allow an efficient and prompt prevention from the reporting companies thanks to the consultation of the Archive data definitely increases along with the growing amount of the Archive information that can represent a real and imminent fraud risk - see the above-mentioned e) point.

In fact, according to the Article 3 of the Act, in the Electronic Archive there are also temporary information related to the points of sales and transactions for which the reporting companies have independently started a monitoring procedure to prevent a potential fraud risk.[40] The definition of "fraud risk" has been integrated in the implementing Regulations of the Act in order to match the thresholds of risk among the different reporting companies.

Obviously, the growth of the Archive's potential is determined by the ability to cross in every possible way all the available data and information when collecting them.

Considering its purposes, the Electronic Archive manifests itself as a technological tool that besides allowing an analysis of the economic and financial impact of the phenomenon, can be used for administrative prevention implemented by the Ministry of Economy and Finance.

With the aim of meeting the growing needs of knowledge and reaction to the phenomenon of fraud against payment cards and to its implications, the Archive is a tool that allows its owner – i.e. the Ministry of Economy and Finance, through UCAMP – to carry out an economic and financial analysis of this phenomenon in order to understand its dynamics, monitor its trend and predict its development, acting at the legal and administrative level, if necessary.

Regarding the administrative prevention, the creation of the Archive is complementary and synergistic with the prevention made by the Police Forces. It represents a basic element of a system that on the one hand meets the needs of the reporting entities to be protected by a common tool allowing the access to relevant operating information,[41] and on the other hand ensure the government's provision of a public interest service.

For the purposes of prevention, the information-sharing is one of the most significant elements and is also taken into account in the Archive structure. In order to ensure the in-depth analysis of the phenomenon, UCAMP can access the information collected in the database of the Central Bank (Banca d'Italia), containing information about stolen or lost payment cards. On the other side, this bank may ask UCAMP to aggregate the Electronic Archive data.

[40] Generally, the monitoring procedures are activated by the companies when the fraudulent activity of each operator reaches or exceeds certain thresholds of fraud risk, as well as the payment conditions of each card reach or exceed the previously-mentioned thresholds .

[41] Through the online consultation (each reporting company has an identification code to access the system), the members of this service can promptly know the facts (revocation of operators, disputed transactions, etc.) at the base of each reported information; secondly, thanks to the intersection of the data and information provided by the reporting companies, consulting Archive allows them to quickly locate any abnormal and fraudulent behavior implemented in the points of sale and to take an instant self-protection action.

Considering the operating function, the Archive has been designed as a "closed system": excluding the reporting companies, no others can consult data and information, with some exceptions like the Police Forces. Furthermore, the access to information for reporting companies is free.

The Act also provides a Working Group of experts who support the Electronic Archive carrying out orientation and analysis activities.

The Archive has been operating since 2008 and publishes a statistical Report every year.

The background of the Law 166/2005 on payment cards, associated with the growing awareness of the risks related to the wide spread of identity thefts and frauds, led to the need of an institutional action even in the other economic sectors that are extremely vulnerable to ID crimes.

The Legislative Decree of April 11, 2011, No. 64 has planned the establishment of a public system of fraud prevention at the administrative level in the consumer credit sector, with specific reference to identity theft.

This system aims to strengthen the prevention of ID theft and, more generally subscription frauds, helping to verify the contractor identity, to increase the discouraging effectiveness towards potential fraudsters and to reduce civil and penal controversy on this subject. At the same time, regulatory action aims to provide support to the citizens who might become a victim of identity theft, and to increase the quantitative and qualitative knowledge of the phenomenon.

The method chosen to achieve these results is focused on the information-sharing and the public-private collaboration, through the implementation of a service that allows the authorized companies to verify the identity and information of people requiring access to credit, thanks to the comparison of the data provided by individuals with those collected by the public databases of Ministries and other institutions.

Moreover, the system includes the collection and analysis not only of the fraud cases that have already affected member companies in the past, but also of the potential anomalies resulting from findings made by the system after a request from companies. These data will enable the provision of preventive messages (alerts) that will be sent to those members in the case of assured risk situations. Finally, citizens can use a phone and online service reporting cases of confirmed and suspected identity theft (hotline), with an additional information service.

From the operational point of view, the implementation of this system and of its functions is based on the creation of a central Electronic Archive, a targeted Working Group and a hotline.

The above-mentioned Archive includes three IT tools:

1. the network's interconnection (gateway) allows the Ministry of Economy to examine the public databases with the aim of responding to the data accuracy confirmation requests made by the prevention system members. The databases are not duplicated and remain under the responsibility and control of the regular owners because the system just operates a control matching and then returns a positive or negative result to the requesting company. In this way, both the data security and the citizens' confidentiality and privacy protection are guaranteed;
2. the centralized program unit does store – anonymously and with data aggregation – the cases in which the non-authenticity or non-matching of data have been confirmed, allowing to the owner of the Archive and to the Working Group to analyze each specific case and also the general criminal dynamics of the phenomenon.
3. the alert program unit collects the reports of the chronological fraud cases affecting members and also the preventive alerts sent to the members.

Currently, the types of data subject to verification are: identity document (including the lost or stolen ones), VAT, tax code number and documents certifying income and the fiscal, security and welfare situation. However, the list of data is not exhaustive because it can be integrated with any new information that may become necessary for preventing ID crimes.

The legal measure implies that the significant results for fighting against the organized crime must be communicated to the Department of Public Security offices of the Interior Ministry, responsible for the analysis of criminal phenomena and for the collaboration, even at the international level, between the Police and the Financial Information Unit of the Banca d'Italia.

The service requires a payment from companies, while it is free for public institutions and Police Forces.

The Working Group, made of public and private sector representatives, is entrusted with the multiple task of preparing, processing and anonymously studying the statistical data about fraud in the areas of competence, and of preparing an annual report that should be used by the Ministry of Economy and Finance to present in Parliament the prevention activities' results.

The current system has been developed with technological components and is ready for the beginning of the testing phase. Even the agreement procedures for members are near to conclusion. The full-swing startup of the system is expected in October 2014.

7.4 Summary of the results of the qualitative analysis

Methodological note

Sample of 413 cases equally provided by Vodafone and Wind and related to the period from December 2010 to August 2013.The collection of information was carried out through an online form, available on the website of the Project with a restricted access. The data are indicated in aggregate terms and in case of specific examples remains anonymous in order to protect the privacy and confidentiality of information

Summary of the results

Mobile phone companie's high vulnerability to the ID crimes related to signing a contract that can manifest themselves as identity thefts (or *impersonation*, that is the use of an identity related to natural or legal existing or existed persons) or as identity frauds (i.e. the use of a fictitious or real identity with an alteration of some relevant sensitive data)

Distinctive features, interesting from the criminological point of view, that characterize and distinguish ID thefts and ID frauds

Predominance of identity theft over identity fraud in phenomenological terms. In the case of ID theft, a high incidence of the company ID theft (identity theft committed against legal persons)

Predominance of the misappropriation of devices (e.g. smartphones, tablets, PCs...) as a significant purpose of the ID crimes, over the phone-related frauds concerning the call traffic

Centrality of the document falsification (e.g. use of the original documents, stolen and with an alteration of pictures and/or data, or use of totally counterfeit documents)

Fraudsters' ability to adjust the criminal schemes of fraud related to signing up on the basis of the specific vulnerabilities of the victimized company (e.g. type of commercial offers, users and equipment, control systems...)

Centrality of the economic damages, but also relevance of the reputational damages that may be correlated to them

High assurance of impunity for the perpetrators

Still superficial knowledge of the phenomenon by companies

Marginal role of the Police Force is both in the process of verification/investigation of suspected fraud and in the case of a confirmed fraud. The complaint concerns only 5% of cases of identity theft and 18.6% of cases of identity fraud

The main features of ID theft

It covered the 75% of the analyzed cases

87% of cases are crimes committed against a legal person (company ID theft)

In 40% of cases of company ID theft, the victims were corporations

In 89% of cases, the perpetrators required to sign a new contract, usually with personal data related to a new customer (85.9%)

In 65% of cases, the average duration of fraud by signing up was limited, not more than 30 days

The most used channels for signing a contract are the "physical" ones of a store/dealer (31%) and those of an agency (26%)

The purpose of fraud by signing up related to the identity theft is the misappropriation of the cutting-edge smartphones (40.8%), mobile phones and tablets. On average, for each case at least 5 devices were stolen

The phone-related frauds associated with the abuse or the resale of call traffic are marginal (17%)

Considering the documents provided when requesting a contract, in 47.3% of cases totally counterfeit documents were used: in particular, the identity card, the fiscal code number, the health insurance card and the VAT registration certificate

The perpetrators' profile is still largely unknown, as well as the detailed information about the documents used for fraud by signing up

The average loss per case is settled between 2000 and 3000 Euros, but sometimes it fluctuates between 20 thousand and 35 thousand Euros per case

The main features of ID fraud

They represent less than a quarter of the sample of analyzed cases (24.7%) and include new activations (96%) made by new customers (95%)

In terms of *modus operandi,* they seem to fit within more precise borders compared to those of the identity theft. Being aimed almost exclusively to the misappropriation of the cutting-edge mobile phones, they require a lower level of expertise and may be committed serially, also considering the fact that their average duration does not exceed 30 days

The most used channel for frauds by signing up related to the identity fraud is the agency (41.2%)

The companies' response

In the case of identity theft, the detection takes place thanks to the alerts generated by the control systems (53%), but also to the analysts' activities (37.9%). In the case of identity fraud, the analysts' work is the essential aspect (72%)

In detecting the identity theft, the human element is crucial and can be found primarily in the operational difficulties of analyzing the documents

In identity fraud, along with the human factor, there are also other issues that result in criminal chances and may concern for example the type of commercial offer or activation channel... In wider terms, considering both the cases of ID theft and ID fraud, operators tend to suspend the contract and verify information with the costumer, and then they usually end the procedure with the unilateral dissolution of the contract. Where fraud is suspected or confirmed, the personal records are included in a black-list and the same happens to the IMEI number.

The mobile phone companies' response to the risk of ID frauds by signing up is also affected by outer limits, such as those imposed by the Privacy Law

Prevention solutions

The public system of prevention at the administrative level of frauds related to the consumer credit, with specific reference to the identity theft, according to the Legislative Decree of April 11, 2011. No. 64, is the most effective solution for preventing the risks related to the ID crimes as it will allow – once fully operational – the prior verification of personal, security and income data provided by individuals when requesting a new contract

08

Alberto Cordioli
(8.3.1, 8.4)

Vincenzo Falletta
(8.3.2, 8.5)

Fabiano Francesconi
(8.1, 8.2)

WASP: an alert system to prevent and tackle ID crimes against companies

Besides the research carried out to improve knowledge on ID crimes against natural persons and companies, project WEB PRO ID has also developed innovative ICT tools to tackle and prevent such crimes at a business level.[42] This chapter describes the results obtained in this area with reference to the development of a prototype software to detect ID crimes automatically. The chapter is organised as follows: it starts with an introduction explaining the need for an ICT tool to support companies in their fraud-detection processes (section 8.1). Next, it describes the methodology for the development of a computerised alert system for the fight against ID-related crimes in the business sector, focusing on the various steps of the methodology, from the data collection process to the strategy pursued on the basis of a twofold approach (section 8.2).

The chapter continues by presenting the alert system prototype produced, providing details on the architecture, performances, and further remarks on how its use can effectively support companies in adopting counter-measures and increasing their efforts to prevent identity crimes (sections 8.3 and 8.4). The chapter concludes with a summary of the results (section 8.5).

8.1 Problem statement

Fraud detection is certainly a key activity among the core business processes of any enterprise. It has high strategic value and is able to generate direct economic effects. In this regard, the tasks of fraud analysts are based on continuous monitoring: they need a high availability of resources (proportional to the amount of cases to analyse), and they must give responses as quickly as possible. Whatever the anomaly to be monitored,[43] this task needs extensive real-world investigations that typically require a great deal of time for the manual verification of all suspicious cases (ACFE, 2012; Fraud Advisory Panel, 2011).

The above considerations also apply to identity-related crimes (identity fraud/theft). These crimes are typically committed by fraudsters as an intermediate step towards the final goal of obtaining an economic reward (e.g. stolen devices). Identity crimes are typically perpetrated when someone subscribes to a new service (e.g. buying a new SIM card from a telecommunication company) or when someone asks for a modification of an existing service (e.g. activating promotional deals).

[42] Objective 2.3.

[43] For example, common anomalies for telecommunication companies are the surpassing of some threshold on admitted traffic, rather than a high amount of active services or requested devices, or unpaid bills. Common anomalies for credit companies are overdrawn ac-counts or unpaid loans.

Therefore, in order to detect these types of frauds, analysts must examine all the records related to the activation of new services or the modification of existing services, with the purpose of highlighting anomalies, which are indicators of suspicious frauds. Many variables are taken into account, including personal details (for both private and business customers), details on the chosen payment method, details on the new service and related options (including details on other services already activated by the customer), plus other general information obtained from third-party databases (e.g. situation of unpaid bills, bad debts).

Although the detection of identity frauds requires manual verification of suspicious cases, it can be supported using a system able to prioritise them. This system reduces the number of cases to analyse focusing the analyst's effort on the most "risky situations". In the literature, this form of assistance to the analyst's work implements what is called 'computer-assisted fraud detection' (Mena, 2003; Phua, Lee, Smith, & Gayler, 2010).

8.2 Methodology

This chapter presents a stepwise methodology selected with the intention of achieving the result of Activity 2.3 "Development of a computerised alert system for the prevention of identity related crimes & correlated crimes against businesses", that is, designing and implementing a software (prototype) to combat ID-related crimes. This methodology consisted of three operational steps:

1) Collecting and integrating data provided by the technological partners of the project;
2) Identifying techniques for the automatic detection of fraudulent activities;
3) Defining the architecture of a system based on the techniques identified in the previous step.

During the first step, all the technological partners of the project provided data from their business flows. These data had different structures as products of different business processes and management software. In order to process this information uniformly, the data had to be integrated in a common repository. From an operational point of view, the first step was crucial and represented a fundamental prerequisite for the success of the subsequent steps. Subsection 8.2.1 describes the structures of the data in terms of attributes as well as their differences and similarities.

Once the data had been integrated, the methodology envisaged the identification and employment of techniques for the automatic detection of fraudulent activities. In this regard, a two-pronged method was proposed: on the one hand, a knowledge-sharing approach was used to propagate useful information (i.e., potential fraudulent identities) among the project partners; on the other hand, techniques pertaining to the data mining field were employed to detect recurring patterns in historical data and to use this information to spot fraudulent activities in incoming data flows. These two approaches are presented respectively in subsections 8.2.2 and 8.2.3.

Finally, an alert system, called WASP (WEB PRO ID Alert System Prototype), was implemented with a modular philosophy and built upon a three-tier architecture. The architecture of this system, its features and evaluation of its performance are discussed in detail in section 8.3.

8.2.1 Data collection and integration

Historical data provided by the associate partners could be split into two major categories: on the one hand, data provided by telecommunication companies[44] (i.e. Vodafone, Wind, Telecom) containing customer requests for the activation or the update of telephone services; on the other hand, data provided by credit companies (i.e. CTC) containing customer requests for the purchase of goods, loans or other financial services. Due to their intrinsic similarity, henceforth we will refer to both these data types as *subscriptions.*

For each company, subscriptions were organized in records (also called rows or instances) within tables (also called datasets). Among all the records contained in these tables, some of them were considered "fraudulent" because they related to ID crimes. The number of fraudulent records represented a minority (1% to 1‰ out of the total number of instances), while, as expected, the majority of the records were related to "legitimate" subscriptions. Each table was also composed of several columns, namely attributes (or variables). For each row, these attributes described the subscription itself, with information about the requested service, the customer requesting the service (henceforth simply referred to as 'the customer') and other status information. Furthermore, among all the attributes, one indicated the class of the record (i.e. if the request was legitimate or fraudulent).

Even though the nature of these attributes depends strongly on the specific company business, it is possible to identify four common categories. Attributes can be:

[44] Henceforth also referred to as 'telcos'.

1) **Record-related**: attributes containing intrinsic information on the record, such as the insertion date and time;
2) **ID-related**: attributes containing personal information about the customer, such as the business type (consumer or corporate), name, address, fiscal code, and so on;
3) **Credit-related**: attributes containing information related to credit aspects, such as the chosen payment method, bill address, number of pending operations, if any, and so on;
4) **Service-related**: attributes containing information related to both the new services requested (type and value of service parameters) and those services already activated by the customer.

Datasets are different from each other since each company adopts custom business processes and may address different market sectors. However, even for companies belonging to the same business segment (e.g. telecommunication companies), it is extremely common to find different methods to collect data and process them. This results in datasets differing in the number of the variables as well as in their naming convention and type. The quality of data affects the information that can be drawn from them. Datasets containing high-quality data are accurate, clean and consistent. When analysed with data mining algorithms, they typically generate results better than those from low-quality data, that is, those containing many wrong or missing values. These types of datasets are often referred to as 'dirty' or 'noisy'.

In order to use the two-pronged method mentioned above (knowledge-sharing and data mining) on all the datasets provided by the partners, a pre-processing step was required. The purpose of this step was twofold: on the one hand, it "prepared" the datasets for the application of data mining algorithms (including cleaning and replacement of wrong and missing values, whenever possible); on the other hand, it allowed the selection of a common attribute able to uniquely identify a customer over different company datasets. This attribute was then used in the sharing-knowledge approach to cross-verify identities associated with suspicious subscriptions (see subsection 8.2.2).

As a final remark, it is worth noting that data collection and integration is generally a non-trivial process. Indeed, retrieving data from enterprise IT systems often involves the execution of complex queries. Even in the same company, data may reside in different databases and may be stored in different formats. Moreover, historical data is typically archived in separate units, and retrieving them may be troublesome, as it generally requires the manual intervention by skilled technicians. Nevertheless, a joint effort by the technological partners of the WEB PRO ID project, together with eCrime staff, was made in this regard. As a consequence, it was possible to complete the data extraction process successfully and optimally integrate different datasets into a common repository.

8.2.2 Tackling frauds by sharing the knowledge

The intuition behind the use of stolen or counterfeited identities in the context of the WEB PRO ID project framework is that a person owning one of them is expected to attempt to defraud as many companies as possible in the shortest time (D. B. Cornish, 1994; Felson & Cohen, 1980). What is likely to happen in telecommunication and credit companies is that, when a fraudulent identity is detected, all past and future service subscriptions associated with it are cancelled – or at least suspended – and law enforcement bodies are consulted to investigate the origin of the fraud. Unfortunately, this information is not propagated to other companies, which are therefore exposed to possible criminal activities from the same identity. This behaviour enables malicious persons to harm more than one company using the same *modus operandi*.

Therefore, the proposed knowledge-sharing approach is a countermove in this context because it provides a common repository of "risky" identities. Specifically, as soon as a company detects a fraudulent (or, in general, suspicious) identity, an auxiliary encrypted attribute univocally linked to that identity is inserted in this repository. As a consequence, these attributes linking to suspicious identities are instantly made available to all the project partners in order to take advantage of this information and prevent economic damage.

The set of attributes to be used within the aforementioned common repository follows the scheme described below:

1) An auxiliary encrypted attribute univocally linking to a suspicious identity;
2) The name of the operator (or company) who performed the insertion;
3) The date of the insertion;
4) The status of the identity: fraudulent or suspiciously fraudulent.

The most critical requirement of companies in the EU is to preserve the privacy of their customers. The proposed approach meets this need by encrypting the content of the attribute linking the specific suspicious identity so that its value cannot be used to infer sensitive information about the person behind a given subscription. Details on the type of encryption chosen are given in section 8.3.

8.2.3 Mining the data to discover knowledge

From a temporal point of view, the knowledge-sharing approach described in the previous section contains identities tied to past activities that have been uncovered as malicious or fraudulent. This approach will support companies in the identification of frauds; however, its effectiveness is directly correlated to the efficiency of the analysts in detecting fraudulent subscriptions. The more the analysts are efficient, the quicker the information is made available to other partners, the more the company will be able to avoid economic damage. The problem of conveying the effort of the analysts in the correct direction is rather challenging since the amount of service subscriptions reaches volumes of roughly ten thousand requests per day.

Therefore, it is necessary to find a way to identify the most risky subscriptions and thus prioritize the work of the analysts. To this end, the information drawn from the historical data can be exploited to create predictive models able to learn recurrent patterns in acknowledged malicious activities in the past. These activities are analysed in order to profile a set of schemes able to detect behavioural anomalies (potential ID frauds) in new, hence uncategorised, data flows.

In data mining, this is formulated as a *classification problem* or *supervised learning problem.* Historical data consist in a set of records labelled by the analysts as “fraud” or “non-fraud”, and they are employed to train a classification model, while the new data flows are those labelled using the knowledge of the trained model (Han, Kamber, & Pei, 2011).

There are many classification algorithms able to extract useful and hidden information from large sets of data. These algorithms can be grouped into categories according to their approach to the problem (e.g. rules induction, decision trees, geometric and probabilistic models). Each category has distinctive features, and suits a particular context better and, thus, should be considered. Henceforth the set of techniques and methods proposed to solve a classification problem is simply referred to as ‘data mining approach’.

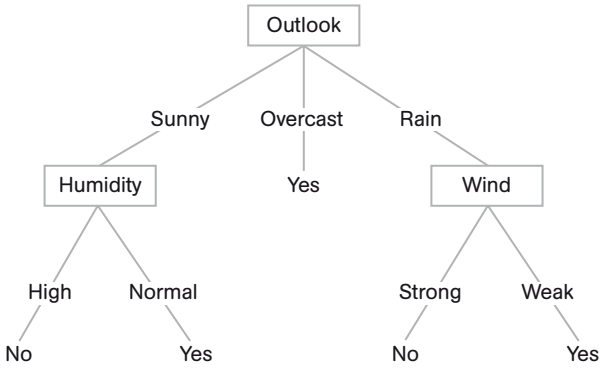
The following categories of algorithms were assessed.[45]

[45] Annex D discusses the classification algorithms employed in more detail.

Classification with decision trees

Decision trees represent a classic methodology in data mining to solve classification problems. By means of them it is possible to obtain prediction rules with a good level of accuracy and graphically representable through tree-like graphs. These tools are used to support decision-making; they are easy to read and to understand; and they are capable of providing a broad overview of the whole system. In detail, each node represents a variable with which a *split condition* is associated. This condition represents a decision to be taken and, according to its value, different paths will be followed to the next levels of the tree (child nodes). Leaf nodes represent values of the target variable, and therefore the decision to be taken. In the context of fraud detection, leaf nodes indicate whether or not the given service subscription is fraudulent.

Figure 32 - Example of a decision tree generated on weather data



Classification with rule induction

An alternative to decision trees is provided by rule induction classification methods. Contrary to decision trees, where the model is built using a top-down approach, rule induction methods start from the single class, and rules are created to obtain the greatest number of instances belonging to that class. This approach, also known as *covering*, seeks to find rules covering the largest number of instances, excluding those belonging to different classes. As in decision trees, the rules generated are of the *IF-THEN* type; however, typically they are shorter and fewer than the set of rules obtainable by running a decision tree algorithm on the same dataset.

Classification with Support Vector Machines

Support Vector Machines (SVM) belong to the class of kernel methods in machine learning typically used in pattern recognition. This type of algorithm applies a

geometrical representation of the data mapping each single instance into points in the multidimensional Euclidean space. Owing to the complexity of this multi-dimensional space, elaborating the models may require remarkable effort; therefore, so-called *kernel functions* are used to avoid computing all the coordinates in the space. This technique is used to solve many machine learning problems, e.g. handwriting and vocal recognition, yielding good results.

8.3 WASP

The last step of the methodology involves the definition of the architecture of a system (alert prototype) based on techniques for the automatic detection of fraudulent activities identified in step 2 and described in subsections 8.2.2 and 8.2.3. This section presents WASP (WEB PRO ID Alert System Prototype), the alert system developed within the WEB PRO ID project framework and able to support the prevention and mitigation of identity-related crimes. Details are given on the architecture, the core functionalities, and the performances obtained with the data provided by the project partners.

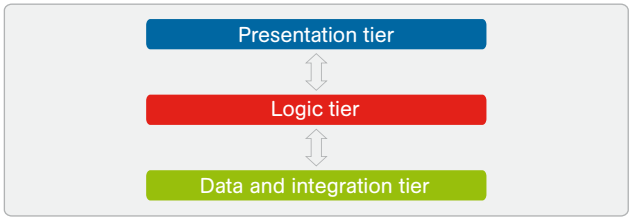
8.3.1 Architecture

In brief, WASP is a *modular* system built upon a *three-tier architecture*. In software engineering, a three-tier architecture is one where the modules implementing the functionalities of the system are logically separated into three levels. This paradigm makes it possible to create applications that are flexible, reusable and easy to manage and maintain. In order to design a system with this type of model, the three levels composing the architecture need to be identified according to their functionalities. In the literature, it is common to structure the architecture into a *presentation tier*, a *business logic tier* (or *logic tier*) and a *data tier*. The presentation tier is the topmost level of the application and manages the interaction of the user with the system. The logic tier controls the application functionalities performing the operation on data stored and retrieved by the *data tier*.

WASP was designed in accordance with this standard philosophy for the presentation and the logic tier. As regards the data tier, instead, it was extended so that it performed the specific function of integrating data belonging to different sources (i.e., the project partners). In fact, as introduced in the previous subsections, an important objective of the WEB PRO ID project has been to promote and implement ID management solutions based on processed information, innovative preventative tools and alert-systems. WASP is a computerized alert system for ID frauds that is based on knowledge-sharing between the project partners, as well as on the application of data mining techniques on company data flows. Moreover, WASP exposes a "common interface" to tackle the problem of ID frauds in the business sector.

A graphical representation of the general architecture of the system is presented in Figure 33 below.

Figure 33 - WEB PRO ID three-tier architecture overview



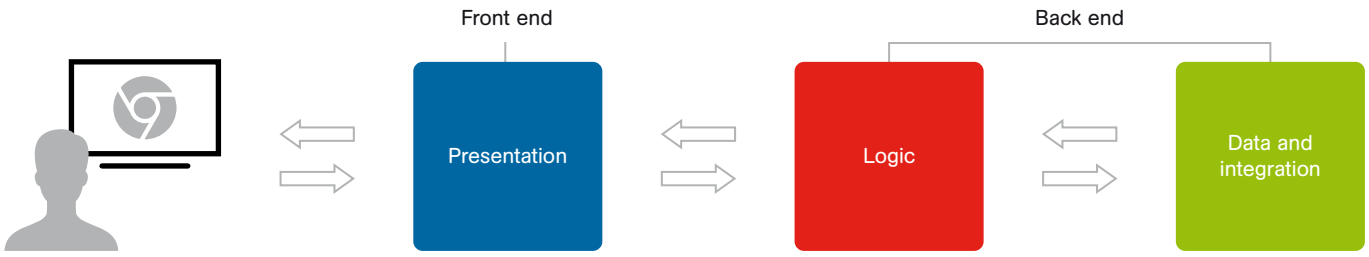
The following subsections discuss the details of the WASP architecture, describing the design, the implementation, and the technology used to build each single module composing the system.

Presentation Tier

As mentioned in the introductory subsection, the presentation tier serves as the system's interface for the final user. The latter interacts with the graphical user interface (GUI) of the system through specific modules placed in this tier. By following common guidelines and best practices, the GUI is designed to be simple, clear and intuitive.

Technical description: The WASP presentation tier has been developed as a Web Application. Therefore the final user of the system (i.e., an analyst) can access the system through a simple web browser (e.g. Google Chrome, Mozilla Firefox). This type of interaction is called *thin-client philosophy* and it does not require the downloading or installing of any additional software on the user's terminal. In order to access the system, the user has simply to open his/her favourite browser and point it to the address of the WASP server. Besides the benefits in terms of simplicity for the analysts, this method allows easy maintenance of the software through a distinct separation of the presentation tier from the actual functionalities of the system. Figure 34 shows the interaction of the user with the presentation tier (front-end, residing on client-side) and subsequently with the other tiers (back-end, residing on server-side).

Figure 34 - Interaction of the user with the WASP presentation tier



Security: Since the system is deployed on a server and is accessible from a network of hosts, it must be protected against illicit accesses and operations. WASP manages authentication and authorization by implementing a secured login mechanism based on username and password tokens. Different levels of authorization can be created as well.

Functionalities: After successfully authenticating with the server, the analyst is redirected to a work area where a list of subscriptions to analyse is displayed (see subsection 8.2.1 for definition of the term "subscription"). This list of subscriptions belongs to the company where the analyst is employed. Each item in the list contains: a) attributes related to the specific request (*record-related*, e.g. date and time); b) attributes related to the identity of the customer (*id-related*, e.g. the name and the client status); c) attributes related to the credit (*credit-related*, e.g. credit risk and number of pending operations); d) attributes related to the service requested (*service-related*, e.g. the type and the number of the service requested). Besides these attributes, each subscription record has two important indexes computed by the system: the ***request score*** and the ***identity at risk*** indicator. These two indexes are of great help to the analysts in their investigative work. The *request score* is the result of the application of data mining algorithms (data mining approach) to the specific request and gives a risk indicator that ranges from 0 (very low risk) to 1 (very high risk). On the other hand, the *identity at risk* index indicates whether the identity associated with the current subscription is associated with an ID fraud for the other project partners (knowledge-sharing approach). Details on these two indexes are provided in the next subsection on the Logic Tier. The analyst, given the information described above, can analyse each single request, deciding to investigate in the case of particularly risky situations.

Logic Tier

The logic tier coordinates the application by implementing the operations the user can perform on data. It also communicates with the other tiers, providing data to visualize to the presentation tier and processing information provided by the data and integration tier. The logic tier represents the core of the system, thus, the modules within it implement both the approaches presented in subsections 8.2.2 and 8.2.3.

Technical description: The WASP logic tier has been developed using the *RESTful Web Services* paradigm. In software engineering, a web service is a method designed to support interoperability between different technologies used to communicate between two applications. By using web services, it is possible to interact between programs (software) written in different programming languages: this characteristic is particularly desirable and appealing in the computer science community. REST (REpresentational State Transfer) is an architectural style that, applied to web services, provides a number of benefits. The most important of them are good performance, scalability, simplicity, reliability and portability. This last feature, in particular, makes the system suitable and attractive for businesses willing to integrate it with their IT systems.

The modules composing the WASP logic tier are: the Ranking System (RS), the Shared Identity Engine (SIE) and the Data Mining Engine (DME). In brief, RS uses SIE and DME to compute respectively the *request score* and the *identity at risk* indexes for each single request. SIE and DME are modules implementing respectively the knowledge-sharing and the data mining approaches. Details on how these two modules help the analyst significantly reduce the number of cases to analyse are provided in subsection 8.3.2.

Functionalities: As described in the introductory subsection, the problem of prioritizing the work of the analysts is particularly important because the number of requests to analyse reaches volumes of up to thousands per day. The WASP logic tier is implemented with a Raking System (RS) that enables the analysts to sort the cases that they have to analyse. The RS is composed of two engines according to the ideas presented in subsections 8.2.2 and 8.2.3: the Data Mining Engine (DME) and the Shared Identity Engine (SIE). The former

applies data mining techniques to the subscriptions in order to give a *request score* to each of them, while the latter indicates whether the customer associated with a particular subscription has to be considered "at risk" because s/he is associated with an ID fraud for one or more other project partners. In order to achieve this, the SIE performs a cross-verification of the customer's identity in the shared database containing identities at risk for all the project partners. The SIE also handles the updating of this shared database when a new identity at risk has been identified: in this way, a bi-directional exchange of information is put in place with benefits for all the companies adhering to this system.

The *request score* and *identity at risk* indexes are two extremely useful criteria with which to reduce the cases to analyse significantly, thus focusing the analyst's work on more "risky situations". These situations are likely to be subscriptions with a high *request score* and for which the customer has been identified as connected to a case of ID fraud by the other project partners.

Data and Integration Tier

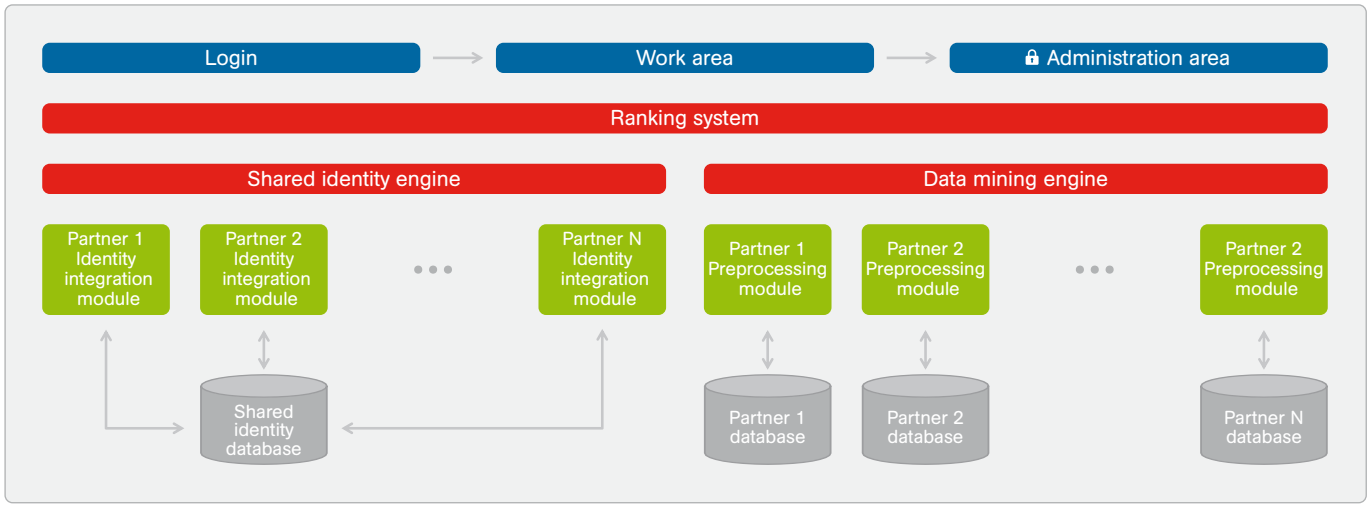
The previous subsections described the core functionalities of the system (logic tier) and how these functionalities are presented to the final user (presentation tier). Analysed in this subsection is the lowest-level data and integration tier, which consists in modules for the storage and the integration of data provided by the different project partners. The primary purpose of the *data and integration tier* is to guarantee the interoperability of the other tiers across the different company databases. In fact, the same data mining algorithms must work with data from distinct databases (i.e. Vodafone, Wind, Telecom, CTC). At the same time, some information has to be shared among all the partners in order to discover whether an identity has to be considered "at risk". Note that an identity may be at risk because it is linked to a person who has been victim of an ID fraud in the past, or just because it has been recognized as not valid (invented/fake identity).

Technical description: The two main functionalities of the data and integration tier are: a) to integrate different types of data from different partners; b) to store data in databases under a common, hence convenient, structure. To achieve these two macro objectives, two sub-layers have been created: a database layer and an integration layer. While the former is devoted to implementation of a set of databases containing partners' data, the latter subsumes specific modules created ad-hoc for each company. In detail, for each partner of the project, an Identity Integration Module (IIM) and a Pre-processing Module (PM) have been created. Details of these modules are given in the next subsection on the functionalities of the Data and Integration Tier.

Functionalities: As explained in subsection 8.2.1, the quality of data affects the information that can be drawn from them and, consequently, the performance of data mining algorithms. Due to their heterogeneous nature, the data provided by each partner of the project are filtered, cleaned and prepared for the application of data mining algorithms. This preparation phase, which is necessarily tailored to each partner's data structure, is implemented in an ad-hoc module called the Pre-processing Module (PM). At the same time, another specific module, called the Identity Integration Module (IIM), converts the identities considered at risk from the specific format of a company to a common one. These identities are encrypted to preserve customers' privacy leveraging the characteristics of so-called *one-way functions*. A one-way function, for a given input, always returns the same output; however, given the output of that function, the original input cannot be retrieved. This method allows the system to create connections between identity attributes in the companies using strings of text that are incomprehensible to a human. Nonetheless, the link is sufficient to relate the same identity among different companies, thus triggering an alarm whenever that identity is used in a service subscription. All these encoded identities are inserted in the Shared Identity Database (SID).

Figure 35 presents the architecture of the system, where each tier has been expanded in order to show the structure of the modules composing it.

Figure 35 - Detailed architecture of the system



8.3.2 Performance

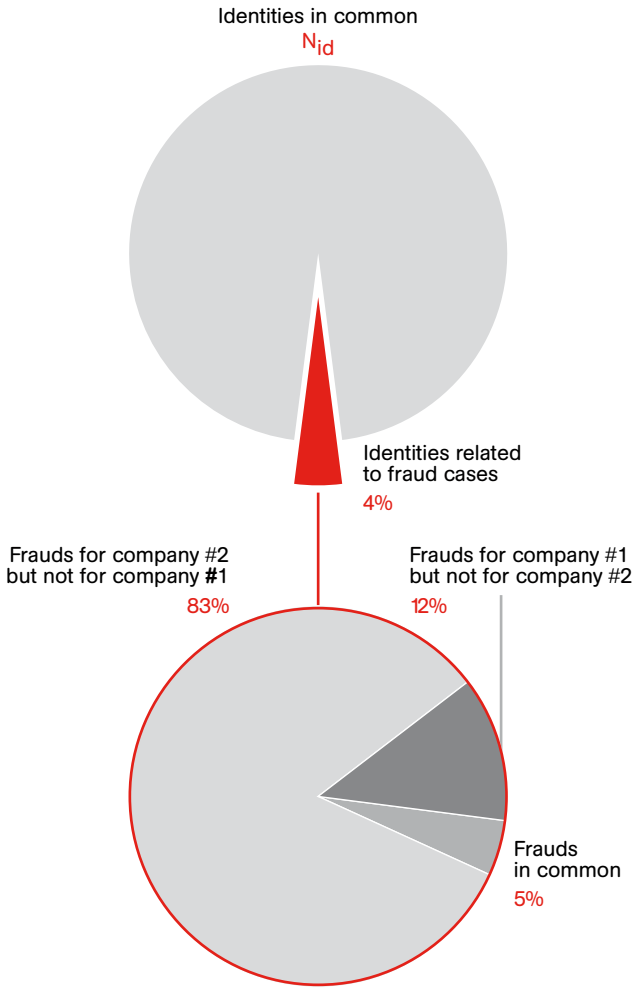
This subsection describes the methodology used to test the WASP alert system and the results obtained. For each of the two proposed approaches (knowledge-sharing and data mining), the respective performances are presented in subsections 8.3.2.1 and 8.3.2.2.

8.3.2.1 Shared Identity Engine Performance

The data obtained from the project partners were used to populate the SID according to the schema presented in subsection 8.2.2 For each company, one attribute was selected in the corresponding dataset to represent the identity of the customer uniquely. In what follows, the attribute chosen to fulfil this functionality is the *fiscal code*. Hence, the set of attributes used in this analysis are: 1) the (encrypted) fiscal code; 2) the name of the company; 3) the actual state of the identity (fraud or suspicious fraud); 4) the insertion date.

The results of this analysis run on two datasets belonging to two different project partners are summarized in Figure 36 and Figure 37. Depicted in Figure 36 is the distribution of the common identities (i.e., identities appearing in both datasets) for the two different companies. If n_{id} [46] is the number of common identities, 4% of n_{id} is related to a fraud for at least one of the two companies. Let n_{fraud} indicate this amount. It is possible to divide it further into three components: a) identities related to ID

Figure 36 – Distribution of identities related to fraud cases common to two companies



[46] Due to a strict non-disclosure agreement between eCrime and the project partners providing the data, in the following some absolute values have been hidden since they may be considered business sensitive or confidential.

frauds for the first company, but not for the second (12% of n_{fraud}); b) identities related to ID frauds for the second company, but not for the first (83% of n_{fraud}); c) identities related to ID frauds for both the companies (5% of n_{fraud}). The missing fraudulent identities for the second and first company in the first two cases respectively are potentially false negatives that could be identified by using the sharing-knowledge approach implemented in the SIE.

Figure 37 – Distribution of the duration of fraud cases common to two companies

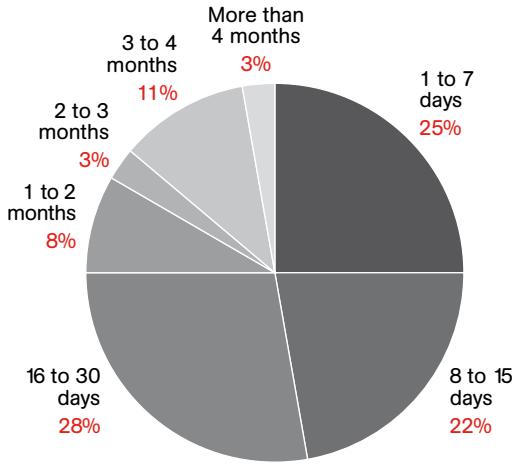


Figure 37 presents the distribution over time of the frauds detected for the two companies. In other words, the third case described above, representing 5% of the common fraudulent identities n_{fraud}, is further analyzed to discover the specific moment when frauds are detected. It is extremely interesting to observe that in 3 out of 4 cases, such fraudulent identities are identified by both the companies within 30 days. The pie chart also shows that in half of the cases the time interval decreases to 15 days, and in 1 out of 4 cases the interval is 7 days. This result confirms the intuition stated in section 8.2. In particular, it has been shown that the false negatives for both the companies can be significantly reduced by the use of SIE. Moreover, the ID frauds perpetrated against both companies are very likely to be detected within 30 days (1 out of 4 cases in 7 days). This proves that the fraudulent activity generally focuses in narrow time intervals, and the use of a shared identity database, like the one implemented in the knowledge-sharing approach, allows more rapid identification of ID frauds by directing the analysts to cases more likely to be fraudulent.

8.3.2.2 Data Mining Engine Performance

Terminology

Before proceeding with presentation of the results obtained with the WASP Data Mining Engine (DME), some concepts useful for understanding the evaluation metrics need to be defined. Let D be a dataset composed of M instances, each of them labelled as legitimate or fraudulent. In the literature, it is also common to indicate the fraudulent class with the term “positive” and the legitimate one with the term “negative”, reflecting the fact that the former has a specific characteristic (fraudulence) that the system wants to identify (Han et al., 2011). Let P be the number of positive instances and N the number of negative instances. The total number of the instances is M = P + N.

When analysing the performance of a classification algorithm on a dataset D, for each instance the prediction that can be obtained belongs to one of the following cases:

1) True Positive: instance belonging to the positive class (fraud) that is classified correctly by the algorithm;
2) False Positive: instance belonging to the negative class (legitimate) that is classified as positive (fraud) by the algorithm;
3) True Negative: instance belonging to the negative class (legitimate) that is classified correctly by the algorithm;
4) False Negative: instance belonging to the positive class (fraud) that is classified as negative (legitimate) by the algorithm.

A good classification algorithm should maximize the number of true positives and true negatives, and it should minimize the number of false positives and false negatives. Let TP be the number of true positives, FP the number of false positives, TN the number of true negatives and FN the number of false negatives. With these four measures it is possible to define what is called a ‘confusion matrix’: see Figure 38.

Figure 38 – Confusion matrix

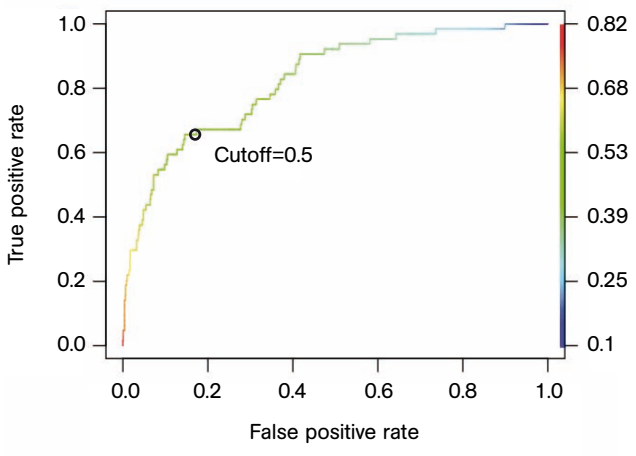
		Predicted Class: Yes	Predicted Class: No
Actual Class	Yes	TP	FN
	No	FP	TN

Note that if P is the number of positive instances, then P = TP + FN. Similarly, if N is the number of negative instances, then N = FP + TN. Finally, starting from these measures, it is possible to define the following performance metrics:

- True Positive Rate (TPR), defined as the ratio of TP to the total number of positive instances: TPR = TP / P;
- False Positive Rate (FPR), defined as the ratio of FP to the total number of negative instances: FPR = FP / N;

- True Negative Rate (TNR), defined as the ratio of TN to the total number of negative instances: TNR = TN / N;
- False Negative Rate (FNR), defined as the ratio of FN to the total number of positive instances: FN = FN / P;
- Accuracy, defined as the ratio of the total number of correct classified instances to the total number of instances: Accuracy = (TP + TN) / (P + N);
- Error rate: defined as the ratio of total number of wrong classified instances to the total number of instances: Error = (FP + FN) / (P + N) = 1 – Accuracy;
- Area Under Curve (AUC), defined as the area under the ROC (Receiver Operating Characteristics) curve. The ROC curve (see Figure 39) depicts the trend of TPR and FPR indexes with respect to all the values for the decision thresholds (cutoff) used by a given binary classification algorithm (i.e., where the classes to predict are two: positive and negative). The AUC metric is an overall performance indicator that summarizes the behavior of an algorithm with respect to the ratio between TPR and FPR. Given a test dataset, for each configuration of the algorithm there exists a ROC curve. For a ROC curve, the larger its AUC, the better the performance of the algorithm.

Figure 39 – Example of a ROC curve generated from experimental data. The specified point corresponds to a decision threshold value (namely cutoff value) of 0.5



Experimental results

Datasets provided by the technological project partners concerned different time ranges (from February 2011 to February 2013). However, all the partners provided data within a time window of at least one year in the above time frame. The experiments carried out used a part of the dataset to train the predictive models by means of data mining algorithms (training set), and to use the remaining part of the dataset to test the performance of the models (test set). During the tests, the datasets were split into chunks, each containing one month of data. Then, the behaviour of the system was simulated in different situations changing the data used to train and to test the model. In particular, the situation of the system at month *n* was simulated by training the model using all the data up to month *n-1*, and evaluating it on the *n-th* month. In this manner, it was possible to simulate the behaviour of WASP on a set of historical data (previously classified by the system itself and verified by the analysts) and generate predictions on a flow of data from the last time frame (i.e., the last month). Note that the system is designed to be updated on a periodic basis, integrating the new data into the set of historical data used to train the system. In the following experiment the time frame unit was set to one "month", but it is possible to choose a different time frame. The methodology described is summarized in the following Figure 40.

In the experiments conducted by the researchers, it was decided to vary the historical training window from a minimum of 6 months to a maximum of 11 months. This resulted in 6 different configurations of training/test sets, as described in the above picture. For each of them, the results are presented in Table 4 and Figure 41. For the sake of simplicity, only results related to a specific company are presented. In particular, in order to show the strength and the aptitude of the system, the results shown were obtained by running experiments on a dataset provided by a telco, on which high accuracy values were achieved. Performances on datasets belonging to other companies were slightly different, like the results of different data used to train the classifiers, but they preserved the positive bearing.

Figure 40 – Methodology for the creation of predictive models using different chunks for training/test

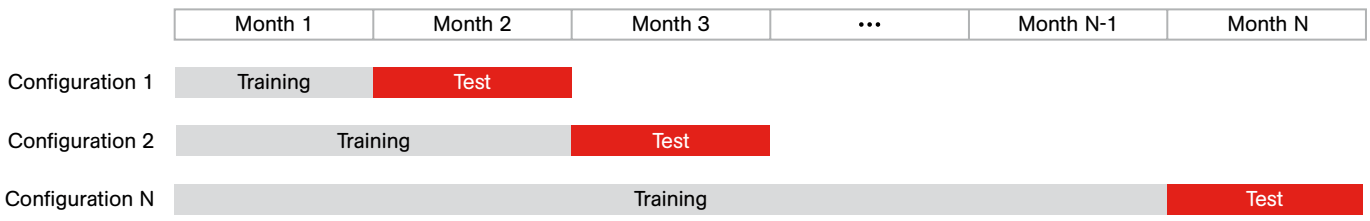
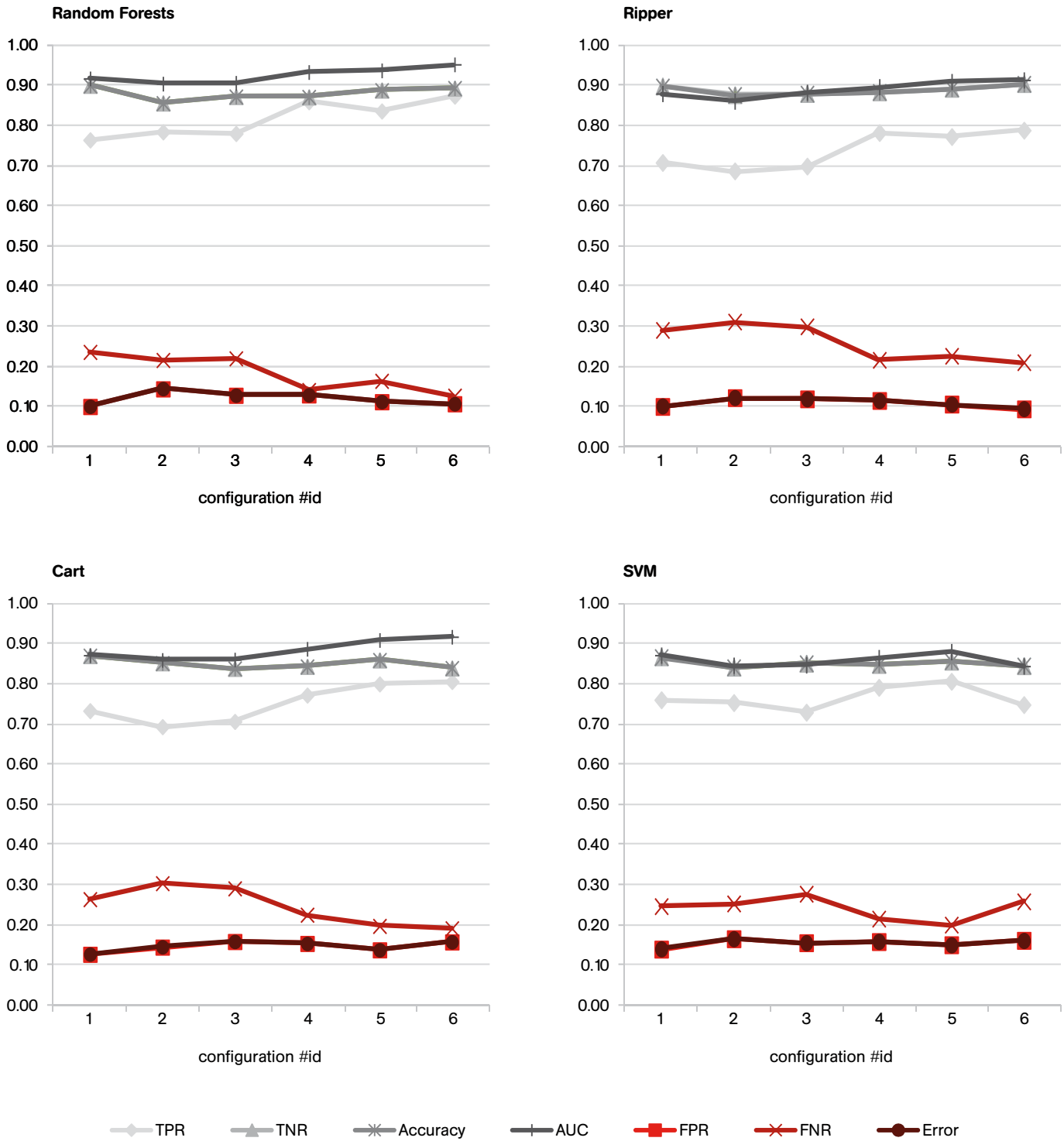


Table 4 - Performance indexes obtained using classification algorithms

Indexes	ID Config.	Random Forests	RIPPER	CART	SVM
TPR	1	0.76	0.71	0.74	0.76
	2	0.78	0.69	0.7	0.75
	3	0.78	0.7	0.71	0.73
	4	0.86	0.79	0.78	0.79
	5	0.84	0.78	0.8	0.8
	6	0.87	0.79	0.81	0.75
FPR	1	0.1	0.1	0.13	0.14
	2	0.14	0.12	0.14	0.16
	3	0.13	0.12	0.16	0.15
	4	0.13	0.11	0.15	0.16
	5	0.11	0.1	0.14	0.15
	6	0.11	0.09	0.16	0.16
TNR	1	0.9	0.9	0.87	0.86
	2	0.86	0.88	0.86	0.84
	3	0.87	0.88	0.84	0.85
	4	0.87	0.89	0.85	0.85
	5	0.89	0.9	0.86	0.85
	6	0.89	0.91	0.84	0.84
FNR	1	0.24	0.29	0.26	0.24
	2	0.22	0.31	0.3	0.25
	3	0.22	0.3	0.29	0.27
	4	0.14	0.22	0.23	0.21
	5	0.16	0.23	0.2	0.2
	6	0.13	0.21	0.19	0.26
ACC	1	0.9	0.9	0.87	0.86
	2	0.86	0.88	0.86	0.84
	3	0.87	0.88	0.84	0.85
	4	0.87	0.89	0.85	0.84
	5	0.89	0.9	0.86	0.85
	6	0.89	0.91	0.84	0.84
ERR	1	0.1	0.1	0.13	0.14
	2	0.14	0.12	0.14	0.16
	3	0.13	0.12	0.16	0.15
	4	0.13	0.11	0.15	0.16
	5	0.11	0.1	0.14	0.15
	6	0.11	0.09	0.16	0.16
AUC	1	0.92	0.88	0.88	0.87
	2	0.9	0.86	0.86	0.84
	3	0.91	0.89	0.86	0.84
	4	0.93	0.9	0.89	0.86
	5	0.94	0.91	0.91	0.88
	6	0.95	0.92	0.92	0.84

Figure 41 - Performance indexes obtained using classification algorithms



It is easy to see that the performances obtained with each of the evaluated algorithms (CART, Random Forests, RIPPER and SVM)[47] were generally good, with significant differences in the 7 plotted metrics. The plots also underline a good general trend over time, with increases in indexes TPR, TNR, Accuracy, AUC and decreases in FPR, FNR and Error rate. Note also that some curves overlap: this is the case e.g. of Accuracy with TNR and for Error rate with FPR. This happens because one of the two classes has many more instances than the other (in this case the dataset is skewed with many more negative than positive examples), so that it affects the performance indexes more. The accuracy and error rate are global performance indicators that take into account the total number of correct classified instances independently of their class. Therefore, their values approach the indexes of the majority class. With an imbalanced dataset biased towards negative, in fact, it is more likely that an instance will be correctly classified as negative, rather than positive. For example, supposing one has a dataset composed 99% of negative instances and 1% of positive instances, a naïve classification algorithm may decide to use a rule that classifies each instance as negative. This algorithm will have an accuracy of 99%, but it would not be of any help in detecting the positive examples, so that it is useless in any practical case.

Consequently, in order to understand if a specific algorithm performs better or worse at any specific configuration, it is necessary to take account of all the indexes displayed in the plots. Better performances will correspond to a better trade-off among the values of all the indexes. A trivial consideration is that performances are as better as the two groups of indexes mentioned above (TPR, TNR, Accuracy, AUC on one side and FPR, FNR, ERROR on the other) diverge. The greater the distance between these groups of points, the better the performances of the analysed algorithm.

It is plain from the plots that Random Forest is the algorithm obtaining the best performance, with a wider separation between the two curves. Moreover, the plots indicate an overall increment of performance over time for all the algorithms considered. Finally, to be noted is that the AUC metric could be used to summarize the behaviour of a given algorithm, and thus to compare two different algorithms at the same configuration. It is easy to verify that a curve with a larger area corresponds to an algorithm that performs better in terms of the TPR/FPR ratio (i.e. for the same TPR it obtains a lower FPR or vice versa). Hence, given all the above considerations, the algorithm that performs best is Random Forest, which detects up to 9 out of 10 frauds with a low false alarm rate (1/10 of legitimate subscriptions). It is followed by RIPPER, CART and SVM.

[47] More details on the algorithms used are presented in Annex D.

8.4 Remarks on WASP

General remarks

The analysis of data has proved to be a useful tool in maximizing both the efficiency and the effectiveness of companies' resources devoted to the identification of frauds. The methods described in this report show that the work of analysts can be optimized if they use a ranking system able to prioritize the suspicious instances to analyse. More importantly, they can improve the detection rate compared to the manual approach. The two approaches, implemented as two modules of the Ranking System (RS), have proved able to remedy, on the one hand, the lack of knowledge between partners sharing the same interest in combating ID frauds, and on the other, the lack of automated tools with which to analyse large flows of data. Another important aspect highlighted by the methodology is the capacity of the state-of-the-art techniques employed to "follow" the evolution of fraud patterns over time. Models generated by using up-to-date data enable the detection of new types of fraud; whence derives their adaptability to evolution within the company ecosystem (e.g. new services, new deals).

The benefits brought by the detection of malicious activities are manifold: a) it prevents economic and reputation damage to the company; b) it directly contributes to feeding the Shared Identity Database, thus producing safety for other stakeholders; c) it feeds future generations of models, thereby improving their accuracy in subsequent iterations. In its long-term use, WASP is expected to achieve further improvement in its - already remarkable - performance.

WASP as a system for the joint effort against ID crimes

WASP is a common interface with which to tackle ID crimes in the business sector. It performs a concrete solution in the standardization of data collection, processing and analysis among companies within the same business sector or, more generally, ones that share common interests. In this project, telcos and credit companies worked together to fight ID-related crimes with the ultimate goal of protecting citizens by preventing the exploitation of stolen identities and reducing the economic and reputational damage caused by the use of counterfeited IDs by malicious customers.

The crucial problem concerning shared repositories of information, especially among competitors, is the

impelling need for companies to protect their *know-how* and *customer lists*. A customer list may be entitled to trade secret protection when it represents a selective accumulation of detailed, valuable information about customers – such as their particular needs, preferences, or characteristics – that naturally would not accrue to persons in the trade or business. In WASP, the customers, their vital statistics, and the types of services to which they have subscribed represent a portion of such knowledge. The Shared Identity Database, i.e. the common repository of malicious identities, addresses this issue by encoding the identity with a one-way function, thus preserving the information relative to a given customer. Nevertheless, all companies will preserve the knowledge on their customers, and they will be able to track that given customer within their systems, retrieving the information already available in their databases.

Another important aspect of WASP is the modularity of its underlying structure. As can be seen in Figure 35, the architecture has been developed so as not to set a limit on the number of partners taking part in the system. In fact, each module comprises a set of methods and functions to elaborate each partner's data independently. Hypothetically, a new partner would be able to join the system at any time simply by implementing a new ad-hoc module that can be seamlessly integrated into WASP, leaving the rest of the system as is.

8.5 Summary of the results of WASP

Features of the fraudulent identities examined

In the partners datasets, fraudulent identities vary from 1% to 1‰ out of the total number of instances

4% of fraudulent identities are in common between partners

75% of frauds last less than one month (25% last 1-7 days, 22% last 8-15 days, 28% last 16-30 days)

Data mining algorithms

Selection of the most suitable data mining algorithms: CART, Random Forests, RIPPER and SVM

Test of the algorithms: best results obtained expanding the training periods (11 months)

Best performing algorithms: 1) Random Forests, 2) RIPPER, 3) CART, 4) SVM

Sharing information to prevent/tackle ID crimes against companies

Creation of pre-processing systems to harmonize different data from partners datasets

Creation of WASP: a three tier architecture software

Presentation tier made up of: Web Application to allow final user to access WASP via browser

Logic tier made up of: a) Ranking System (RS), a component that ranks identities according their risk to be fraudulent; b) Shared Identity Engine (SIE), a database in which fraudulent identities (encrypted) are stored and shared among project partners; Data Mining Engine (DME), a component in which several data mining algorithms are used to produce predictions about the risk for an identity to be fraudulent

Data integration tier made up of: a) Database layer for the implementation of a set of databases containing partners' data; b) Integration layer for the integration and interoperability of the various (and different) partners datasets

Bibliography

ACFE. (2012). *Report to the nations on ocupational fraud and abuse*.

Acoca, B. (2008). Online identity theft: a growing threat to consumer confidence in the digital economy. In D. Chryssikos, N. Passas, & C. D. Ram (Eds.), *The evolving challenge of identity-related crime: addressing fraud and the criminal misuse and falsification of identity* (pp. 74–75). Milan: ISPAC.

Bradford, W. R. (2013). Online Routines and Identity Theft Victimization Further Expanding Routine Activity Theory beyond Direct-Contact Offenses. *Journal of Research in Crime and Delinquency*, *50*(2216-238).

Breiman, L. (2001). Random Forests. *Machine Learning*, *45*(1), 5–32.

Breiman, L., Friedman, J. H., Olshen, R. A., & Stone, C. J. (1984). *Classification and Regression Trees*. *The Wadsworth statisticsprobability series* (Vol. 19, p. 368).

Commission of the European Communities. (2004). Communication COM(2004) 679 final from the Commission to the Council, the European Parliament, the European Economic and Social Committee, the European Central Bank and Europol. Brussels: European Commission.

Cornish, D. B. (1994). The Procedural Analysis of Offending and its Relevance for Situational Prevention. *Crime Prevention Studies*, *3*, 151–196. Retrieved from http://www.popcenter.org/library/CrimePrevention/Volume_03/06_cornish.pdf

Cornish, D., & Clarke, R. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. *Crime Prevention Studies*, *16*(2003), 41–96.

Cortes, C., & Vapnik, V. (1995). Support-vector networks. *Machine Learning*, *20*(3), 273–297.

De Morales, R., & Muñoz, M. (2009). *From Nothing to Having It All?: The Importation of Identity Theft by the EU*. Albacete: Instituto de Derecho Penal Europeo e Internacional.

Elston, M. J., & Stein, S. A. (2002). International Cooperation in On-Line Identity Theft Investigations: A Hopeful Future but a Frustrating Present. *16th International Conference of the International Society for the Reform of Criminal Law*. Charleston. Retrieved from http://www.isrcl.org/Papers/Elston and Stein.pdf

Europol. (2006). *OCTA - EU Organised Crime Threat Assessment 2006*. Retrieved from https://www.europol.europa.eu/sites/default/files/publications/octa2006_0.pdf

Federal Trade Commission. (2001). Identity theft complaint data: Figures and trends on identity theft, January 2000 through December 2000. Retrieved from http://www.ftc.gov/bcp/workshops/idtheft/trends-update_2000.pdf

Federal Trade Commission. (2013). *Consumer Sentinel Network Data book for January - December 2012*. Washington DC. Retrieved from http://www.ftc.gov/sites/default/files/documents/reports_annual/sentinel-cy-2012/sentinel-cy2012.pdf

Felson, M., & Cohen, L. E. (1980). Human ecology and crime: A routine activity approach. *Human Ecology*. doi:10.1007/BF01561001

Foley, L. (2003). *Identity theft: The aftermath 2003*. Identity Theft Resource Center. Retrieved from http://www.idtheftcenter.org/idaftermath.pdf

Fraud Advisory Panel. (2011). An introduction to fraud detection. *Fraud Facts*, (12).

Fraud Prevention Expert Group. (2007). Report on Identity Theft/Fraud. Brussels: European Commission.

Groves, R. M., Fowler, F. J., Couper, M. P., Lepkovski, J. M., Singer, E., & Tourangeau, R. (2013). *Survey methodology*. Hoboken Nj: John Wiley & Sons.

Han, J., Kamber, M., & Pei, J. (2011). *Data mining: concepts and techniques*. Morgan Kaufmann.

Harrell, E., & Langton, L. (2013). Victims of Identity Theft , 2012, (December).

Hasselm, A. E. (2011). *Crime: causes, types and victims*. New York: Nova Science Publishers.

Identity Theft Resource Center. (2010). *Identity Theft: The Aftermath 2009*. Retrieved from http://www.idtheftcenter.org/images/surveys_studies/Aftermath2009.pdf

ISTAT. (2013). La vita quotidiana nel 2012 - Indagine multiscopo annuale sulle famiglie - "Aspetti della vita quotidiana" Anno 2012. Rome: Istituto nazionale di statistica.

Levy, P. S., & Leme, S. (2008). *Sampling of populations: methods and applications*. San Francisco: Wiley.

Linch, J. P., & Addington, L. A. (2007). *Understanding crime statistics: revisiting the divergence of the NCVS and UCR*. Cambridge: Cambridge University Press.

McNally, M. M., & Newman, G. R. (2008). Editors' introduction. In M. M. McNally & G. R. Newman (Eds.), *Perspectives on identity theft* (pp. 1–8). Cullompton: Willan Publishing.

Mena, J. (2003). *Investigative data mining for security and criminal detection*.

National Fraud Authority. (2013). Annual fraud indicator. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/206552/nfa-annual-fraud-indicator-2013.pdf

OECD. (1999). Organisation de Coopération et de Développement Economiques Organisation for Economic Co-operation and Development. Paris: OECD. Retrieved from http://www.oecd.org/internet/consumer/34023235.pdf

OECD. (2003). OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders, HTML. Paris: OECD.

OECD. (2008a). OECD Policy Guidance on Online Identity Theft. Paris: OECD.

OECD. (2008b). Scoping Paper on Online Identity Theft. Paris: OECD.

Patchin, J., & Hinduja, S. (2006). Bullies move beyond the schoolyard: a preliminary look at cyberbullying. *Youth Violence and Juvenile Justice*, *4*(2), 148–169.

Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). A comprehensive survey of data mining-based fraud detection research. *arXiv Preprint arXiv:1009.6119*.

Quinlan, J., & Cameron-Jones, R. (1993). FOIL: A midterm report. *Machine Learning: ECML-93*.

Roberts, L. D., Indermaur, D., & Spiranovic, C. (2013). Fear of Cyber-Identity Theft and Related Fraudulent Activity. *Psychiatry, Psychology and Law*, *20*(3), 315–328.

Robinson, N., Graux, H., Parrilli, D. M., Klautzer, L., & Valeri, L. (2011). Comparative Study on Legislative and Non Legislative Measures to Combat Identity Theft and Identity Related Crime. London: Rand Europe.

Smith, P. K. ., Mahdavi, J. ., Carvalho, M. ., Fisher, S. ., Russell, S. ., & Tippett, N. (2008). Cyberbullying: its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry*, *49*(4), 376–385.

Synovate. (2007). Federal Trade Commission – 2006 Identity Theft Survey Report. McLean (VA): Synovate.

TNS Opinion & Social. (2012). Cyber security. Brussels: European Commission.

United Nations Economic and Social Council. (2007). *Results of the second meeting of the Intergovernmental Expert Group to Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity*. Retrieved from http://www.unodc.org/documents/organized-crime/E_CN_15_2007_8.pdf

UNODC. (2006). Strengthening the United Nations Crime Prevention and Criminal Justice Programme and the role of the Commission on Crime Prevention and Criminal Justice as its governing body. Retrieved from https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ-ECOSOC/CCPCJ-ECOSOC-00/CCPCJ-ECOSOC-07/Resolution_16-3.pdf

UNODC. (2011). *Handbook on Identity-related Crime*. Vienna: United Nations Office on Drugs and Crime.

UNODC. (2013). Open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime. Retrieved from http://www.unodc.org/unodc/en/organized-crime/expert-group-to-conduct-study-cybercrime-feb-2013.html

Vettori, B. (2010). *Le statistiche sulla criminalità in ambito internazionale europeo e nazionale - Fonti e tecniche di analisi con SPSS*. Milano: LED.

Wall, D. S. (2007). *Cybercrime*. Cambridge: Polity Press.

World Bank. (2008). Integrity in Mobile Phone Financial Services. Measures for Mitigating Risks from Money Laundering and Terrorist Financing.

Annex A

Guidelines for exporting the web modules to carry out a victimization survey on identity-related crimes in EU Member States

Andrea Cauduro

Background

Victimization surveys are among the most effective tools with which to collect reliable information on crimes suffered by citizens and their perception of security. For this reason, they have become commonly used by criminologists and statisticians all over the world in the past 40 years. However, in the past victimization surveys have proved to have drawbacks (e.g. costs, sampling, administration time) that have limited both their application only to some crimes (e.g. burglaries, sexual offences) and their repetition (usually every 3-5 years). In order to overcome such limitations, eCrime researchers have consequently decided to exploit the potentialities of the Web and adopt innovative data collection strategies. Some suggestions on exporting this approach are set out below, as foreseen by the project objectives.

1) Data collection strategy

In order to exploit the potentialities of victimization surveys and reduce their shortcomings, it was decided to conduct a web victimization survey (using the CAWI method) for three main reasons. Firstly, this approach makes it possible to reach a high number of persons in a short time and with costs lower than those of traditional surveys (e.g. CATI/CAMI methods). Secondly, it is possible to administer the survey through an online questionnaire hosted on a publicly accessible website in order to acquire the highest visibility possible. Thirdly, the idea is to rely on a post-sampling strategy. Consequently, for WEB PRO ID the questionnaire was published online and advertised so as to attract as many respondents as possible. This approach led to a self- selected sample that was then weighted (see also point no. 5 below).

2) Creation of a questionnaire

In order to carry out a victimization survey, a questionnaire should be prepared with a set of questions on ID thefts. In this regard, in order to obtain more comparable results, it is advisable to use questions already employed in previous victimization surveys. This is the case of WEB PRO ID, which included a series of section and questions similar to those of the surveys carried out by Synovate for the US Federal Trade Commission (Synovate, 2007). This approach proves very useful in obtaining results in line with other previous experiences (e.g. those in the USA). More specifically, the following sections were included in the WEB PRO ID survey in order to explore a) Internet use; b) victimization; c) security perception.

1) Information on the respondents (gender, age, city of residence, etc.).
2) Use of the Internet (frequency of online purchases, means of payment used online, technological devices owned, etc.).
3) ID theft victimization (number of ID thefts suffered, use of stolen data, means used to steal the ID, time taken to restore the situation, information about the perpetrators).
4) Perception of the risk of suffering an ID theft (reasons to be worried/not worried about ID thefts, fear of being victimised, measures to be enacted to tackle ID crimes).

As a general rule, questions should be as concise and clear as possible. Above all, their overall number should below: long questionnaires cause high dropout rates with the consequence that substantial information is lost.

3) Creation of a web module

Choose the suitable software

The web module should be designed so that it can be embedded in a website and thus be easily reachable by Internet users. For this reason, a range of commercial/free software programs can be employed to “translate” the questionnaire into a web survey. Some of them are: SurveyMonkey (www.surveymonkey.com), SurveyGizmo (www.surveygizmo.com), both of which require a fee for full use. As for free software, LimeSurvey (www.limesurvey.com) is a powerful and totally free software program (it was used for the WBE PRO ID project), and it is likely to be the most suitable one in the majority of cases. Another easy and free software is Google Drive (Modules), but it has limitations in the customization of the features/questions; therefore, it should be used only for short questionnaires.

Develop the module

Independently from the software chosen, the following suggestions are useful for designing an effective tool. In detail:

1) Insert hints to clarify definitions e.g. about ID theft.
2) Use “logic” (named “filters” in some pieces of software) to skip through the questionnaire according to the answers given: if the answer to the question “have you ever been the victim of ID theft?” is “no”, skip directly to the following section without showing e.g. the questions on the ID theft *modus operandi*. All the software illustrated above has these features.
3) Use a plain, but focused, graphic with only a few colours highlighting the questions.
4) Insert a “progression bar” that lets the respondent see what stage of the questionnaire s/he has reached.

4) Test of the module

Once the web module has been finished, it is crucial to test it in order to eliminate “bugs” that might make the survey useless (e.g. crucial questions not shown, “looping” of the system). For this reason, a sample of users should try to answer the questionnaire and report possible mistakes or bugs. In this phase, it is also essential to monitor the average time taken to complete the questionnaire. All the above software has this function. If the questionnaire takes too long to answer (e.g. more than 15-20 minutes) it is better to “sacrifice” some questions and refine the module accordingly.

5) Administration of the survey

Once the above steps have been completed, it is time to administer the survey. In this regard, there are several strategies that can be used, as follows.

1) Administer the survey to a previously selected representative sample of the population that one intends to monitor. The advantage of this approach is its reliability, the disadvantage is that it is very expensive and time consuming.
2) Advertise the survey online and let it be completed by a self-selected sample of Internet users. The advantage of this approach is its cheapness, the disadvantage is that reliability is weaker, above all if the number of respondents is low.

As an example, for WEB PRO ID, researchers contacted a company specialised in web advertising, which sent around 1.2 million emails to Italian Internet users asking them to participate. For details, see Chapter 4 above.

Annex B

Guidelines for exporting the web modules for the collection of business case studies on identity-related crimes

Andrea Di Nicola

Background

Case studies on ID crimes provided by company partners of the project were of added value in understanding the features and the dynamics of such offences, as well as the strategies employed by ID fraudsters to achieve their criminal goals. Similarly to the ID thefts examined by means of the web victimization survey, also in this case, the researchers exploited the Web as an instrument to collect data from companies to gather information on case studies. There follow guidelines for the use of the module and its export to other national contexts.

1) Creation of a questionnaire

Before creating the web module, a form should be prepared with a set of questions on ID crimes. For example, the following sections were included in the module employed in WEB PRO ID.

1) classification of the ID crime (ID theft/ID fraud);
2) features of the ID crime[48] victim (physical/legal person, type of occupation);
3) timing of the ID crime (year/month in which the crime took place, duration of the offence, date of discovery);
4) types of goods/services stolen (mobiles, smartphones, pc, credit fraud, mobile service fraud, etc.);
5) crime dynamic (stages of the offence, vulnerability exploited, ID documents employed, quality of the counterfeited documents);
6) perpetrators of the ID crime (employees, clients);
7) damage suffered (economical, reputational);
8) counter-measures adopted (tackling/prevention).

As a general rule, questions should be as concise as possible and should be fine-tuned with stakeholders (e.g. telecommunication or credit companies). In addition, since the tool could be used by analysts, the time needed to fill in the form should be as short as possible.

[48] Respectively for ID theft or ID fraud.

2) Creation of a web module

Choose the suitable software

The web module should be designed so that it can be embedded in a website and thus be easily reachable by Internet users. For this reason, a range of commercial/free software programs can be employed to "translate" the questionnaire into a web survey. Some of them are: SurveyMonkey (www.surveymonkey.com), SurveyGizmo (www.surveygizmo.com), both of which require a fee for full use. As for free software, LimeSurvey (www.limesurvey.com) is a powerful and totally free software program (it was used for the WBE PRO ID project), and it is likely to be the most suitable one in the majority of cases. Another easy and free software is Google Drive (Modules), but it has limitations in the customization of the features/questions; therefore, it should be used only for short questionnaires.

Develop the module

Independently from the software chosen, the following suggestions are useful for designing an effective tool. In detail:

1) Insert hints to clarify definitions e.g. about ID theft.
2) Use "logic" (named "filters" in some pieces of software) to skip through the questionnaire according to the answers given: if the answer to the question "have you ever been the victim of ID theft?" is "no", skip directly to the following section without showing e.g. the questions on the ID theft *modus operandi*. All the software illustrated above has these features.
3) Use a plain, but focused, graphic with only a few colours highlighting the questions.
4) Insert a "progression bar" that lets the respondent see what stage of the questionnaire s/he has reached.

3) Test of the module

Once the web module has been finished, it is crucial to test it in order to eliminate "bugs" that might make the survey useless (e.g. crucial questions not shown, "looping" of the system). For this reason, a sample of users should try to answer the questionnaire and report possible mistakes or bugs. In this phase, it is also essential to monitor the average time taken to complete the questionnaire. All the above software has this function. If the questionnaire takes too long to answer (e.g. more than 15-20 minutes) it is better to "sacrifice" some questions and refine the module accordingly.

Annex C

Guidelines to export WASP

Fabiano Francesconi

The methodology used to build WASP and presented in this document combined the efforts and knowledge of different partners with the purpose of improving existing strategies and providing computer-supported means to aid the manual work of the operators. Given the configurability of the two approaches proposed, the methodology can be easily transferred to other EU Member States by replacing the Italian partners, contributing to this project, with the equivalents in those countries.

From the operational perspective, various tasks need to be performed to collect the data, integrating them and making them suitable for processing by the various algorithms and techniques comprised in the WASP presented here.

Collecting and understanding the data

Different partners mean different datasets. The first task to be completed, in agreement with the project partners, is the data collection. Typically, these data come in different formats because they are exported from the different business processes and management software used in the companies. Understanding the semantics of the data, in addition to the structure with which they are represented, is probably the most important goal to be achieved in the entire methodology. Each subscription, regardless of whether it relates to telephone or financial services, is defined as a combination of variables (or attributes). Hence, capturing the meaning of the latter is crucial for the success of the methodology. The benefits of deep knowledge of the data are manifold since it allows: a) identification of the most important attributes (the ones best characterizing a subscription); b) identification of attributes producing unwanted noise in the data (those providing information irrelevant to the purpose); c) creation of the so-called *computed* attributes. In particular, identifying new attributes can make the difference in the performance of the data mining algorithms since such new attributes may furnish hidden non-trivial information.

In order to acquire the best insights into the data provided by the project partners, consulting the domain experts is crucial because of their expertise. Moreover, spending time on investigating the data, visualizing them, and observing how they change over time, is also advisable.

Integrating the data

Pieces of data organised in different structures are not suitable for analysis by data mining techniques. These algorithms expect to work on a common structure, treating the data according to the values of the attributes defining it.

For instance, two companies may store the information about the gender of a customer using two different attribute names: *gender* and *sex*. The semantics are the same; however, the data mining algorithms would not be able to treat these two attributes as one.

Together with the integration of semantically equivalent attributes, there is the integration of semantically equivalent values for an attribute. For instance, date attributes may be stored in different formats (for example, a date may be expressed in several formats, e.g. 22-10-1990 vs. 22-10-90 vs. 10-22-1990 vs. 1990-10-22). Unifying values describing the same concept improves the coherence of the data, and hence the performance of the algorithm. This task, together with the explicit marking of *missing* and *invalid* values, is frequently termed *cleaning* in the literature.

Integrating the data is therefore a desirable step when dealing with multiple sources, and defining a proper schema is not a straightforward task. In this context, it is advisable to configure the cleaning and processing algorithms properly, because they have to match the correct data format.

Defining a strategy

Once the datasets have been created, their content is ready to be processed with the purpose of extracting knowledge. This methodology comprises two complementary approaches: a) a knowledge-sharing approach based on the creation of a repository of malicious identities, hence fostering collaboration between partners sharing the same purposes; b) a knowledge-discovering approach that leverages state-of-the-art data mining techniques with the purpose of extracting recurring patterns from data belonging to the past.

The strategy proposed in this document combines the benefits of both solutions: sharing knowledge about already discovered fraudulent identities and promptly identifying potential frauds by detecting recurrent patterns in historical data. With respect to the first approach, particular attention should be paid to the data encryption process, because it is important to preserve customer privacy and, at the same time, adopt the same encryption method (i.e. one-way function) across all the project partners. The effectiveness of the data mining approach, instead, depends closely on the partners' data. For this reason, in order to collect and integrate them successfully, joint effort among all the project partners is necessary. Unfortunately, in the data mining area there is no general-purpose algorithm that can be applied to solve any problem. Picking the right technique is a matter of intuition and expertise that must be supported by results. It is therefore necessary to run extensive evaluations on different state-of-the-art techniques so as to choose the method that best fits the problem to address.

Annex D

Notes on the algorithms employed

Vincenzo Falletta

Classification and Regression Trees (CART)

CART (L Breiman, Friedman, Olshen, & Stone, 1984) is one of the most popular algorithms for classification based on decisional trees. Using this algorithm makes it possible to generate a tree model for the prediction of variables that are categorical (classification tree) or numerical (regression tree). The generated tree is binary, i.e. each node (*parent node*) has exactly two descendants (*child node*) or is a terminal node (*leaf node*). An internal node in the tree represents a variable that is selected among all the available ones based on its *predictive capability*; an arc from a parent to a child node represent a split condition that involves the variable related to the parent node. Finally, a leaf node contains the predictions for every instance ending up in such a particular node.

The procedure used to generate the model involves a recursive partitioning of the data. The entire dataset is initially assigned to the root node. Then, the dataset is split into subsets based on an attribute value. The process is repeated on each derived subset in a recursive manner until the minimum level of impurity is achieved (i.e. the instances in a leaf node all belong to the same class, or when splitting no longer adds value to the predictions). In case of a classification tree, the *impurity* is computed using the Gini index:

$$Gini = 1 - \sum_{j=1}^{c} \left(\frac{n_j}{n}\right)^2$$

However, the tree generated with this method generally has a very high dimensionality, so that the model obtained loses generality and is complex to manage. For this reason, once the tree with maximum dimension has been generated, a pruning step is performed. The pruning phase deletes subtrees from the original tree in order to simplify the model without losing accuracy. This pruning criterion is called *minimal cost-complexity pruning*. The goal of this step is to minimize the cost-complexity function, defined as:

$$R_\alpha(T) = R(T) + \alpha|T|$$

where T is the pruned sub-tree, $|T|$ its complexity (number of leaf nodes), α the complexity parameter, and $R(T)$ the misclassification rate for the sub-tree T. Choosing the best tree means finding the value for complexity parameter α minimizing $R_\alpha(T)$.

Random Forests

Random Forests (Leo; Breiman, 2001) is a classification algorithm based on decision trees. An ensemble of n tree models is grown, where the predictions of each model are aggregated in order to gain better performances. Each of the n decision trees creating the "forest" is generated starting from a distinct random sample (*bootstrap sample*) from all the available data. Instances which are not included in a bootstrap sample, denoted *out-of-bag* (*oob*) *instances*, are about one-third of the original data and are used as a test set. The algorithm employed to grow each tree is similar to CART, although pruning is not performed and the split condition at each node is not evaluated using all the available predictors, but rather on a subset of them consisting in m randomly chosen variables.

Despite its simplicity (it only has two parameters n and m), the algorithm is able to perform rather well. Moreover, the algorithm is also able to measure the importance of each predictor, namely the *variable importance*, by applying a perturbation on the out-of-bag data and then measuring the error difference between those perturbed data and the non-perturbed ones, or rather by calculating the average value of the Gini index for each predictor within all the trees in the forest.

RIPPER

Repeated Incremental Pruning to Produce Error Reduction (*RIPPER*) (Cohen, 1995) is a rule induction algorithm based on the previous *IREP - Incremental Reduced Error Pruning* (Furnkranz & Widmer, 1994), including some modifications to achieve improved performance. It is a *sequential covering* algorithm with the following features: i) rules are learned sequentially, one by one; ii) each rule for a given class must ideally cover (i.e. be verified by) the greatest number of tuples belonging to that class, and possibly none of the tuples belonging to other classes; iii) for each new learned rule, the tuples being covered are removed and the process is then repeated on the remaining tuples. This sequential learning technique contrasts with the approach implemented in decision trees learning: in the latter each rule corresponds to a path from the origin node to a leaf node; hence we can consider a decision tree as a set of rules learned simultaneously.

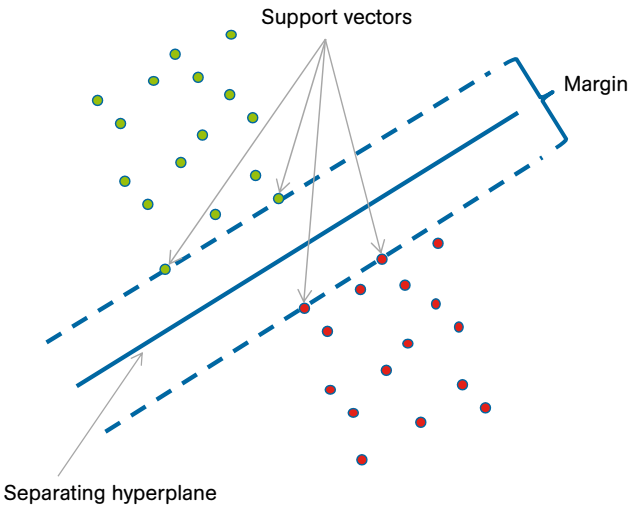
The algorithm is *greedy* in learning the rules (meaning that there is no guarantee of finding a global optimal solution because the optimal choice is performed only at a local level, step by step) starting from an empty construct and adding at each round new constraints on the evaluated attributes, according to their information content (following a scheme well known in the literature (Quinlan & Cameron-Jones, 1993), which maximizes the *information gain*). At first, rules are generated, and then *pruning* is performed, similarly to what happens with decision trees, which consists in removing a constraint on a selected attribute so as to obtain a simpler rule, keeping the accuracy level below a given threshold.

Support Vector Machines (SVM)

In order to explain how classification via Support Vector Machines (Cortes & Vapnik, 1995) works, we need to draw concepts and terminology directly from linear algebra. Given an input dataset, we can build a model through a coordinate transformation (usually non-linear), consisting in a mapping of the input dataset into a space where it is possible to separate them linearly. Therefore, the solution of the new problem becomes finding an hyperplane able to optimally separate the two classes contained in the dataset. This hyperplane is characterized by its *support vectors*, namely the tuples at minimum distance from the hyperplane itself belonging to each of the two classes (hence they will be on opposite sides of the hyperplane, see Figure 42). The Optimal Separating Hyperplane (OHS) is the one maximizing the margin: that is, the distance between support vectors and the hyperplane itself. When it is not possible to separate the data linearly, the previous approach can be extended by adopting different *kernel functions* able to perform non-linear transformations on input data, mapping them into a higher dimensional space. In this space it will be possible to find an Optimal Separating Hyperplane corresponding to non-linear separating surfaces in the input space.

SVM-based classifiers are quite accurate; moreover, they have some advantages (lack of local minima, poor inclination towards overfitting) deriving from the fact that the algorithm is not greedy. Instead, a global optimal solution is found using quadratic programming techniques.

Figure 42 – Classification using SVM



Annex E

An example of a WASP Graphical User Interface (GUI)

Figure 43 - An example of a WASP Login page

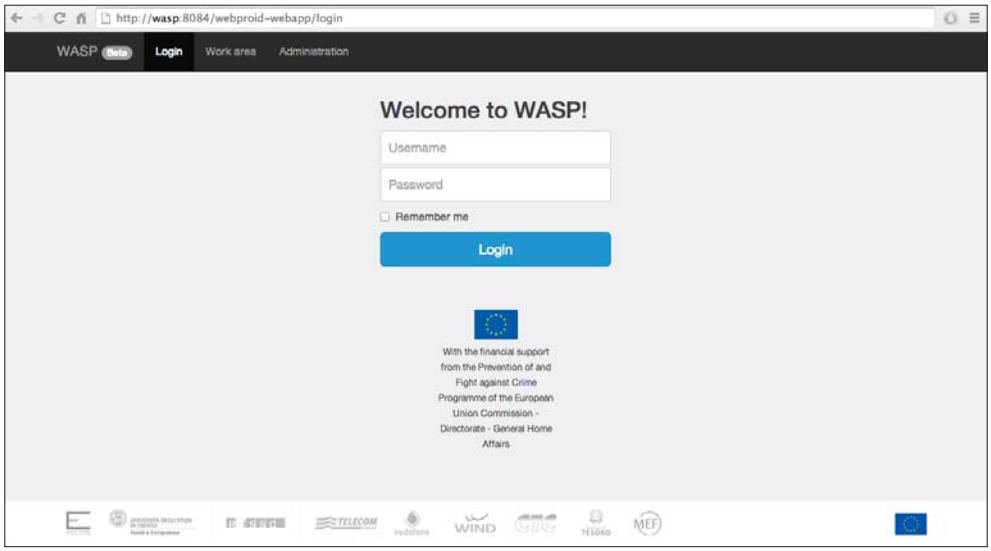
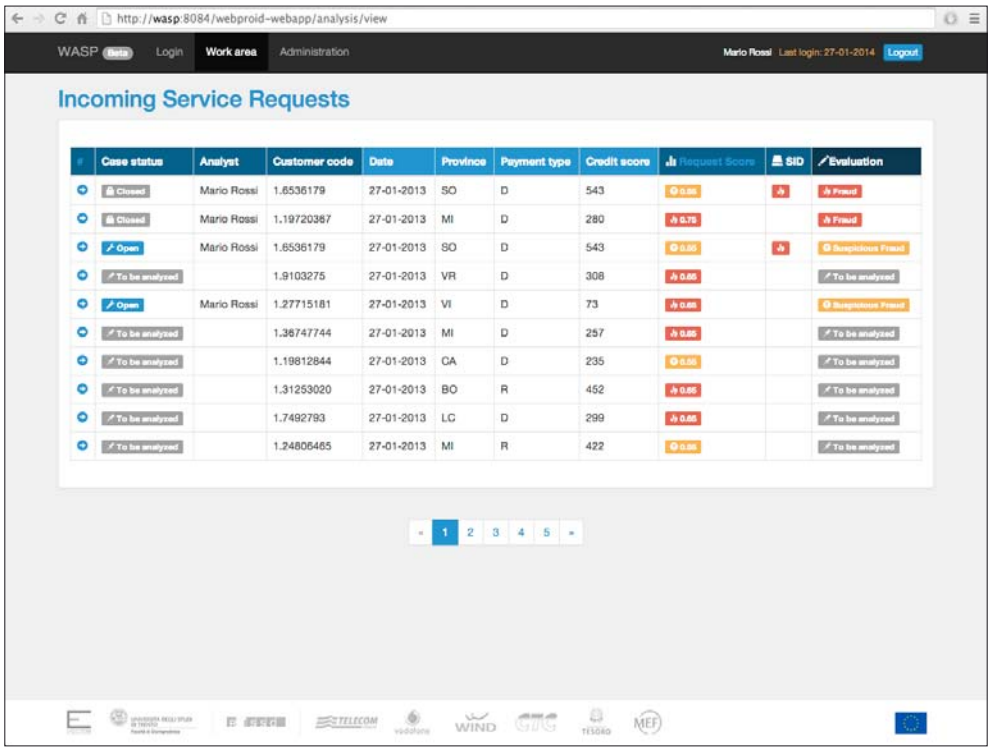


Figure 44 - An example of a WASP work area



This screenshot shows the list of subscriptions to analyse. Note the two attributes “Request Score” and “SID”: the former indicates the score given by data algorithms to each request; the latter indicates if the identity of the customer is found in the SID and is hence “at risk” because related to an ID fraud.

Annex F

Questionnaire of the victimization survey

There follows the translation of the web questionnaire employed for the victimization survey.

Personal data treatment

1) According to art. 13 of Legislative decree 196/2003, I authorize the treatment of my personal data for the purposes of this survey

Yes

No

Section 1. Information on the respondent

2) You are:

Male

Female

3) How old are you?

Type the answer here: ____

4) What is your marital status?

Single

Married - in a relationship

Widowed

Separated - divorced

5) Including yourself, how many members of your family are there?

1

2

3

4

5 or more

6) In what area of the country do you live?

North West (Liguria, Lombardia, Piemonte, Valle d'Aosta)

North East (Emilia Romagna, Friuli Venezia Giulia, Trentino Alto Adige, Veneto)

Centre (Lazio, Marche, Toscana, Umbria)

South and Islands (Abruzzo, Basilicata, Calabria, Campania, Molise, Puglia, Sicilia, Sardegna)

7) What is your education?

None

Elementary

High school

University degree

Postgraduate degree (Ph.D., etc.)

8) At present you are:

Employed

Unemployed

Retired

Student

Housewife

Other ____

9) What is your job?

Answer only if the following rule is fulfilled: the answer to question 8 *"At present you are:"* was 'Employed'

Atypical worker (occasional job, etc.)

Professional

Entrepreneur

Manager officer, university lecturer, magistrate

White-collar worker

Teacher

Blue-collar worker, waiter, shop assistant

Other ____

10) What is your family's net yearly income?

< 10,000 euros

10,001-20,000 euros

20,001-30,000 euros

30,001-40,000 euros

40,001-50,000 euros

> 50,000 euros

Section 2. Internet use

11) In the past few months, have you used the Internet to buy goods or services for private purposes?

Yes, in the past 3 months

Yes, from 3 months to 1 year ago

Yes, 1 year ago or more

Never

12) What method do you most frequently use to pay for goods/services?

Answer only if the following rule is fulfilled: the answer to question 11 "*In the past few months, have you used the Internet to buy goods or services for private purposes?*" was 'Yes, in the past 3 months' *or* 'Yes, from 3 months to 1 year ago' *or* 'Yes, 1 year ago or more'

Credit card (traditional or prepaid)

Paypal

Payment on delivery

Online money transfer

I buy online and pay at the shop

Other ____

13) In the past few months, have you used the in-banking system to check your bank statement, transfer money, recharge your mobile phone credit, or make online payments?

Yes, in the past 3 months

Yes, from 3 months to 1 year ago

Yes, 1 year ago or more

Never

14) What device(s) do you own/use?

More than one answer is possible

Smartphone

Tablet (iPad, Galaxy Tab, etc.)

Laptop

PC

Other (e.g. iPod touch)

I own no devices

Section 3. Identity theft

The next questions deal with identity theft.

An identity theft occurs when a person steals and uses the data/personal documents of another person to request a loan, a mortgage, or to sign a contract (e.g. mobile phone subscription, house rental, energy service)

15) How many times have you suffered an identity theft in your life?

0

1

2

3 or more

Section 3.1. Use of stolen data

This section collects information on the use of data stolen in the last identity theft that you suffered.

16) As regards the last identity theft that you suffered, do you know for what criminal purpose your personal data were used?

Answer only if the following rules is fulfilled: the answer to question 15 "*How many times have you suffered an identity theft in your life?*" was equal to or greater than '1' .

Yes

No

17) Were your data used to forge documents?

Answer only if the following rules are satisfied: the answer to question 15 "*How many times have you suffered an identity theft in your life?*" was equal to or greater than '1'; *and* the answer to question 16 "*As regards the last identity theft that you suffered, do you know for what criminal purpose your personal data were used?*" was 'Yes'.

Yes

No

Don't know

18) What documents were created from your data?

Answer only if the following rule is fulfilled: the answer to question 17 "*Were your data used to forge documents?* was 'Yes'

More than one answer is possible

Identity card

Driving licence

Passport

Social security number

Pay packet

Tax return

Other _____

19) Were data used to ask for a loan or a mortgage?

Answer only if the following rules are satisfied: the answer to question 15 "*How many times have you suffered an identity theft in your life?*" was equal to or greater than '1'; *and* the answer to question 16 "*As regards the last identity theft that you suffered, do you know for what criminal purpose your personal data were used?*" was 'Yes' .

Yes

No

20) Can you state the amount requested (in euros)?

Answer only if the following rules are fulfilled: the answer to question 15 "*How many times have you suffered an identity theft in your life?*" was equal to or greater than '1'; and the answer to question 19 "*Were data used to ask for a loan or a mortgage?*" was 'Yes'.

€ _____

21) Were your data used to buy one or more goods?

Answer only if the following rules are fulfilled: the answer to question 15 "*How many times have you suffered an identity theft in your life?*" was equal to or greater than '1'; *and* the answer to question 16 "*As regards the last identity theft that you suffered, do you know for what criminal purpose your personal data were used?*" was 'Yes'.

Yes

No

22) Can you indicate what kind of goods they were?

Answer only if the following rules are fulfilled: the answer to question 15 "*How many times have you suffered an identity theft in your life?*" was equal to or greater than '1'; *and* the answer to question 21 "*Were your data used to buy one or more goods?*" was 'Yes'.

More than one answer is possible

Jewellery/watches

Electronic or IT devices

Sports equipment/clothes

Music or film CDs/DVDs

Don't know

Other _____

23) Were your data used to sign one or more contracts (e.g. mobile phone, house rental)?

Answer only if the following rules are fulfilled: the answer to question 15 "*How many times have you suffered an identity theft in your life?*" was equal to or greater than '1'; *and* the answer to question 16 "*As far as the last identity theft you suffered, do you know for which criminal purpose your personal data were used?*" was 'Yes'.

Yes

No

24) Can you indicate which contract?

Answer only if the following rules are fulfilled: the answer to question 15 "*How many times have you suffered an identity theft in your life?*" was equal to or greater than '1'; *and* the answer to question 23 "*Were your data used to sign one or more contracts (e.g. mobile phone, house rental)?*" was 'Yes'.

Multiple choice

Mobile phone (e.g. new SIM or mobile number, mobile phone, Ipad, smartphone)

Credit (e.g. opening a bank account)

Service (e.g. energy, gas)

Rental

Don't know

Other _____

Section 3.2. Other use of stolen data

This section collects information about the use of the data stolen in the last identity theft that you suffered.

25) Your stolen data were used to...

Answer only if the following rules are fulfilled: the answer to question 15 "*How many times have you suffered an identity theft in your life?*" was equal to or greater than '1'; *and* the answer to question 16 "*As regards the last identity theft that you suffered, do you know for what criminal purpose your personal data were used?*" was 'Yes'.

More than one answer is possible

Fill in a fake tax return/VAT certificate

Obtain medical services

Obtain a job

Provide state authorities with your identity in the case of driving infractions and/or related offences (e.g. driving while drunk)

Provide state authorities with your identity for crimes other than those related to driving

Obtain welfare benefits?

Defame (e.g. give your contact to an adult website)

Stalk or commit violence against you (e.g. mass emailing, stalking or blackmailing emails)

None of the above

Other _____

Section 3.3. Features of the identity theft

This section collects information about the dynamics of the last identity theft that you suffered (how the data were obtained, when theft was discovered, reported to the police).

26) As regards the last identity theft that you suffered, do you know how your personal data were obtained?

Answer only if the following rule is fulfilled: the answer to question 15 "*How many times have you suffered an identity theft in your life?*" was equal to or greater than '1'

Yes

No

27) Can you say how your data were obtained?

Answer only if the following rule is fulfilled: the answer to question 26 "*As regards the last identity theft that you suffered, do you know how your personal data were obtained?*" was 'Yes'

More than one answer is possible

Theft from my wallet

From my mail box

From my trash

During an online purchase or money transfer

During a non-online purchase or money transfer

Through an IT attack on my pc/smartphone (e.g. virus, Trojan)

Through an email that switched me to a fraudulent website apparently identical to my bank/mail/firm website

Through a fraudulent telephone call/SMS made by fake officials of banks/mail services/firms who asked for my personal data

From my Facebook profile (or other social network)

Theft/trespass at the premises of a company/office that possessed my data

Other _____

28) How much time passed until you discovered the theft?

Answer only if the following rule is fulfilled: the answer to question 15 "*How many times have you suffered an identity theft in your life?*" was equal to or greater than '1'

1 day or less

Some days, but less than a week

1-3 weeks

1- 6 months

7-12 months

Don't know when the identity theft occurred

29) Did you report the theft to the police?

Answer only if the following rule is fulfilled: the answer to question 15 "*How many times have you suffered an identity theft in your life?*" was equal to or greater than '1'

Yes

No

30) For what reason(s) did you report the theft to the police?

Answer only if the following rule is fulfilled: the answer to question 29 "*Did you report the fact to the police?*" was 'Yes'.

More than one answer is possible

To track the thief down

To get the goods/money stolen back

To avoid paying for unrequested goods/services

To comply with the duty of informing police and other competent authorities

To obtain an insurance reimbursement

Because I had to report the loss of documents, cheques, etc.

To obtain stronger control by the police

Other _____

31) For which reason(s) did you not report the fact to the Police?

Answer only if the following rule is fulfilled: the answer to question 29 "*Did you report the theft to the police?*" was 'No'.

More than one answer is possible

I dealt with the situation on my own/with the help of my family

It was not important/serious enough

There was no evidence, the police could not have done anything

I did not have insurance

The police discouraged me from reporting

I did not want to lose time with the report

I was afraid of retaliation

I did not want to be involved in a possible trial

I had previously had negative experiences with the police and the judicial system

Nothing was stolen

Other _____

Section 3.4. Perpetrators of the identity theft

This section collects information on the perpetrator(s) of the last identity theft that you suffered.

32) As regards the last identity theft that you suffered, were the perpetrators discovered?

Answer only if the following rules are fulfilled: the answer to question 15 "*How many times have you suffered an identity theft in your life?*" was equal to or greater than '1'

Yes

No

33) Can you indicate the number of the perpetrators?

Answer only if the following rule is fulfilled: the answer to question 32 "*As far as the last identity theft you suffered, were the perpetrators discovered?"* was 'Yes'.

1

2

3

4 or more

34) Can you say who the perpetrator was?

Answer only if the following rule is fulfilled: the answer to question 33 "*Can you state the number of perpetrators?*" was '1'

Stranger

Relative/friend

Colleague

Neighbour

Owner/employee of a shop I used to go to

Employee of a bank/firm that I deal with

Other _____

35) Was the perpetrator Italian or foreign?

Answer only if the following rule is fulfilled: the answer to question 33 "*Can you state the number of perpetrators?*" was '1'

Italian

Foreign

36) Where did s/he come from?

Answer only if the following rule is fulfilled: the answer to question 35 "*Was the perpetrator Italian or foreign?*" was 'Foreigner'.

European Union

Central Eastern Europe

Other European countries

Northern Africa

Western Africa

Eastern Africa

Central-Southern Africa

Western Asia

Central-Southern Asia

Eastern Asia

Northern America

Central-Southern America

Oceania

Stateless

37) Can you state who the perpetrators were?

Answer only if the following rule is fulfilled: the answer to question 33 "*Can you indicate the number of the perpetrators?*" was greater than '1'.

Strangers

Relatives/friends

Colleagues

Neighbours

Owners/employees of a shop I used to go to

Employees of a bank/firm I deal with

Other _____

38) Were the perpetrators Italians or foreigners?

Answer only if the following rule is fulfilled: the answer to question 33 "*Can you indicate the number of the perpetrators?*" was greater than '1'.

Italians

Foreigners

Italians and foreigners

39) Where did they come from?

Answer only if the following rule is fulfilled: the answer to question 38 "*Were the perpetrators Italians or foreigners?*" was 'Foreigners' *or* 'Italians and foreigners'.

More than one answer is possible

European Union

Central Eastern Europe

Other European countries

Northern Africa

Western Africa

Eastern Africa

Central-Southern Africa

Western Asia

Central-Southern Asia

Eastern Asia

Northern America

Central-Southern America

Oceania

Stateless

Section 3.5. Consequences of the identity theft

This section collects information on the consequences of the last identity theft that you suffered (damage, time take to resolve the situation)

40) Can you indicate the amount of economic loss (in euros)?

Answer only if the following rule is fulfilled: the answer to question 15 "*How many times have you suffered an identity theft in your life?*" was equal to or greater than '1'

€ _____

41) Can you indicate the extent to which the following situations caused you difficulties?

Answer only if the following rule is fulfilled: the answer to question 15 "*How many times have you suffered an identity theft in your life?*" was equal to or greater than '1'

	Much	Somewhat	Little	Nothing
Amount of the economic loss				
Time lost to resolve the situation				
Difficulties in understanding whom I could ask for help				
Personal distress; in particular insecurity and increased fear of frauds				

42) Can you say how long it took you to you to solve the problem?

Answer only if the following rule is fulfilled: the answer to question 15 "*How many times have you suffered an identity theft in your life?*" was equal to or greater than '1'

1 day or less

Some days, but less than a week

1-3 weeks

1-6 months

7-12 months

I am still dealing with the problem

Don't know

Section 4. Social and personal perception of insecurity

In this section we ask your opinion about security and the risk of suffering an identity crime, especially as regards the use of technologies (PCs, tablets, smartphones).

43) Do you think that people should be worried about the risk of suffering an identity crime?

Yes

No

44) Why?

Answer only if the following rule is fulfilled: the answer to question 43 "*Do you think that citizens should be worried about the risk of suffering an identity crime?*" was 'Yes'.

More than one answer is possible

Such crimes are increasingly common

The Internet and new technologies give anonymity and impunity to identity thieves

Identity theft makes it possible to get a lot of money in a short time

Don't know

Other _____

45) Why?

Answer only if the following rule is fulfilled: the answer to question 43 "*Do you think that citizens should be worried about the risk of suffering an identity crime?*" was 'No'.

More than one answer is possible

Such crimes are not particularly common

The Internet and new technologies do not give anonymity and impunity to identity thieves

Identity theft does not make it possible to get a lot of money in a short time

Don't know

Other _____

46) In the past 12 months how much have you thought about possibly being the victim of an identity theft?

A great deal

Somewhat

Little

Nothing

47) To what extent do you think that the following factors increase the risk of identity theft?

	Much	Somewhat	Little	Nothing
Poor control by the police				
Norms too weak				
The ease with which fraudsters can get your personal data (e.g. credit card numbers) from banks and firms				
People's carelessness in protecting their personal data				

48) Indicate here other factors that you think can facilitate identity theft

49) To what extent do you think the following measures should be a priority in protecting citizens?

	Much	Somewhat	Little	Nothing
Creation of a public agency dedicated to identity theft detection and prevention				
Introduction of specific legislation on identity thefts				
More severe punishment of identity theft				
Inform and sensitize citizens				
Creation of a toll free number to report identity thefts and/or obtain information				

50) Indicate here other measures that could provide better protection against identity theft

Contacts

51) Can you give us your email address?

Answer only if the following rule is fulfilled: the answer to question 1 "*According to art. 13 of the Legislative decree 196/2003, I authorize the treatment of my personal data for the purposes of this survey*" was 'Yes'.

If you give us your email, we will inform you when the research report (containing your answers as well) is ready and, if you wish, we will contact you for future research.

This completes the questionnaire.
Thank you.

Digital print: www.rotooffset.it - Trento, Italy

Trento, March 2014

ISSN 2284-3302
ISBN 978-88-8443-529-3