

**REPORT ON IDENTITY THEFT/FRAUD
FRAUD PREVENTION EXPERT GROUP¹**

EXECUTIVE SUMMARY	2
1. INTRODUCTION:	5
2. SCOPE OF THE PROBLEM	7
2.1. WHAT IS IDENTITY THEFT? WHAT IS IDENTITY FRAUD?.....	7
2.2. HOW BIG IS THE PROBLEM?	8
2.3. WHICH ARE THE CONSEQUENCES OF IDENTITY THEFT/FRAUD? THE VICTIMS.....	9
3. THE IDENTITY CHAIN IN THE FINANCIAL AREA	11
3.1. THE LEGAL IDENTITY AND THE AUTHENTICATION METHODS (INTERACTIONS).....	11
3.2. RISKS & VULNERABILITIES	12
3.3. RESPONSES: THE CHAIN OF RESPONSIBILITIES.....	12
4. PREVENTATIVE MEASURES: THE FINANCIAL SYSTEM	17
4.1. PHASE 1: ENROLMENT PHASE (ENTERING INTO A BUSINESS RELATIONSHIP).....	17
4.1.1. <i>Legal obligation: Customer due diligence – how is it applied?</i>	17
4.1.2. <i>Risks and vulnerabilities (phase 1)</i>	21
4.1.3. <i>Responses – weak points? (phase 1)</i>	22
4.2. PHASE 2: USE OF THE FINANCIAL SYSTEM (CONTINUING A BUSINESS RELATIONSHIP).	24
4.2.1. <i>Legal obligation: monitoring the business relationship - how is it applied?</i>	24
4.2.2. <i>Risks & vulnerabilities (phase 2)</i>	26
4.2.3. <i>Responses – weak points? (phase 2)</i>	28
4.3. PHASE 3: END OF THE CONTRACT (ENDING A BUSINESS RELATIONSHIP).....	30
4.3.1. <i>Legal obligation: Monitoring the business relation - how is it applied?</i>	30
4.3.2. <i>Risks & vulnerabilities (phase 3)</i>	30
4.3.3. <i>Responses – weak points? (phase 3)</i>	31
5. PREVENTATIVE MEASURES: ASSISTANCE BY PUBLIC AUTHORITIES	32
5.1. WHAT IS BEING DONE?	32
5.2. WHAT ELSE CAN BE DONE?	33
6. THE PROSECUTION SIDE:	35
6.1. THE NEED FOR EFFECTIVE PENALTIES	35
6.2. POLICE AND JUDICIAL RESPONSES	35
7. CONCLUSIONS	37
ANNEX 1 - APPLICATION FRAUD TYPOLOGIES (CIFAS)	38
ANNEX 2 – OCCURRENCES OF IDENTITY THEFT/FRAUD [FIDIS]	39
ANNEX 3 – DEFINITIONS OF MODUS OPERANDI IN THE ONLINE WORLD	41
ANNEX 4 - SELECTED BIBLIOGRAPHY	45

¹ This paper has been prepared by the FPEG subgroup on identity theft, composed of representatives from several stakeholders, on the basis of the work carried out by a drafting task force. The secretariat to the FPEG is provided by unit F2 of DG Internal Market and Services of the European Commission. None of the views in this paper, however, should be attributed to the European Commission.
http://ec.europa.eu/internal_market/fpeg/index_en.htm

EXECUTIVE SUMMARY

The misuse of personal data to impersonate somebody else and abuse of his/her banking/financial services facilities is a **growing concern** in developed societies. In some EU Member States identity theft/fraud is the fastest growing type of financial fraud. In its Action Plan of 2004 on payment fraud prevention, the European Commission pointed at this problem and underlined the need to strengthen businesses and consumers confidence regarding non-cash means of payment, in particular those used in non-face to face situations.

The **aim of this non-exhaustive paper** prepared by the FPEG is to provide an overview of the identity theft/fraud problem in the financial sector² in particular in the payment and retail banking areas, outlining the main risks and the vulnerabilities all along the identity chain in the financial system.

The first difficulty is to define the **scope of the problem** as there is no clear common definition of what should be understood by identity theft or identity fraud. The most important feature is the appropriation and use of identity data for conducting other illegal activity, in particular economic/financial fraud. From this perspective, "identity" theft/fraud would essentially relate to application fraud and account take-over. For other stakeholders, however, the problem also encompasses the "appropriation and use of identity details" (e.g. a card number or a password), regardless of whether there is full impersonation: for instance, general payment card fraud would also fall under this problem.

Measuring the problem is not easy. On the one hand, it is largely dependent on the type of definition used; on the other hand, some of the consequences for victims are not always easy to measure. Existing figures in Europe seem to suggest at this stage that the identity theft/fraud problem (using a narrow definition) in Europe in connection to payment fraud is touching more severely the UK than any other country in Europe. However, it would be a wrong conclusion to believe that the problem does not concern other EU countries.

Identity theft/fraud in the financial system affects four main kinds of **victims**, essentially governments, private companies detaining large amounts of data, financial services providers and customers (whether businesses or natural persons). The consequences for them vary. There are obviously direct financial losses, e.g. the amounts directly extracted by criminals from the accounts etc, but also indirect costs for businesses, governments and consumers, who may need to clean up their own name.

Zero fraud does not exist. Indeed, there are **vulnerabilities** in the identity chain but also **responses** to those vulnerabilities that can help in reducing current identity theft/fraud levels in the financial system: first and foremost, preventive measures; In addition, the fight against identity theft/fraud cannot be complete without strict prosecution and traditional law enforcement measures.

² Identity theft/fraud is a phenomenon that touches on other areas beyond the financial sector. These other areas are, however, not examined in this paper.

Preventative measures, however, are not the responsibility of an isolated actor within the identity chain, but of all actors. Joint cooperation by stakeholders is therefore needed to enhance security. No one aspect of the identity chain can be managed in isolation.

There are a number of **preventative measures which are applied by the financial system actors** in the three main phases of the business/commercial relationship: enrolment, system use and termination. Risk and vulnerabilities are different (account takeover, false application etc), as well as the responses. There is scope for improvement. First of all, stakeholders point to the lack of sufficient harmonisation of the EU legislation in relation to data protection and to money laundering as a particular problematic point. Secondly, increasing the reliability on documents and verification procedures used could constitute adequate responses depending on the circumstances. Thirdly, customers (and victims) have also a role to play. Fourthly, the banking/payment sector (whether directly or indirectly through data storage service providers) has a particular responsibility in relation to secure maintaining the personal data of their customers. This responsibility also extends to merchants and governments where they kept personal data that can be of relevance for the purposes of identity theft.

Current **solutions for authenticating customers** have limitations and may be relatively insecure. Therefore, there are a number of other measures that could be used to confirm the "contractual identity" of the client. Still very much based on a "what you know" method, they contain other features which make them more reliable: e.g. a more secure authentication. These measures are, *inter alia*: 2 (or more) factor authentication; new generated – not static – passwords for each transaction, also called one-time passwords; VPN connection between bank and customer; site data protection programs, 3D secure card transactions or in home banking (validation by SMS, one time password using a token device; smart authentication card) etc. Biometrics are deemed more secure as they are more closely linked to the person (the iris never leaves the human body, for instance). However, there are concerns about the consequences in case of compromising (e.g. reversibility problem), the ability of the customer to challenge a 'false-positive' and the resistance on privacy and civil liberties grounds.

Concerning **phishing** (and similar scams such as pharming), customer education is important so as to enable him to recognise false messages. Customers should indeed be more responsible for their actions in the internet world. In this context, two-way authentication could improve security. Technology can also help. Moreover, the involvement of internet service providers is key to provide rapid responses (e.g. closing down of fake sites) to his kind of scams, once detected.

Public authorities are also responsible for **preventing identity theft/fraud**. There are several best practices applied by some authorities. First of all, some public authorities (either alone or in cooperation with the financial services industry) are launching awareness and educational measures, including maintaining of devoted websites. Secondly, there are databases kept by public authorities on identity documents, identity related information or on payment instruments. These databases may be accessible beyond the public authorities themselves to the financial services industry, or generally to the public. Thirdly, single contact points allowing citizens to declare identity fraud/theft related problems have been set up in some countries, including third countries.

Generalisation of the best practices described would be welcomed by stakeholders. It appears that more public awareness and education on Internet issues in connection with

financial services are needed. Better communication and cooperation between public authorities is needed. Exchange of information between all parties is also needed, as banking activity (and the related fraud) is becoming increasingly electronic and cross border in nature.

Identity theft/fraud in the payment area is normally not a **criminal offence** on its own, but an enabler for other offences. As a result, there is a vast disparity of penalties applied in Europe. Stakeholders have the perception that those penalties are generally too low to be dissuasive. A certain harmonisation of EU criminal legislation in this regard seems to be supported by stakeholders. The European Commission will be launching a comparative study on the definitions of identity theft used in EU countries and their criminal consequences.

In addition to increasing the deterring effect of penalties, there are **other law enforcement related measures** that could help in increasing the fight against the identity theft/fraud phenomenon. Those measures are not different from those applied against other economic and financial crime.

In conclusion,

- (1) It is important to maintain the integrity of the identity chain. Currently the weakest links of the chain are: the customer's PC (he should be aware of it and be motivated to secure his own environment); the Internet Service Providers; the data storage service providers acting as third parties, as well as the databases operated by merchants and public authorities. In this chain, the responsibility should be taken up by all the parties to the chain, within their own limitations.
- (2) Identity theft/fraud does not only affect the financial sector. Its effects go beyond. Other stakeholders should be associated to this fight.
- (3) It is of great importance make available educational tools for weak parties (citizens and SMEs) in relation to the use of the Internet.
- (4) Technology is part of the solution but will not be the only solution.
- (5) Caring for victims make sense as it should provide for improved trust.

1. INTRODUCTION:

The misuse of personal data to impersonate somebody else and abuse of his/her banking/financial services facilities is a growing concern in developed societies. Concern is growing because, over the course of a lifetime, a citizen will transfer personal information and data to dozens of entities, data which end up being stored electronically in countless destinations and files with little protection. In the United States, there are already over a hundred of thousands of cases per year. In Europe too, this phenomenon, usually referred to as identity theft or fraud, is a growing problem. Organised crime is increasingly moving into this kind of activities with the aim of raising (illegal) revenue. In some EU Member States identity theft/fraud is the fastest growing type of financial fraud.

In its Action Plan of 2004 on payment fraud prevention³, the European Commission pointed at this problem and underlined the need to strengthen businesses and consumers confidence regarding non-cash means of payment, in particular those used in non-face to face situations⁴. Following this Action Plan, the Fraud Prevention Expert Group (FPEG) created a subgroup on identity theft issues which was tasked with preparing a report on this issue.

The aim of this paper prepared by the FPEG is to provide an overview of the identity theft/fraud problem in the financial sector⁵, in particular in the payment and retail banking areas, outlining the main risks and the vulnerabilities all along the identity chain in the financial system. This paper, however, does not pretend to be exhaustive. To this end, the paper will:

- present the scope of the problem (section 2);
- provide an overview of the identity chain in the financial system, outlining the responsibility of all stakeholders (section 3);
- describe the preventative measures which are applied by the financial system actors in the three main phases of the business/commercial relationship: enrolment, system use and termination (section 4). This will normally include the description of end-to-end process of identity verification by introducing the legal obligations and their practical implementation, identifying the risks, and outlining vulnerabilities and responses;
- describe the role of assistance of public authorities in the prevention field (section 5);

³ Communication from the Commission of 20.10.2004, COM(2004)679: 2004-2007 Action Plan to prevent fraud on non-cash means of payment. Available at: http://ec.europa.eu/internal_market/payments/fraud/index_en.htm

⁴ As part of the awareness raising initiatives, the Commission also organised a High Level Conference on 22/23 November 2006 with a view to emphasise the importance of a deeper involvement of policy makers in this connection. The presentations of the conference are available at the Commission's website: http://ec.europa.eu/justice_home/news/information_dossiers/conference_integrity/index_en.htm

⁵ Identity theft/fraud is a phenomenon that touches on other areas beyond the financial sector. These other areas are, however, not examined in this paper.

- present the prosecution and law enforcement aspects of the fight against this phenomenon (section 6); and
- finally provide some conclusions (section 7).

2. SCOPE OF THE PROBLEM

2.1. What is identity theft? What is identity fraud?

The first difficulty is to define the scope of the problem as there is no clear common definition of what should be understood by identity theft or identity fraud. For example, different definitions are used for statistical purposes in different countries, if there is a definition at all. Moreover, in many cases, the terms "identity theft" and "identity fraud" are used as if they had both the same meaning. There have been attempts, however, to delimitate the definition of both terms.

Box n° 1 – Definitions

The **UK Home Office Identity Fraud Steering Committee** has recently provided its definitions for these terms (although they are not legal definitions or linked to specific criminal offences)⁶:

- "Identity Theft occurs when sufficient information about an identity is obtained to facilitate identity fraud, irrespective of whether, in the case of an individual, the victim is alive or dead."
- "Identity Fraud occurs when a false identity or someone else's identity details are used to support unlawful activity, or when someone avoids obligation/liability by falsely claiming that he/she was the victim of identity fraud. Examples include: using a false identity or someone else's identity details (name, address, date of birth etc) for commercial or monetary gain, to obtain goods or access to facilities or services e.g. opening a bank account, applying for a loan or credit card".

CIFAS, a fraud prevention organisation in the UK provides slightly different definitions⁷:

- "Identity Theft - (also known as impersonation fraud) is the misappropriation of the identity (such as the name, date of birth, current address or previous addresses) of another person, without their knowledge or consent. These identity details are then used to obtain goods and services in that person's name."
- "Identity Fraud - is the use of a misappropriated identity in criminal activity, to obtain goods or services by deception. This usually involves the use of stolen or forged identity documents such as a passport or driving licence."

The most important feature is the appropriation and use of identity data for conducting other illegal activity, in particular economic/financial fraud. From this perspective, "identity" theft/fraud would essentially relate to application fraud and account take-over. For other stakeholders, however, the problem also encompasses the "appropriation and use of identity details" (e.g. a card number or a password), regardless of whether there is full impersonation: for instance, general payment card fraud would also fall under this

⁶ See www.identitytheft.org.uk

⁷ See www.cifas.org.uk

problem⁸. Indeed, this view is similar to the concept of identity fraud used in the United States⁹.

Therefore common definition of what the problem is appears desirable: talking of the same thing facilitates preventing and combating it¹⁰. This need was also underlined by the participants to the high level conference organised by the European Commission in November 2006 in this field.

For the purposes of this paper, however, no attempt to find a common definition will be undertaken. The problem will be referred to as "identity theft/fraud".

2.2. How big is the problem?

Measuring the problem is not easy. On the one hand, it is largely dependent on the type of definition used; on the other hand, some of the consequences for victims are not always easy to measure.

If one takes the wide definition of identity theft/fraud, the problem can be considered to be significant. According to the U.S. Federal Trade Commission (FTC)¹¹, identity theft tops the list of fraud activities in the USA in recent years. Around 245,000 complaints on identity fraud were filed over the period January – December 2006. This represents 36% of all fraud complaints in 2006. Out of the identity fraud complaints, payment card fraud represents around 25% of the most common form of reported identity fraud over 2006. Identity fraud in the on-line world is still growing¹².

Statistics about identity fraud in Europe are also available, but usually on a piecemeal basis. If we take the example of the United Kingdom, according to the latest Home Office estimate¹³, identity fraud costs the UK economy £1.7 billion annually. It is estimated that more than 100,000 people are affected by identity theft in the UK each year. Of this total cost in the UK, losses resulting from payment cards being used by criminals pretending to be the rightful owner or by criminals using a fictitious identity

⁸ This view is challenged by others, who consider that such a wide definition is not appropriate: e.g. the use of customer card data details do not allow for generally conducting other kind of financial fraud, but merely payment fraud.

⁹ For an overview of the identity theft/fraud phenomenon in the US, see the website of the US Federal Trade Commission (www.ftc.gov). For a comparative description of the legal responses in the US and the UK, see Binder and Gill, "Identity theft and fraud: learning from the US, Perpetuity Research and Consultancy International, 2005.

¹⁰ The FIDIS research project is inter alia examining this issue. FIDIS (Future of Identity in the Information Society) is a network of excellence supported by the European Community under the 6th Framework Programme for Research and Technological Development. Work Package 5 of the FIDIS project deals with identity theft. See in particular Deliverable 5.2b, *ID-related crime: towards a common ground for interdisciplinary research*, May 2006. See www.fidis.net.

¹¹ <http://www.ftc.gov/bcp/edu/microsites/idtheft/reference-desk/national-data.html>

¹² <http://www.ftc.gov/opa/2006/01/topten.htm>

¹³ Updated estimate of the cost of identity fraud to the UK economy, February 2006, www.identity-theft.org.uk.

amounted to £504.8 m (the highest amount of all estimated types of identity fraud¹⁴), with the following repartition:

<i>Counterfeit (skimmed/cloned) cards</i>	<i>£129.7m</i>
<i>Cards lost or stolen</i>	<i>£114.4m</i>
<i>Card not present</i>	<i>£150.8m</i>
<i>Mail non-receipt</i>	<i>£72.9m</i>
<i>Fraudulent applications</i>	<i>£13.1m</i>
<i>Account takeover</i>	<i>£23.8m</i>

If, on the contrary, one uses a narrower definition of identity theft/fraud (e.g. fraudulent applications and account takeover cases only), the problem in Europe is still important, but its scope is limited compared to the other fraud typologies. It is also interesting to note that according to the intervention of a major payment card scheme at the high level conference of November 2006 organised by the European Commission, account takeover and application fraud cases in the UK accounted for around three quarters of all cases of these types of fraud in Europe (including non EU Member States). This seems to suggest at this stage that the identity theft/fraud problem (using a narrow definition) in Europe in connection to payment fraud is touching more severely the UK than any other country in Europe.

However, it would be a wrong conclusion to believe that the problem does not concern other EU countries. According to a Dutch Financial Institution who registered false applications since 2004, application fraud is on the rise. In 2004, this institution identified 380 false applications, 470 cases in 2005 and in the first quarter of 2006, it registered 151 cases of false applications.

2.3. Which are the consequences of Identity Theft/Fraud? The victims.

Identity theft/fraud in the financial system affects four main kinds of victims, essentially governments, private companies detaining large amounts of data, financial services providers and customers (whether businesses or natural persons). The consequences for them vary. There are obviously direct financial losses, e.g. the amounts directly extracted by criminals from the accounts etc. These financial losses are covered, in most cases, by the financial institutions themselves in the end. However, consumers may also suffer direct losses. There are also indirect costs for businesses in so far as they should upgrade their prevention systems. Both the direct financial losses and the indirect costs are likely to be passed on, as costs, to the final clients of financial institutions, thus contributing to diminution of the performance of the financial system. Governments may also suffer from direct financial losses (in some cases there are identity theft/fraud cases against public bodies), but essentially bear indirect costs in relation to prevention and law enforcement systems. In any case, any direct loss would also be indirectly passed on to consumers as taxpayers.

There are also associated indirect costs for consumers, who may need to clean up their own name. Estimations in the UK¹⁵ indicate that a victim may employ between 3 and 48

¹⁴ Interestingly, no figures are provided in relation to e-banking fraud, due to lack of specific statistics. The UK 2002 Study further indicates that "the financial cost of identity fraud is almost certainly under-reported. In the private sector, in particular, it is suspected that much identity fraud is not fully investigated or categorised as such, being written off instead as "bad debt"". See UK Cabinet Office, *Identity Fraud: a Study*, July 2002, p. 13.

hours of time in cleaning his/her name after an identity theft/fraud attack, which appears to be significantly less than in the US, although in some cases it took up to 6 months. In addition, there are the emotional costs for victims which, though difficult to quantify, should not be underestimated. In the CIFAS survey, "about half of the victims said that their experience had a big impact on their stress and health levels, and slightly more claimed that it caused them great inconvenience"¹⁶.

Further to these financial losses, there are reputational risks involved. First to governments, as the identification documents they deliver may suffer from discredit. Second to the financial system itself, as consumers may lose confidence in non-cash means of payments¹⁷. Additionally, there are reputational problems for data storage service providers and financial sector providers, which affect the entire market environment and the business model itself.

¹⁵ See the study conducted for CIFAS: *Identity Fraud: What about the Victim?*.

¹⁶ The CIFAS website discloses some case histories:
http://www.cifas.org.uk/identity_fraud_case_histories.asp.

¹⁷ On the question of consumer confidence in non-cash means of payment, see the study conducted by PwC for the European Commission in 2003: *Study on the Security of Payment Products and Systems in the 15 Member States*. Available at:
http://ec.europa.eu/internal_market/payments/fraud/index_en.htm#studies

3. THE IDENTITY CHAIN IN THE FINANCIAL AREA

Fraudsters are always moving towards the weakest link. In Europe, cards are being secured against counterfeit attempts through the introduction of the EMV chip. So, fraudsters will have an incentive to move to a different activity which may provide them with easier access to victims' accounts: i.e. obtaining original cards through identity theft/fraud. This is why it is needed to secure the information required to commit identity theft/fraud.

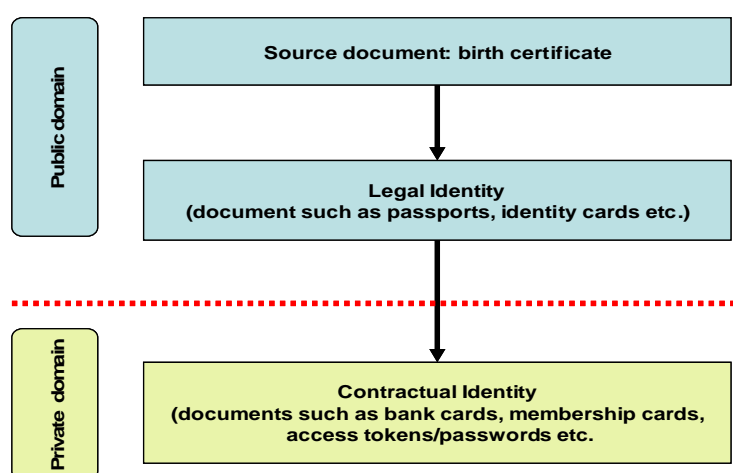
3.1. The legal identity and the authentication methods (interactions)

First and foremost, a personal identity is composed of attributes that are unique to an individual (so-called biometric identity), i.e. fingerprints, voice, retina, facial structure, DNA profile, hand geometry, heat radiation, etc.

However, in the context of identity theft/fraud, the interest does not really lie on such biometric identity, but rather on the attributed identity or initial legal identity. The components of such attributed identity are essentially those given at birth, including full name, date and place of birth, parents' names and addresses, nationality etc. Indeed, for the financial world, these identity details are normally the most relevant. They are also supplemented with some biographical elements of the identity¹⁸, which builds up over time, notably the address.

Governments can issue a legal identity (and/or identity documents, which are compulsory in some countries but not in others). A legal identity is based on a source document, generally a birth certificate. Indeed, the legal proof of identity is normally the responsibility of the state.

This identity (possibly backed by a document) can be taken in turn to personalize an "authentication method", such as: bank accounts; debit/credit cards; tokens etc.



¹⁸ The biographical identity covers life events and how a person interacts with structured society, including: registration of birth; details of education/qualifications; electoral register entries; details of benefits claimed/taxes paid; employment history; registration of marriage; mortgage account information/property ownership; insurance policies; history of interaction with organisations such as banks, creditors, utilities, public authorities, etc. See UK Cabinet Office, *Identity Fraud: a Study*, July 2002, p. 17.

This report will focus on issues related to the authentication category. These categories of authentication methods are not really identities or legal identity documents, although they carry sometimes identifying information (or "identity details") on them that can lead to a legal identity.

3.2. Risks & vulnerabilities

The appropriation and subsequent misuse of the identities or of the "identity details" is a serious concern for the financial system, as well as for its users. Such appropriation or misuse can take place at any level of the identity chain in the financial sector. It is important to underline that there are vulnerabilities at any level of the chain, whether regarding the legal identity or regarding the authentication.

The main vulnerabilities at the level of the legal identity are:

- the Identity identification performed by Governments (ones wrongly identified always wrongly verified);
- personal data collection and storage by the public authorities;
- the quality of and trust in the legal identity documents issued by Governments are critical in a proper identification of the natural person who applies for a financial service. However, the type and quality of identity documents issued by government (passports, driving licences, national identity documents etc) is disparate. Such variability in type will continue and increase with moves by some countries towards incorporating biometric data. Unsurprisingly, legal identity documents are forged, some more easily than others. Even latest technology documents (e.g. electronic cards) might not totally free from falsifications. It should be also recognised, however that identity fraud/theft today is a major problem in countries where no national identity document exists and where identification relies on documents which can be easier to forge (documents which do not bear a photograph etc.).

At the level of authenticating a customer, there are also vulnerabilities. Many financial transactions which require the identification of the client are conducted either on a non-face to face basis, or if in person, between individual who are strangers to each other. This easily results in an asymmetry of the information available to the parties, which turns to the advantage of the fraudster: e.g. the "authentication methods" may be based on false or forged details presented by the fraudster, or the fraudster may use true identity details belonging to somebody else for his own benefit. Indeed, the ability of private companies to access the necessary controls to properly assess these documents when presented as evidence of identity is variable. Specific additional risks arise wherever businesses outsource parts of the 'identity chain management' process. Commercial considerations also play a role: businesses need to conduct client identification and acceptance at speed and in a cost effective way.

No one document will ever provide a panacea for all identity verification.

3.3. Responses: the chain of responsibilities

Zero fraud does not exist. As the UK 2002 Study points out: "we will never completely eliminate identity fraud, but that there is much that we can do to make life very much

more difficult for the organised criminal – and the opportunist¹⁹. Indeed, there are **responses to those vulnerabilities identified above** that can help in reducing current identity theft/fraud levels in the financial system:

- First and foremost, preventive measures
- In addition, the fight against identity theft/fraud cannot be complete without strict prosecution and traditional law enforcement measures.

The chain of responsibilities in the prevention of identity theft. Preventative measures, however, are not the responsibility of an isolated actor within the identity chain, but of

All parties are responsible in maintaining the integrity of identities

all actors. Joint cooperation by stakeholders is therefore needed to enhance security. No one aspect of the identity chain can be managed in isolation. Personal data needs to be protected, be it at the level of collection, storage or communication. All stakeholders bear (at least partial) responsibility in maintaining the integrity of identities²⁰. Each part of the chain needs to be competent enough to ensure security of the whole chain. This also includes consumers, who are part of the problem but also of the solution.

The course to technology. The first question in this connection is how secure should the payment methods, data collection/storage and communication channels with customers be²¹. Appropriate levels of technology are important in relation to security of product, product characteristics, data storage, access controls etc. It is true that there is available technology that could render identity theft/fraud more difficult or even inexistent. But this technology is in most cases either too expensive and too complex to implement (which renders it commercially unsuitable) or possibly too privacy-intrusive (in particular in the case of biometrics²²). Therefore, the prevention of and the fight against

¹⁹ UK Cabinet Office, *Identity Fraud: a Study*, July 2002, p. 3.

²⁰ See also Leenes (ed.), FIDIS network, deliverable 5.2b, *ID-related crime: towards a common ground for interdisciplinary research*, May 2006, p. 95 and seq. This study explains that identity theft/fraud involves people (victims and fraudsters) and machines (e.g. devices and protocols & software), and that countermeasures can address both people (social aspects) as well as the machines and the interaction between the two (technical aspects). Often, three types of trust are needed in order to prevent identity theft as much as possible: (i) trust in a user that he keeps certain information secret; (ii) trust in the authenticating party to keep the data obtained for and during authentication secret and not disclose or leak the data to others that may sue them for malicious purpose; and (iii) trust in devices and protocols & software, leading to trust in the producer/verifier of the devices/software that their products will not leak information and will resist attacks.

²¹ See the upcoming 2007 Commission study on user identification methods in card payments, e-payments and m-payments.

²² See UK Cabinet Office, *Identity Fraud: a Study*, July 2002, op. 61: "Biometric systems come in a number of forms, including fingerprint verification, hand-based verification, retinal and iris scanning, DNA verification, facial recognition, voice recognition and signature recognition.

Biometrics offer a number of benefits. There is a far lower risk of counterfeiting than exists with documents. Biometrics cannot be lost or forgotten and checking processes are less susceptible to human error than, for example, checking photographs. All things considered, biometrics offer the highest level of security verification available.

current levels of identity theft/fraud are necessarily a combination of (i) the reduction of this evolving technology gap as well as (ii) other preventative measures. This paper will not focus on the technological developments of payment methods²³, but rather on the other preventative measures.

The financial industry response. Despite the responsibility of all actors, the vulnerabilities described call in particular for the development of a stringent authentication and verification policy within the financial industry. The purpose of a more stringent policy is to enable the establishment of someone's identity or the verification that the person involved is the right one in increasingly more situations and with greater reliability. The importance of the distinction between these two forms of identity check is that verifying that someone is the right person doesn't necessarily require knowledge of who he is. This will gain more importance in keeping up with the growing number of transactions that are conducted electronically and at a distance without social control or visual supervision. Indeed, identity checks are more and more likely to be performed electronically and at a distance.

The influence of legislation in the preventative measures. There are no specific identity theft/fraud rules at EU level²⁴. However, two main set of rules at European level are applicable to identification/verification of identity issues and indirectly contribute to the preventative measures adopted by the financial industry and other actors.

- On the one hand, the anti-money laundering legislation²⁵ establishes: (i) which institutions should identify customers and verify their identities; (ii) circumstances when identity verification is required; and (iii) that supporting evidence is needed. This European anti-money laundering legislation harmonises the national legal framework to certain extent, still it does not impose a unique solution.
- On the other hand, the privacy legislation establishes limits and guarantees to the processing of personal data by financial institutions²⁶.

The human factor has a non negligible influence on the prevention side.

But there are drawbacks. First, they are expensive: in addition to the cost of issuing the biometric, "reading" equipment is required. There are issues around public acceptability. Biometric systems are by no means foolproof: all types of biometric systems currently available run the risk of reporting "false positives" or "false negatives"; around 10–15% of "genuine" people will fail the test if it is set to minimise the numbers of fraudulent people let through. This is very much a developing area. Biometrics offer undoubted potential, but it is a potential which has yet to be realised in any large scale applications."

²³ For a description technology issues, see Leenes (ed.), FIDIS network, deliverable 5.2b, *ID-related crime: towards a common ground for interdisciplinary research*, May 2006, p. 97 and seq.

²⁴ For a description of the legal situation in some EU Member States, see Owen, Keats and Gill, *The Fight Against Identity Fraud: A Brief Study of the EU, the UK, France, Germany and The Netherlands*, Perpetuity Research & Consultancy International, June 2006.

²⁵ http://europa.eu.int/comm/internal_market/company/financial-crime/index_en.htm#moneylaundering

²⁶ On privacy issues, see the report established by the FPEG on data management of 8 December 2006, available at: http://ec.europa.eu/internal_market/fpeg/work_en.htm

- Personal behaviour may have important consequences in the prevention of identity theft/fraud activities. In general, the consumer is the weakest link in security due to lack of knowledge and protection, in particular in the on-line environment. Natural persons need to understand in this regard the importance of their legal identity document(s), which is(are) vulnerable for misuse. Individuals also need to understand the value of their financial details and be aware of the risks they may face, in particular in the on-line world. Apart from the actual damage, identity theft/fraud lead to additional problems to consumers by giving rise to suspicion and damaging the identities reputation. Consumers need effective prevention, repression and assistance as victims. It is in their interest to make use of recommended security advice and of protection systems offered.

Consumer protection rules also have implications. A Commission recommendation²⁷ which has been implemented throughout Europe recommends that consumers shall bear the loss of unauthorised transactions up to a maximum of 150 € provided they have not acted with extreme negligence. The recently agreed Payment Services Directive amends the provisions of this recommendation by providing that consumers' liability will be limited in the same way even if they have "failed to keep the personalised security features safe from misappropriation of a payment instrument"²⁸. Some stakeholders (notably industry) fear the impact of this provision for the level of fraud prevention: jurisdictions will indeed be faced with substantial difficulties when interpreting these contradicting provisions. At the same time, these stakeholders believe consumers will be discouraged to be vigilant: why offering 3D secure services if the law encourages consumers to keep their payment instrument in an unsecured environment?

- Cultural differences are also important. The differing cultural attitudes to what is considered acceptable as public or private information have an influence on the way to treat identity issues (e.g. compare the Swedish open access to tax information compared to the French culture of protecting financial privacy). Cultural differences also apply to the provision of financial services. In France and Belgium, for instance, *every person* has the right to apply for a bank account, subject to the fulfilment of specific conditions – at the same time, the enrolment phase is considered to be of more bureaucratic nature. In Anglo-Saxon countries, enrolment procedures tend to be more flexible, though no particular rights of access to bank accounts are granted. While the end result may be similar, these differences have different implications as regards the establishment of contractual relationships.

Finally, there are different cultural attitudes with regard to security issues too. In some countries, customers do accept stringent identification requirements from financial institutions more easily than in others, where privacy concerns may prevail.

The role of public authorities on the prevention side. Further to their legislative production, public authorities also have a role to play as regards the prevention of identity theft/fraud.

²⁷ Recommendation (97/489/EC)12 of 30 July 1997 concerning transactions by electronic payment instruments and in particular the relationship between issuer and holder, OJ L 208, 2.8.1997, p. 52.

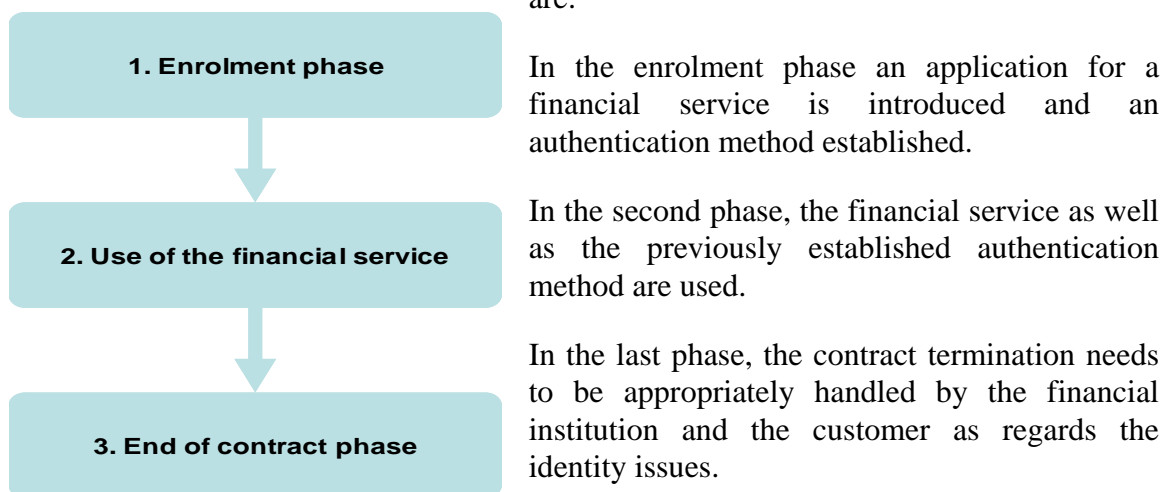
²⁸ See in particular Article 50(1) of the draft Payment Service Directive as agreed by the European Parliament and the Council. The definitive text has not been yet formally adopted and published.

This paper will examine in further detail those preventative and reactive measures.

- ➔ **Section 4, for the preventative measures in the financial system;**
- ➔ **Section 5, for the assisting role of the public authorities;**
- ➔ **Section 6, for the reactive measures (prosecution and law enforcement).**

4. PREVENTATIVE MEASURES: THE FINANCIAL SYSTEM

Participation in the Financial System can be divided in three main phases. These phases are:



Each of these phases has its own risks, vulnerabilities and responses. They will be respectively examined in the following subsections.

4.1. Phase 1: enrolment phase (entering into a business relationship).

4.1.1. *Legal obligation: Customer due diligence – how is it applied?*

Identifying a possible new customer in the financial world consist of two actions. During the first action, a financial institution identifies the possible new customer by collecting information from him. In the second part of the action, the financial world has to verify the information received through the first action²⁹.

The legal obligation: customer due diligence. The identification of clients in the financial world is subject to some legal obligations, mostly deriving from prudential requirements (e.g. "know your customer" – Basel Committee) and from anti-money laundering legal obligations (e.g. "customer due diligence procedures"). At EU level, the main anti-money laundering obligations are set by Directive 2005/60/EC³⁰ on the prevention of the use of the financial system for the purpose of money laundering and terrorist. The European Legal framework is the basis for national legislation within the Member States of the European Union.

²⁹ Identification: Issuing an official source document that proves the identity of a person is an exclusive right of Governments. This is based on Identification. Identification requires research. An important aspect of identification is that a person is actually present. The aim of identification is to secure each person's true identity.

Verification: Identity verification is generally sufficient for legal acts in a private context. If, for instance, a private organisation agrees to grant a loan to a person, it is then sufficient to ask for proof of identity and to check the validity of the proof of identity shown.

³⁰ Directive 2005/60/EC is not totally new and builds on previous legal texts, notably the first directive on Prevention of the Use of the Financial System for the purpose of Money laundering (91/308/EEC) and the 40 recommendations of the Financial Action Task Force of 1990, modified in 2001.

Box n° 2 - EU Anti-money laundering obligations - Identification of clients

Directive 2005/60/EC establishes:

- Article 7: "The institution and persons covered by this Directive shall apply customer due diligence in the following cases: (a) when establishing a business relationship; [...]"
- Article 8: "Customer due diligence measures shall comprise: (a) identifying the customer and verifying on the basis of documents, data or information obtained from reliable and independent source; [...]"

The institutions and persons covered by 2005/60/EC should also, in conformity with this Directive, identify and verify the identity of the beneficial owner. To fulfill this requirement, it should be left to those institutions and persons whether they make use of public records of beneficial owners, ask their clients for relevant data or obtain the information otherwise, taking into account the fact that the extent of such customer due diligence measures relates to the risk of money laundering and terrorist financing, which depends on the type of customer, business relationship, product or transaction.

According to Directive 2005/60/EC, to avoid repeated customer identification procedures, leading to delays and inefficiency in business, it is appropriate, subject to suitable safeguards, to allow customers to be introduced whose identification has been carried out elsewhere (third party introduction or derive verification). Where an institution or person covered by this Directive relies on a third party, the ultimate responsibility for the customer due diligence procedure remains with the institution or person to whom the customer is introduced. The third party, or introducer, also retains his own responsibility for all the requirements in this Directive, including the requirement to report suspicious transactions and maintain records, to the extent that he has a relationship with the customer that is covered by this Directive.

The Directive also requires to apply enhanced customer due diligence measures in the case of non-face to face relations with the customer³¹.

The practice. The enrolment phase can take place in the physical world or in the online world.

- In the physical world, the enrolment phase starts when a person applies for financial services. The application is mostly made in person at a financial institution in a face-to-face situation.
- In the online world, the enrolment phase starts with a person's application for a financial service online³². This means that there is no face-to-face contact between the financial institution and a potential new client.

The application form or the on-line application requires at least the following information from the applicant³³: surname, first name, date of birth; address, place of residence, phone number(s), etc.

³¹ See the European Commission Staff Working Document, *The application of Directive 91/308/EEC on the prevention of the use of the financial system for the purpose of money laundering in relation to the identification of clients in non-face to face transactions and possible implications for electronic commerce*, SEC(2006)1792, December 2006.

³² Call centres are an in-between situation, where applications are done in a non-face to face manner but still there is a direct contact with a human being.

³³ See for instance the "General Guide to Account Opening and Customer Identification", February 2003, attachment to Basel Committee publication n°5 "Customer Due Diligence for Banks". This

As proof of identity the applicant has to provide an official or other reliable identifying document. In the European Member States this means legal documents containing identity details such as: Passports, Identity cards, Driving licenses, etc. The quality of the official identity documents provided by Public Authorities is absolutely crucial to ensuring that the person enrolling for banking services is legitimate. The personal information provided by the applicant will be verified with the personal information mentioned in the document. The authenticity and the validity of the document must be checked. A copy of the document must be added to the application form as part of the overall application.

It is possible that other (identifying) information is required like information about the applicant's residence, his profession and the financial situation. Sometimes the applicant is also asked to provide a copy of a phone bill, an electricity bill or another document as proof of residence.

Additionally, in some cases the identity details will be checked against accessible databases containing personal data. Combining different authentication methods is important for prevention purposes.

Box n° 3 - CIFAS – the UK's Fraud Prevention Service

In the United Kingdom, the fraud prevention service CIFAS operates a database which is used by the majority of the British financial services industry. It was established in 1988. Its founder members in the retail credit industry were joined firstly by finance and leasing organisations, then banks and credit card issuers, followed by building societies and mortgage lenders. Today the CIFAS membership extends beyond consumer credit and encompasses telecommunications, factoring, insurance, utilities, share dealing and commercial credit. CIFAS services are offered not just to Members but also to the general public through its Protective Registration Service which helps to protect consumers from identity fraud. Its membership totals around 260 organisations. It is a not-for-profit fraud prevention data sharing scheme.

Membership of CIFAS is needed in order to have access to the database. The database pools information provided by Members on cases where they have been defrauded, or someone has attempted to defraud them. Members of CIFAS are required to operate effective in-house procedures to enable fraud or attempted fraud to be identified. Cases are classified into different types, including "Identity Fraud" and people involved in each fraud can be further classified; e.g. as the "Victim of Impersonation". CIFAS only contains information on frauds and attempted frauds confirmed to a high level of evidence, but not on suspected frauds where the possibility of a Member making an error would be higher. Indeed, Members must be prepared to make a formal complaint to the police on the information they add to the database. Members are able to delete or amend data, so that it is kept up-to-date.

When a Member checks customer details, usually on an application for financial services, against the CIFAS database, it will be advised if another Member has filed a CIFAS warning at any of the addresses on the application. When a Member receives a warning, it accesses the CIFAS database over the Internet to obtain full details of the fraud the other Member has filed. This assists it with its own investigation into potential fraud. In simplistic terms, a Member openly advises all other Members that it has been defrauded, or someone has attempted to defraud it, from these addresses with these details. Another Member, receiving an application from any of these addresses, is immediately put on notice that a fraudster may be applying to it and it can then make detailed checks. A match with a record on the database is a warning and no more. Following the Member's investigation, it will either notify CIFAS of a further attempt to commit fraud or, if the application is not fraudulent, proceed with its normal account opening process. The Member cannot automatically

guide details the information that should be obtained (where applicable) in relation to natural persons and corporates/institutions.

reject an application or close an account just because a warning has been matched. The Member cannot use a CIFAS warning in a scoring mechanism. It is important to note that CIFAS is not considered, nor does it qualify as, a credit reference agency providing information on the financial standing of individuals.

The database contains numerous personal data safeguards and is deemed to be compliant with UK data protection legislation.

In some countries, specific practices have been developed.

Box n° 4 – Specific practices

The Netherlands

If in the Netherlands a person applies for a financial service his /her identity has to be verified based on *Wet identificatie dienstverlening (WID)*. According to the WID financial institutions have to verify the identity of potential new customers as well as of existing customer in relation to the execution of various financial transactions. For the verification of identity legal documents such as passport, driving licenses, national identity cards, identity cards for refugees etc. are accepted. According to internal rules within financial institutions in the Netherlands documents must be verified in the VIS (Verification of Identity Systems) database, which keeps details of lost and stolen documents (see section 5).

France

Banks must check the identity of the person before opening a bank account. They do it on the basis of “any official document bearing a photograph” (article L.563-1 of the Financial and Monetary Code). Valid ID cards, passports, driving licences, card of war veteran, can be considered as “official document”. They must also check his/her domicile (bills, proof of ownership of the domicile, etc.). Most credit institutions send a letter to the address given by the applicant and consider it valid if the letter is not returned. When opening bank accounts in a remote way, banks would apply identical procedures and in case of doubts require the applicant to provide additional proof of identity and domicile.

Belgium

The identity of the customer has to be verified on the basis of the national identity card, the passport or a resident’s permit. The new Belgian ID card is an electronic ID card with chip. The bank branches are equipped with “bank branch devices” and the ID card has to be read when the account is opened in face-to-face. When the account is opened via Internet or the loan is requested remotely, the financial institution must ask for a copy of the ID card and the customer has to prove his address by other means, such as an electricity bill. The financial institution must archive an electronic copy of the ID card of its customers and this is being audited on a regular basis by the banking supervisor. The ID card numbers that have been stolen in blank can be checked via Internet.

United Kingdom

The following information should be established and independently validated for all private individuals whose identity needs to be verified: (a) true full name and/or names used; and (b) current permanent address, including postcode. The information obtained should provide satisfaction that a person of that name exists at the address given and that the applicant is that person. Where a new residential address cannot be proved then the previous residential address should be verified. The confirmation of name and address should be established by reference to a number of sources. The checks should be undertaken by cross validation that the applicant exists at the stated address either through the sight of actual documentary evidence, or by undertaking electronic checks of suitable databases, or by a combination of the two. The checks may include the use of internal or external systems to target previously identified high-risk fraud areas.

In the United Kingdom, the following suitable documentary evidence for UK-resident private individuals are commonly used:

- Personal identity documents such as: Current signed passport; EEA member state identity card; Current full UK driving License (old version); Shotgun or firearms certificate; etc.
- Documentary evidence of address such as: Record of home visit; Recent utility bill or utility statement etc.; Local authority tax bill; Solicitor's letter confirming recent house purchase or land registry confirmation; etc.

In a non face-to-face verification at least one additional measure or check is required to supplement the documentary or electronic evidence.

In 2005/2006, there was a Public-Private identity verification pilot for a period of eighteen months between four major UK bank and the UK Passport Services. During the identity verification pilot the four banks were able to verify the validity of UK passports directly at the UK Passport Services. The pilot was successfully evaluated. Currently (June 2007), there are no facilities to check the validity etc. of personal identity documents.

In today's financial environment particularly with the growth and expanded use of the Internet, fraudulent applications are now becoming a source of substantial risk to financial institutions, often causing significant losses in individual cases. That is why applicant information verification and risk assessment are such critical steps when opening a new client account. There is no European remedy or single tool that can totally eliminate application fraud risk. However, the more accurate, verifiable information available, the better Financial Institutions can evaluate risk and avoid losses. Procedures to verify the application information and tools vary from Financial Institution to Financial Institution. It is up to each financial institution to decide which application items to validate and how.

Application acceptance: the request for financial services and payment instruments.

Applications are introduced in connection to a particular financial service and, in some cases, to a payment instrument. This includes applications for on-line/e-/phone banking, e-payment services, mobile payment services, payment cards, etc. Applications for payment cards (e.g. personalised physical payment instruments that need physical delivery) present some particularities.

4.1.2. Risks and vulnerabilities (phase 1)

The enrolment phase is identified as a critical moment because this is the moment when the correct identity has to be caught. However, this task is getting more complicated because of technological progress and the wider use of non-face to face identification procedures, in particular (but not only) in the on-line world. The main risk in this enrolment phase is **application fraud (or false application)**, that is to say, the use of false personal details (including identity documents) to apply for a financial service³⁴.

**Main risk:
application fraud**

In order to make a false application, the fraudster needs first to **obtain personal data** on the legal identity of another person (or on the "authentication methods" if the fraudster intends to ask for a secondary financial service: e.g. a credit card linked to an existing

³⁴ Some examples prepared by CIFAS are provided in Annex 1.

account). There are many ways to obtain personal data, they are examined in more detail in section 4.2.

Secondly, the (false) application will be **treated by the financial service provider**. The vulnerable areas specific to this application processing, both in the case of face to face and non-face to face applications (such as call centers or the online world)³⁵ are as follows: dishonest employees with access to personal information; the security in general where the application is processed; lack of reliable verification possibilities; level of knowledge about identity documents during the enrolment phase, accepting copies of legal identity documents and other verification documents; application for financial services without opening a bank account; or outsourcing of application assessment and acceptance outside Europe (not covered by European Data protection); production files forwarded for the attention of card producers.

Additionally, in the case of the on-line world there are special vulnerabilities: no special tool available that can identify and prevent fraudulent Internet applications; lack of knowledge about the Internet Protocol (IP) address of each applicant, date and time of application and the duration of time applicant spends at a site of a financial institution; no standardised application forms (with analysis capabilities); and efficient online security against illegal access. It should be noted that the on-line world present particular features: the playing field (i.e. Internet or other telecommunications networks) is not entirely controlled by the financial institutions. Call centers are also reputed for being a weak link in the integrity of the identity chain, particularly in relation to the involvement of staff in the compromise of personal data about customers.

An important vulnerability in this phase is **predictability**. Identity documents and identity checking procedures are governed by regulations (see above). These regulations, however, unintentionally play into the hands of the identity fraudster. They enable him to predict where, when, how and by whom his identity will be checked. Moreover, identity verification procedures are often public and can be inconspicuously observed in order to establish weak points in the technology, the organisation or the procedures. With a certain amount of preparation, an identity fraudster can outwit most identity checks.

4.1.3. Responses – weak points? (phase 1)

First of all, stakeholders point to the lack of sufficient harmonisation of the EU legislation in relation to data protection and to money laundering as a particular problematic point.

- ***The limitations to the management of suspicious data.*** Data sharing is widely used by the private sector in its efforts both to prevent and detect fraud, including identity fraud. In the public sector too, data sharing can be a useful tool in the detection and investigation of crime³⁶. Stakeholders are of the opinion, however, that there are barriers to increased sharing of data, including legal barriers. National data protection legislations seem to significantly differ from country to country, leading to different access levels to verifiable data related to identities. This makes it almost impossible for a financial institution to conduct a consistent prevention policy across Europe. In

³⁵ Call centers handle telephone applications, transactions, changes of personal details.

³⁶ Acknowledged in UK Cabinet Office, *Identity Fraud: a Study*, July 2002, p. 29.

addition to the segmentation effect, another problem relates to the type of personal data that can be processed without infringing the law. There is no possibility for the financial institutions to keep data on suspected identities or individuals, further than the (limited) possibilities offered by the anti-money laundering legislation³⁷.

- ***The risk-based approach and the diminution of predictability.*** Financial institutions also claim that the anti-money laundering legislation is not sufficiently harmonised either as regards the procedures for client's acceptance. Still, the new EU legislation has taken a different approach in this regard, granting more freedom to financial institutions in evaluating the risks involved and in applying the customer due diligence procedures. The application of the risk-based approach should make the policy of financial institutions less predictable for fraudsters and therefore reinforce the prevention effect of the customer due diligence procedures.

Secondly, increasing the reliability on documents and verification procedures used could constitute adequate responses depending on the circumstances.

- ***Higher reliability on documents.*** The enrolment phase heavily relies on documents to confirm the identity of the customer. However, there are numerous ways fraudsters can obtain false documents. Hence, there is value in developing cross-industry tools to identify the false/forged documents. Additionally, access to 'negative databases' (containing data for instance on lost and stolen primary source identity documents such as passports, national identity documents, driving licences etc) could be of particular help (*see section 5 on the assistance by public authorities*).
- ***The increased role of electronic identity verification vs traditional verification.*** One enabler of speedy verification of volume identities is the increasing use of electronic verification. Whilst face to face verification has long been considered the pre-eminent method of verification, business is turning in some markets more and more towards verification through electronic sources. Electronically verified identities often have a 'longer footprint' than the traditional 'snapshot in time' approach of simple one-document face to face verification: e.g. a driving licence, even if entirely genuine at the time of production, merely shows that at the date of issue a person who looked like the photograph was authorised to drive and lived at a particular address. On the contrary, data from credit reference agencies (increasingly used in some countries) or accessible from public sources (e.g. voter's registration in the United Kingdom) may indicate a ten year period in someone's life, several addresses, a pattern of legitimate consumer behaviour, loans etc³⁸. Nevertheless, despite its value electronic verification has its own limitations. First, electronic searches ultimately have to have been derived from a more traditional type of verification. Second, such verification methods can unintentionally exclude certain

No one method of identity verification will suit all purposes.

³⁷ See the report established by the FPEG on data management of 8 December 2006, available at: http://ec.europa.eu/internal_market/fpeg/work_en.htm

³⁸ This is recommended by the Guidance Notes prepared by the UK Joint Money Laundering Steering Group (JMLSG), January 2006. The JMLSG, an industry body, has issued guidance notes to help organisation across the financial services sector with the interpretation of the anti-money laundering legal requirements. The guidance includes procedures with regard to the identification of the customer. The guidance notes are not legally binding.

groups, such as students or the elderly. Third, while electronic verification can confirm the consistency of the various proofs presented by an applicant, it cannot verify that the person providing the information is the person mentioned in the information. In any case, no one method of identity verification will suit all purposes. All channels have vulnerabilities and some may be more suitable for certain businesses and processes.

Thirdly, customers (and victims) have also a role to play.

- ***The monitoring role of customers over their personal data stored by other stakeholders.*** Some stakeholders claim that in some EU countries the balance in favour of personal data protection is undermining attempts to properly combat identity abuses. In Sweden, where personal tax data is public, the agency in charge has specific controls that allow consumers to alert the authorities to abuse of their data, and thus minimise the on-going impact of such an abuse (i.e. the often circular arguments with institutions about who a person is, and whether he or his identity has been responsible for certain actions).
- ***The protective measures by victims of identity theft.*** In the United Kingdom, CIFAS³⁹ (see also box n° 3 above) provides a protective registration service to people who have had their identity documents stolen or are otherwise concerned that they may have been the victim of identity theft. This is a system whereby individuals may request, for a small fee, to be included in the database (by flagging their own address) to protect them against possible impersonation attempts. There are processes in place to ensure the person reporting the theft is the true owner by crime reference numbers or sending a confirmation form to the address on file. There are similar databases in other countries (e.g. Spain⁴⁰, Sweden) also containing identity theft/fraud victims' voluntary registration.

Fourthly, the banking/payment sector (whether directly or indirectly through data storage service providers) has a particular responsibility in relation to secure maintaining the personal data of their customers (see [section 4.2](#), especially in relation to electronic databases and the hacking risk). This responsibility also extends to merchants and governments where they kept personal data that can be of relevance for the purposes of identity theft.

4.2. Phase 2: use of the financial system (continuing a business relationship).

4.2.1. Legal obligation: monitoring the business relationship - how is it applied?

The use or making use of the financial system can be in either the physical or the online world. In both environments, the financial system may be used in a closed loop (internal transfers initiated by the client from and to his on bank accounts), or to make payments and transfers, which implies that third parties (“payees”) are involved. In accordance with the anti-money laundering regulations, financial institutions have an obligation to **monitor the business relationship with their clients**. While this monitoring obligation

³⁹ www.cifas.org.uk

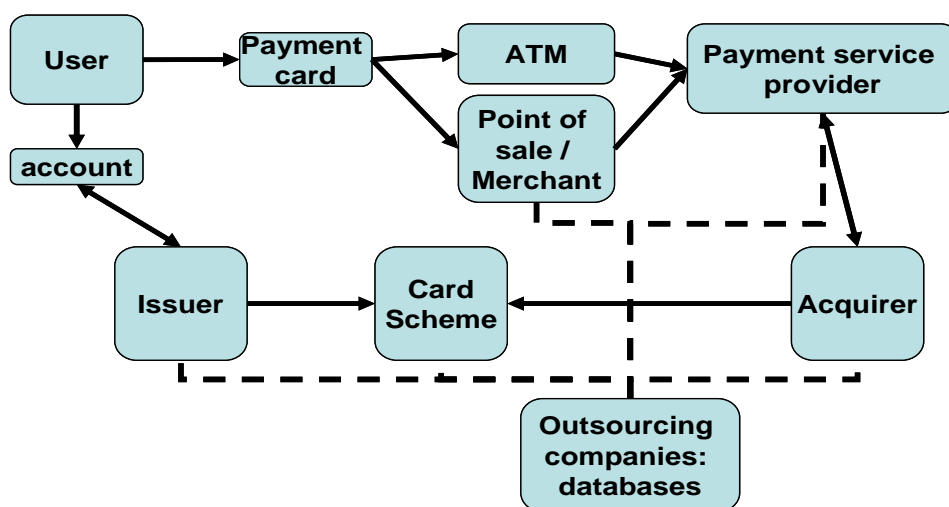
⁴⁰ www.asnef.com; www.sepfra.es

essentially relates to the prevention of money laundering, it has indirect effects as regards the prevention of identity theft/fraud. Indeed, such monitoring should normally imply in practice that the financial institutions should be sure that the "contractual identity" of clients is respected.

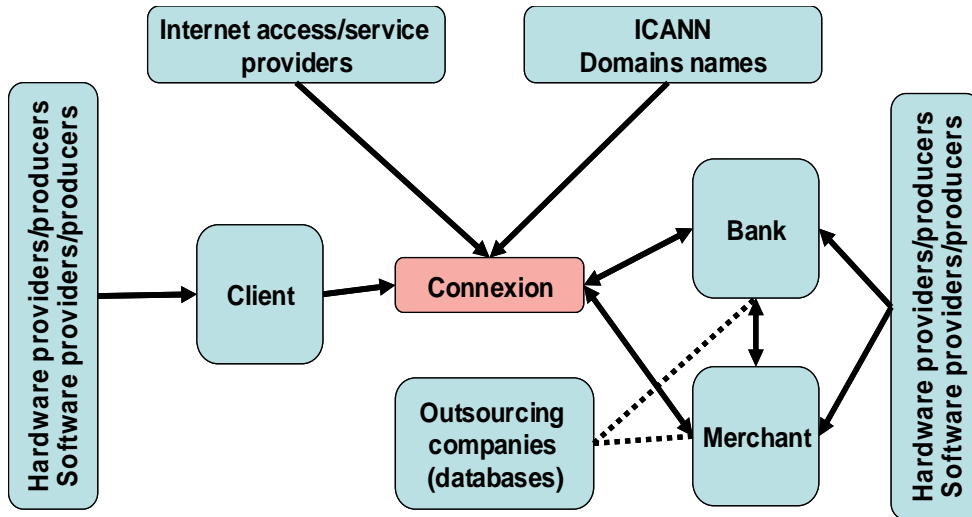
In this respect, stakeholders anticipate that importance of the monitoring tasks will grow as a result of the possibility offered by the latest EU legislation on money laundering prevention to rely on a third party to conduct customer due diligence procedures. They see a movement away from a traditional "identity checks" scenario to a "monitoring of customer's transactions and profile" scenario for the purposes of knowing the customer⁴¹.

It should also be noted that the responsibility in monitoring "contractual identity" goes **beyond the financial services providers**. In both the physical and the online world, the client makes use of technical equipments that are managed by multiple stakeholders: terminal manufacturers, communication and internet providers, domain names providers, anti-virus software, banks, merchants, etc. Each of these stakeholders has the responsibility to secure the services it provides to its clients who, in turn, need to be accountable for securing their own environment. The following two charts provide a simplified view of the **processes involved in the physical and online world** (Even if the both worlds are more and more closely linked to each other without any physical border and processes combine both in most cases).

Physical world



⁴¹ See the European Commission Staff Working Document, *The application of Directive 91/308/EEC on the prevention of the use of the financial system for the purpose of money laundering in relation to the identification of clients in non-face to face transactions and possible implications for electronic commerce*, SEC(2006) 1792, December 2006, paragraphs 25 and seq, in particular paragraph 29.



4.2.2. Risks & vulnerabilities (phase 2)

The main risk in this phase is **account takeover**, that is to say, the impersonation of, or attempt to, assume the identity of an existing account holder (which has been previously properly identified). This requires two steps: firstly gathering personal information on financial institutions clients, secondly, using them to get further financial services.

**Main risk:
account takeover**

The first step is to obtain the relevant data. There are different *modus operandi* to obtain personal data⁴².

- In the **physical world**, criminals still use classic systems to get access to relevant data:

Dumpster Diving or bin raiding	Obtaining personal information through trash cans searching for pieces of unshredded personal information that they can use or sell.
Mail Theft	Seeking out and stealing from unattended/unlocked mailboxes to obtain pre-approved credit offers, bank statements, tax forms, and/or (convenience) checks.
Inside Sources	A dishonest employee with access to personnel records, payroll information, insurance files, account numbers and/or sales records can wreak havoc.
Imposters	Victims who have been taken in by an individual who fraudulently posed as someone who had a legitimate or legal reason to access the victim's personal information (e.g., landlord asking for background information, an employer, marketer, etc.). It can also be done by using spoof letters or telephone calls.
Theft	Gaining legitimate access into someone's home and personal information through household work, babysitting, healthcare, friends or roommates, etc.
Purse/Wallet Theft	Stolen purses and wallets usually contain bankcards and personal

⁴² Describing the modus operandi may take different forms. Annex 2 provides a different approximation to the problem.

	identification
Shoulder surfing	Capturing personal data by looking over the shoulder of unsuspecting individuals or using more sophisticated observation methods (e.g. cameras etc.)

- In the **on-line world**, regarding systems and software processes, the access and authentication process to online financial system is complex and involves several elements and various stakeholders. Each stakeholder in the online world is, in itself, a point of weakness, starting from the user to the e-merchant:

Users	The weakest point in the chain. Social engineering techniques (Social engineering is the technique of circumventing technological security measures by manipulating people to disclose crucial authentication information) like <u>phishing</u> take advantage of people ignorance about security. In addition, not securing home Internet connection could amount to negligence.
Access Points (Hardware and software providers)	A lot of « ID theft » actions occur at the Access Point level (Workstation, PDA, Cell Phone, cyber-coffee, etc) by taking advantage of the known weakness of currently used technologies (<u>viruses</u> , <u>Trojans</u> , <u>worms</u> , etc .).
Internet Service providers	Internet Service Providers also play a rule in the « ID theft » actions, through a lack of security by default provided to their customers.
Internet Third Parties	Internet Third Parties also play a role in the « ID theft » actions, like their lack of control in the domain name registration process that enables fraudsters to use typo squatting methods.
E-Enterprises	The ultimate repository of the users' credentials is e-Enterprises (Cyber Merchants, Banks, Search Engines, Mail Providers, etc ..). A fraudster can hack into the system, if it is not secure enough.

Phishing (as well as the related pharming problem) is perceived as an important problem by the public opinion, thus receiving significant attention (see box n° 5 below).

Box n° 5 - The specific case of phishing in e-banking and e-payments.

Phishing is based on common methods of social engineering: victims are approached in a manner that superficially seems trustworthy, and are simply asked to hand over sensitive data. As such, phishing has a longstanding offline tradition. The easiest way to gain access to confidential information is not to steal it, but to simply ask for it. With a small amount of social manipulation (e.g. presenting one's self as part of the IT maintenance department) a surprisingly large number of victims appears to throw all caution in the wind. The reason why phishing has recently garnered so much attention is because of a new trend: combining phishing with mass e-mail sending (similar to spamming activities), and relying on the pure size of the victim base to ensure a good return on this scam.⁴³

Staff involvement in the comprise of personal data about customers has become recognised as a major security threat, notably because of its reputational, financial, regulatory, internal and customer service impact. Staff fraud also enables third parties to take over accounts easily without being challenged: staff corruption is favoured by criminal groups as it is easier, cheaper and quicker than a sophisticated infiltration. For instance, in the UK there have been several recent high profile cases of major banks being fined by the regulatory authorities for fraud committed by their staff. Still, staff fraud is largely underestimated, under-detected and under-reported.

⁴³ Leenes (ed.), FIDIS network, deliverable 5.2b, *ID-related crime: towards a common ground for interdisciplinary research*, May 2006, p. 19.

It appears, however, that the main risk at this stage is connected to **mass data compromise and in particular hacking of electronic data warehouses**, whether public or private. Outsourcing data processing activities in the banking environment to third party service providers, who might even be located in countries where no privacy legislation exists, increases the hacking of databases risk⁴⁴. Organised crime appears to be moving from the compromise of individual accounts or access devices to mass compromise of data storage facilities, thus enabling cross-border abuses on a large scale. Risk exposure is therefore growing.

A combination of the physical and online world results in **personal information being available for acquisition through the Internet**. Public records and even credit card numbers are available to anyone who knows how to search for them. There are Websites where personal details that are usually required on an application are available at little or no cost.

The second stage is the use by criminals of the personal data of existing clients.

Contrary to the situation described in phase 1, in phase 2 criminals are impersonating already registered clients, which adds to the difficulty of detection for the financial institutions. Classic account take-over will normally result in using the identity of an existing client to make new credit applications or ask for new payment cards. This usually requires the use of a different address for the same client.

For some stakeholders, the misuse of personal data goes beyond account takeover. It also includes situations in which the payment instruments (such as payment cards) or banking facilities (especially e-banking or phone banking) of the clients are directly misused without a new application to the financial institution. From this perspective, fraud in relation to lost & stolen cards, counterfeit cards, card-not-present situations, phishing and pharming should also be considered to be identity theft/fraud cases. For the financial institution it is very difficult to detect those cases, unless the true client makes a notification.

4.2.3. Responses – weak points? (phase 2)

There are different responses to those vulnerabilities⁴⁵.

Current solutions for authenticating customers (i.e. once access to the financial service has been set up) are largely based on relatively simple "what you have" (documents) and "what you know" (e.g. passwords) methods (as opposed to biometrics: e.g. "what you are" method). Currently most solutions rely on single static complicated passwords (e.g. PIN in cards or e-banking password). Those static passwords have limitations (restrictions on the number of digits that can be memorized) and their static nature make them more easily subject to compromising (e.g. PIN capture in ATM environments using

⁴⁴ Outsourcing activities of this kind to third countries is broader than just the banking sector. Risks are also present in those cases.

⁴⁵ See also the recent survey by the UK Financial Services Authority on "Authentication and Safeguarding of Customer Identity". Financial Crime Newsletter, issue n°8, August 2007. Available at www.fsa.gov.uk/pubs/newsletters/fc_newsletter8.pdf.

cameras, shoulder surfing; tapping in publicly accessible terminals etc). Therefore, they **are relatively insecure**⁴⁶.

Therefore, there are a number of **other preferred measures** that could be used to confirm the "contractual identity" of the client. Still very much based on a "what you know" method, they contain other features which make them more reliable: e.g. a more secure authentication. These measures are, *inter alia*: 2 (or more) factor authentication; new generated – not static – passwords for each transaction, also called one-time passwords; VPN connection between bank and customer; site data protection programs, 3D secure card transactions or in home banking (validation by SMS, one time password using a token device; smart authentication card) etc.

Biometrics are deemed more secure as they are more closely linked to the person (the iris never leaves the human body, for instance)⁴⁷. However, the use of biometrics is not necessarily the best solution for the verification of the "contractual identity". Whilst biometrics can appear to be a step towards enhance security, there are concerns about the consequences in case of compromising⁴⁸ (e.g. reversibility problem), the ability of the customer to challenge a 'false-positive' and the resistance on privacy and civil liberties grounds.

Concerning phishing (and similar scams such as pharming), customer education is important so as to enable him to recognise false messages. Customers should indeed be more responsible for their actions in the internet world. In this context, two-way authentication could improve security⁴⁹. Technology can also help⁵⁰. Moreover, the involvement of internet service providers is key to provide rapid responses (e.g. closing down of fake sites) to his kind of scams, once detected. This was acknowledged at the Commission High Level Conference of November 2006, which considered that a dialogue with Internet Service Providers on prevention issues could be beneficial.

An appropriate protection of databases requires in particular the increase in the security of databases kept by the banking community, whether operated directly by the

⁴⁶ See also Leenes (ed.), FIDIS network, deliverable 5.2b, *ID-related crime: towards a common ground for interdisciplinary research*, May 2006, p. 98 on authentication.

⁴⁷ See also footnote n°17.

⁴⁸ On possible scenarios for identity fraud with biometrics, see Leenes (ed.), FIDIS network, deliverable 5.2b, *ID-related crime: towards a common ground for interdisciplinary research*, May 2006, p. 85. See also page 102 and seq.

⁴⁹ Usually organisations authenticate clients in a one-way process, while the client cannot authenticate the organisation sufficiently. In addition to the one-way authentication, the client could authenticate the organisation e.g. by using certified signatures for the exchange of messages. Two-way authentication can make certain attacks like phishing or man-in-the-middle attacks more difficult. See also Leenes (ed.), FIDIS network, deliverable 5.2b, *ID-related crime: towards a common ground for interdisciplinary research*, May 2006, p. 99 and seq.

⁵⁰ The European Commission is funding a research project under the Research Framework Programme 6 aiming at developing spam and phishing filters with unprecedented accuracy for use both on traditional e-mails and mobile messaging services. This research action, "AntiPhish: Anticipatory Learning for Reliable Phishing Prevention", started in January 2006 and will run until December 2008. Partners to this project are Symantec, Fraunhofer-Gesellschaft, Nortel, Katholieke Universiteit Leuven and Tiscali. For further details see: www.antiphishresearch.org

financial institution or by a third party (call centres, document handing service providers, transaction processing entities...). It also requires the increase security of merchant websites (e.g. they should be able to effectively protect the personal data they receive from their customers when transactions take place), of the administration and of security in general.

Concerning **consumers**, it is in their own-interest not to be negligent when using the financial system, particularly in the on-line environment. However, it is important to keep in mind that their computers are not high-security devices. Consumers can only assume responsibility for risks that they can actually influence in terms of risk-avoidance and risk-minimization. For instance, they have no real influence in preventing high tech approaches or attacks concerning systems periphery. From their perspective, this requires solutions that are safe, but also convenient to be a success. Consumers need to be able to understand, remember and practice them. It would be wrong to exclusively rely on one-tier high-tech security systems as prevention systems. Dialogue between the consumer and the financial sector on security issues is equally important as the consumer can only heed the advice he gets. The consumer needs a trustworthy feeling that everything possible will be done to prevent harms. Consumers associations consider that a way to proceed would be to define best practices and to provide for independent checks of systems.

As regards **staff fraud**, institutions should consider following best practice policies and procedures specifically aiming at diminishing this risk: e.g. vetting and security screening, monitoring staff employed, internal controls etc.

Unfortunately, no matter how tight security measures are made, there is always the possibility that hackers will obtain the genuine party's security details and commit a fraud even when the identity of the individual has been verified.

4.3. Phase 3: end of the contract (ending a business relationship).

4.3.1. Legal obligation: Monitoring the business relation - how is it applied?

The end of a relationship between a financial institution and a client is normally possible because:

- The client ends his/her relationship with a financial institution;
- The financial institution ends the relationship with the client;
- The client died.

4.3.2. Risks & vulnerabilities (phase 3)

The main risk, in the end of contract situation, is the takeover of the existing account, if the termination is not appropriately handled by the parties involved. In this context, fees to closing the business relationship could act as a barrier to formal closure and notification, thus increasing the risks.

This could first relate to the interception of the termination related mail between client and financial institution, leading to a situation in which a third person can impersonate the client. It could also relate to the appropriation of dormant accounts, in particular if

there is poor monitoring of those accounts by financial institutions. The situation, in this case, is not far from the take-over of accounts described in the phase 2 above.

The decease of the client, however, leads to specific risks. In particular, the financial institution may not be able to learn about the death of the client. Fraudsters may take advantage of this situation to impersonate the death person.

Box n° 6 - Theft of the Identity of the Deceased – Modus operandi in the UK⁵¹

E.g. 1: an obituary/In Memoriam notice is placed in a newspaper giving the full name and date of birth as well as date of death of the genuine party. Fraudsters then locate the residential address of the genuine party through electoral roll data, telephone directories etc. Applications are made in the genuine party's name and date of birth from a new address giving the deceased address as the previous address.

E.g. 2: fraudsters visit cemeteries and crematoriums looking for the details of any funeral services being held. They make a note of the details and then as in Example 1 commit the fraud using the genuine party's details.

E.g. 3: details of children who died before their 18th birthday are obtained either from cemeteries or from viewing records of births, marriages and deaths. The fraudster then adopts the identity of a child who has died but who would now be over 18 and eligible to apply for credit. False documents are manufactured to support the applications.

A specific problem is also raised in connection with some e-payment providers whose payment accounts appear to be "impossible" to close. This barrier to closing increases the risks of misusing the personal details of the original payment account owner.

4.3.3. Responses – weak points? (phase 3)

The risks related to the death of the clients are specifically handled in some countries:

Box n° 7 – Handling the death of clients.

In **France**, banks share data on **deaths of clients** related to account closings. All accounts will be closed upon such cross industry notifications.

In **Belgium**, the **end of the business relationship** between a bank and its customer is organised as follows:

- The customer has to notify his bank of any change of address, which reduces considerably the number of “dormant accounts” and the bank has the possibility to block the customer’s cards when he left without address change.
- A national “social crossroad database” has been created, which guarantees that all allowances (pension, allowances for unemployed people etc.) paid to a person are stopped when his death has been certified. Any death has to be certified by a doctor and he has to inform the municipality, which has input in this database. Banks are informed and they must inform the tax authorities. This national database allows cross-checking of death certificates with allowances being paid and thus reducing this risk to a minimum.

⁵¹ Examples provided by CIFAS to the FPEG working group.

5. PREVENTATIVE MEASURES: ASSISTANCE BY PUBLIC AUTHORITIES.

5.1. What is being done?

Public authorities are also responsible for preventing identity theft/fraud. There are several best practices applied by some authorities.

- First of all, some public authorities (either alone or in cooperation with the financial services industry) are launching awareness and educational measures, including maintaining of devoted websites⁵². Those awareness/educational measures may be for the general public or for specific 'weaker' categories (e.g. children etc). Stakeholders consider that public authorities should be accountable for public awareness on possible threats of misuse of citizen's identity.

Box n° 8 – Awareness and educational measures

UK – Website "Identity theft-Don't become a victim"

The Home Office, in collaboration with other government departments and private sector organisations, has set up the Home Office Identity Fraud Steering Committee to lead a cross public/private sector work programme to tackle identity theft and identity fraud. The programme coordinates existing activity in the public and private sectors and identifies new projects and initiatives to reduce identity crime.

Among those initiatives, an awareness campaign was launched in September 2005 and a website was created (www.identity-theft.org.uk). The website contains information on how to protect one's identity and prevent criminals from committing fraud in one's name; on what to do in case of becoming a victim; on who can help; and on what is being done. The leaflet and poster from the awareness campaign are also available in the website.

France – Website for children and teenagers

The French public authorities, together with some private partners, launched in 2006 a website (<http://www.protegetonordi.com/>) specifically addressed to children and teenagers which contains information on how to make a safer use of the internet environment⁵³. It includes tips concerning e-banking and e-commerce, the prevention of phishing etc.

- Secondly, there are databases kept by public authorities on identity documents, identity related information or on payment instruments. These databases may be accessible beyond the public authorities themselves to the financial services industry, or generally to the public.

Box n° 9 – Public databases

The Netherlands – VIS (Verification of Identity Systems) database

⁵² The US authorities (in particular the FTC) have also produced numerous materials on how to prevent identity theft/fraud and what to do in case of becoming a victim. See the web links in the annex.

⁵³ The European Community has also established a programme on promoting safer use of the Internet and new online technology (see Decision No 854/2005/EC of the European Parliament and of the Council of 11 May 2005; OJ L 149, 11.6.2005). This programme, however, focuses on the fight against illegal, unwanted and harmful content.

VIS is a database that keeps details of lost and stolen documents. Details of around six million documents are held on the central database. Whilst the majority of documents recorded are Dutch, details of documents issued in other countries, but lost or stolen in the Netherlands are also held. Records of deaths are also held in case someone tries to assume the identity of a deceased person. The database can also be used to validate some of the data recorded on a document. Public and private sector organisations can use the database: there are around 2.500 terminals used to access the database nation-wide. Consumers normally give consent to their details being included in the database.

Belgium – database on stolen ID cards

The ID card numbers that have been stolen in blank can be checked via Internet.

Germany – database on lost and stolen payment cards

The German police has introduced a database (KUNO) that keeps records of lost and stolen payment cards. Merchants can check with KUNO before accepting a payment whether the card has been stolen or lost.

Interpol - Database on lost and stolen documents

Interpol maintains Stolen and Lost Travel Documents Database (SLTD) which contains details of more than 11 millions of such documents. For the moment, this database is only accessible to law enforcement authorities.

Interpol – Database on counterfeit payment cards

Interpol also keeps a database on counterfeit payment cards (CPCD), which is accessible to both public and private sectors.

Sweden – Database on personal taxation data

In Sweden, the administration provides the general public (in some cases only to financial institutions) with access to several databases. For example, the Swedish National Tax Board gives access to personal data of citizens related to taxation issues. This includes: name, personal number, address (including birth place and previous address history) and taxed assets. Service providers (such as Info Torg) provide a combined solution giving access to all databases at once.

- Thirdly, single contact points allowing citizens to declare identity fraud/theft related problems have been set up in some countries, including third countries.

Box n° 10 – Single contact point.

Canada – Reporting Economic Crime Online (RECOL): www.recol.ca

RECOL is an initiative that involves an integrated partnership between International, Federal and Provincial Law Enforcement agencies, as well as with other State agencies and private commercial organizations. Since October 2003, citizens who become victims of economic crime (in particular credit card fraud and identity theft) in Canada or the U.S.A. can file a complaint on-line. When filing the complaint, the victim can immediately send it to some or all the agencies and bodies that might need to know about it. This innovative means of reporting e.g. credit card fraud, accelerates the access of police services to relevant information and facilitates the sharing of information with other agencies and the private sector (e.g. credit card companies, banks, credit reference agencies), subject to the prior consent by the complainant.

5.2. What else can be done?

Generalisation of the best practices described would be welcomed by stakeholders.

- It appears that more public awareness and education on Internet issues in connection with financial services are needed⁵⁴. Current efforts to make sure that the chain of responsibility is made of high levels of security should be enhanced. The whole e-society should be secured, not only the banking industry. For example, the customer PC is an essential part of this chain and it adds, in itself, a new element of complexity. The same goes with SMEs who are not necessarily equipped to protect their data bases in an adequate way.
- Facilitation of access to databases is also considered to be appropriate⁵⁵.
- Setting up a central point of notification in each country would also be helpful, but also efforts should be done to make sure that the information notified is verifiable and usable.

Better communication and cooperation between public authorities is needed. Exchange of information between all parties is also needed, as banking activity (and the related fraud) is becoming increasingly online and cross border in nature. In this context, it was highlighted by the participants to the High Level Conference of November 2006 that there is a need to intensify cooperation and exchange of information between the public and the private sector⁵⁶. It is important to better communicate and to better know who does what. There are some recent experiences in other countries in relation to phishing.

Box n° 11 - Public-private partnerships – Phishing

An important public-private initiative (Anti-Phishing Working Group) to fight against phishing was launched in the US, though it is open to participants from other regions of the world (www.antiphishing.org).

A major software provider has also launched an anti-phishing initiative (so-called Digital Phishnet) in partnership with law enforcement authorities in the US and in some EU countries. The goal is to react quickly in order to stop illegal sites and to bring fraudsters before the courts.

Participants to the high level conference agreed that more statistical data are necessary in order to quantify the extent and the impact of identity theft. The Commission has recently created a Group of Experts which looks at policy needs on crime and crime statistics that most likely will take up this challenge.

⁵⁴ The Commission organised in March 2007 a conference on consumer financial capability. Its aim was to encourage the provision of high-quality financial education to consumers, and provide a forum for the exchange of best practices. For further information, including presentations and minutes, see: http://ec.europa.eu/internal_market/finservices-retail/capability/index_en.htm

⁵⁵ See also the conclusions of the UK 2002 study: "A central register of stolen documents (passports, driving licences, National Insurance number cards etc) would reduce the value of such goods in the market." [...]. "Additional levels of security can be achieved through checking applications against a register of known frauds and fraudsters, such as is run in the private sector by CIFAS, and through the use of IT systems which can check applications for consistency against data already held by government." UK Cabinet Office, *Identity Fraud: a Study*, July 2002, p. 5.

⁵⁶ See also the conclusions of the UK 2002 study: "Detection and prosecution of identity fraud falls to many government departments and private sector bodies. Stronger co-ordination of counter fraud activity is needed." UK Cabinet Office, *Identity Fraud: a Study*, July 2002, p. 5.

6. THE PROSECUTION SIDE:

6.1. The need for effective penalties

Identity theft/fraud in the payment area is normally not a criminal offence on its own, but an enabler for other offences⁵⁷. As a result, there is a vast disparity of penalties applied in Europe⁵⁸. Stakeholders have the perception that those penalties are generally too low to be dissuasive. Additionally, many of them also believe that creating a specific offence for identity theft would facilitate prosecution. As the UK 2002 Study indicated:

"Prosecution of offenders should be pursued more vigorously. One way to ensure this might be through the creation of a new offence of identity theft, which might make successful prosecution both more worthwhile and easier."⁵⁹

A certain harmonisation of EU criminal legislation in this regard seems to be supported by stakeholders. The European Commission is indeed studying this issue. The Commission (DG Justice, Freedom and Security) has launched a comparative study in July 2007 on the definitions of identity theft used in EU countries and their criminal consequences. It will include recommendations on best practices. Depending on the results, legislative development would not be completely ruled out.

6.2. Police and judicial responses

In addition to increasing the deterring effect of penalties, there are other measures that could help in increasing the fight against the identity theft/fraud phenomenon. Those measures are not different from those applied against other economic and financial crime.

They essentially relate to improving the capacity of police forces through the creation of dedicated specialised units with operational responsibilities (where they do not exist).

⁵⁷ For a description of identity related crimes, see Leenes (ed.), FIDIS network, deliverable 5.2b, *ID-related crime: towards a common ground for interdisciplinary research*, May 2006, in particular section 3.

See also the Results of the second meeting of the Intergovernmental Expert Group to Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity, UN Commission on Crime Prevention and Criminal Justice, Sixteenth session, Vienna, 23-27 April 2007, doc. E/CN.15/2007/8.

Cybercrime is closely related to identity theft/fraud criminal activities. On the issue of cybercrime, see the Council of Europe Convention of 23 November 2001. See also the EU Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, OJ L69 of 16 March 2005, p. 67. See also the Communication from the Commission of 22 May 2007 to the European Parliament, the Council and the Committee of the Regions - Towards a general policy on the fight against cyber crime, COM(2007)267.

⁵⁸ See Owen, Keats and Gill, *The Fight Against Identity Fraud: a Brief Study of the EU, the UK, France, Germany and the Netherlands*, Perpetuity Research & Consultancy International, June 2006. See also Deliverable 5.1 of the FIDIS research project (*A survey on legislation on ID theft in the EU and a number of other countries*), May 2005.

⁵⁹ UK Cabinet Office, *Identity Fraud: a Study*, July 2002, p. 5.

These dedicated units, if created in all EU Member States, would provide a significant added value in the fight against identity theft/fraud.

They also relate to enhancing cross border police and judicial cooperation, by for example creating centralised contact points or improving training of magistrates and prosecutors in financial issues (financial investigations, etc.)

It is essential to be able to conduct rapid end-to-end investigations (thus covering the whole chain) in an international context. This is the only means to stop the criminal money flows. In this context, it has been raised in the group that the private sector could facilitate these investigations by eliminating certain costs for the police (e.g. in some countries, the police should pay the Internet Service Providers to have an IP address identified).

There is also a need for enhanced cross-border prosecution of certain forms of cybercrime.

7. CONCLUSIONS

From the discussions in the meeting of the FPEG and its subgroups, it emerges that:

- (1) It is important to maintain the integrity of the identity chain. Currently the weakest links of the chain are: the customer's PC (he should be aware of it and be motivated to secure his own environment); the Internet Service Providers; the data storage service providers acting as third parties, as well as the databases operated by merchants and public authorities.

In this chain, the responsibility⁶⁰ should be taken up by all the parties to the chain, within their own limitations. Consideration could be given to a voluntary code for stakeholders that they could sign up. This way, all members of the chain would know that they were involving themselves in a responsible 'chain'.

- (2) Identity theft/fraud does not only affect the financial sector. Its effects go beyond. Other stakeholders should be associated to this fight.
- (3) It is of great importance make available educational tools for weak parties (citizens and SMEs) in relation to the use of the Internet.
- (4) Technology is part of the solution but will not be the only solution.
- (5) Caring for victims make sense as it should provide for improved trust.

*

* *

⁶⁰ In this context, some stakeholders are of the view that we cannot put the responsibility with the consumer, but we should raise his awareness. Banks and payment schemes should make sure that the products they are selling are secure.

ANNEX 1 - APPLICATION FRAUD TYPOLOGIES (CIFAS)⁶¹

Previous address fraud:

- E.g. 1: application received from Mr Brown giving a current address for 5 months and a previous address where he claims to have lived for 3+ years. Mr Brown is unconfirmed at current address (not unusual as he has recently moved there) but is confirmed through electoral roll data and account information registered at the address. However a Mr Brown still lives at the previous address given on the application and the applicant has created an identity in the name of Mr Brown to get an account approved using the genuine Mr Brown's credit history.
- E.g. 2: an elderly person moves into residential/nursing care. The fraudster makes an application in the elderly persons name giving a current address with a short time of residency and gives the elderly persons address as their previous address. Usually somebody of this age will be on the electoral roll register and will either have a good credit record or no credit record as they have always dealt in cash. The genuine party will be unaware of the fraud but he/she or their family may be contacted at a later date having being traced to the home by debt collectors. (This type of fraud can also occur with the address being the only address supplied on the application with a long residential period provided by the fraudster).

Current address fraud:

- E.g.1: Father and son, mother and daughter, brother and brother, sister and sister, indeed any family relations all residing at the same address. In this example the son Mr James Black is unable to obtain credit in his own name due to adverse information recorded against him with the credit reference agencies. However he still requires finance and makes an application using his fathers name Mr John Black. The son knows all the fathers personal details and passes all underwriting checks.
- E.g. 2: block of flats, converted house or any property where there is a shared letterbox. One resident intercepts post for another tenant. This could be a bank/credit card statement, utility bill, tax notification or any other document that could be used as a form of identity. It could even be a piece of junk mail pre-completed in the innocent residents name. The fraudulent resident then applies for credit using the innocent residents details intercepting any post that arrives.
- E.g. 3: financial difficulties within a relationship result in one of the parties (for example the husband Mr Green) making an application for a product in joint names without his wife Mrs Green having any knowledge of the application. This fraud is difficult to detect, as the fraudster will know all the genuine details of the other party. Post can be intercepted resulting in the innocent party being unaware of the fraud.

'Same Name' fraud

- Mr Andrew White is unable to obtain credit in this own name due to adverse credit information. Through looking at electoral roll data or telephone directories he is able to locate another Mr A White. He then makes an application for a loan with direct payment into his bank account using the address details of the genuine Mr White.

⁶¹ Typologies provided by CIFAS to the FPEG working group.

ANNEX 2 – OCCURRENCES OF IDENTITY THEFT/FRAUD [FIDIS]

One of the FIDIS network deliverables provides the following categories of occurrences of identity theft/fraud⁶²

1. Identity Theft

- **Direct attack on the link between the person and the authentication data** using one or more steps
 - **Worms** installing for example a **key logger**. Authentication data is directly taken from a person by manipulation of his input device (in most cases local computer). This attack is directed non selectively to many input devices (1 : n attack); the person is not addressed directly.
 - **Social engineering**. Using communication for example via telephone authentication data is directly taken from the user by giving him a seemingly plausible reason for disclosing the requested data e.g. for testing purposes by administrative personal of the enterprise's IT department. This type of attack is directed to a specific person.
 - **Trojan Horses / Key logging** etc. sent via e-mail attachment. In the first step a spam mail containing malicious code in an attachment is not specifically sent to various users (1 : n attack). By opening the attachment for example a key logger is installed that starts obtaining the authentication data in a second step.
 - **Spoofing of (biometric) sensors** without co-operation of the person to which they were originally linked. In the first step the needed biometric data such as a photo of the eyes is take from the person. In a second step, a printout of the photo is used to spoof for example an iris scanner. This type of attack is directed to a specific person.
- **Indirect attack on reference data** or via other links
 - **Readout of Person related identifiers, authorisations and reference data**. In this case the attack is directed to the centrally stored reference data and related additional identifiers. This attack can either be carried out against the whole database (1 : n) or specific data records (1: 1).
 - **Manipulation of reference data concerning a person**. By manipulation of the reference data, the attacker is able to redirect link to the authentication data to himself while the IT systems expects an authentication by the person the not manipulated reference data originally was linked.
 - **Phishing** (3 Steps, indirect attack, 1:n) In the first step the attacker sends a spam mail that seems to originate from a trusted brand name (e.g. a bank)

⁶² Leenes (ed.), FIDIS network, deliverable 5.2b, *ID-related crime: towards a common ground for interdisciplinary research*, May 2006, p. 83.

to many recipients (1 : n attack). This email usually urges the recipients to click on an embedded link that leads them to a manipulated web site. This web site again has the layout of the trusted brand, so that the link between IT system and authentication data (link 3) is being attacked. On this site the user is duped to enter authentication data.

2. “Man in the middle” attacks; they allow for both forms of attacks. In this type of attacks the communication between user and system is intercepted. This type of attacks is potentially very powerful and allows, among others (such as substitution attacks), for different types of identity theft:

- **Identity theft by readout of authentication data** not securely communicated by the user (direct attack on link 1, 1 : 1 attack).
- **Replay Attacks.** An IP-packet containing authentication data is manipulated concerning the sender address and resent to the receiving system. This type of attack is directed to a user of a specific input device (direct attack on link 1, 1 : 1 attack).
- **Identity theft by redirecting the communication to a manipulated web site** e.g. by using DNS-spoofing, manipulated proxies or manipulation of routing tables. On the manipulated web site the user is duped to enter authentication data. This type of attack is concerning some steps similar to phishing (2 steps, indirect attack on link 3, 1 : n attack).

3. Deceitful Identity delegation and deceitful identity exchange. In this case the person co-operates with the attacker giving his authentication data deliberately to him with the knowledge that this data will be abused. The attack is directed towards link 1 and is directed 1 : 1 (deceitful identity delegation) or more complex in cases of deceitful identity exchange.

4. Identity Creation. In cases of identity creation, the attacker typically uses the enrolment phase to manipulate either link 1 or link 2 (see Figure 8) so that the chain from him as the physical person to the authorisation breaks. Thus he probably can abuse the IT system for a certain (and probably long) time.

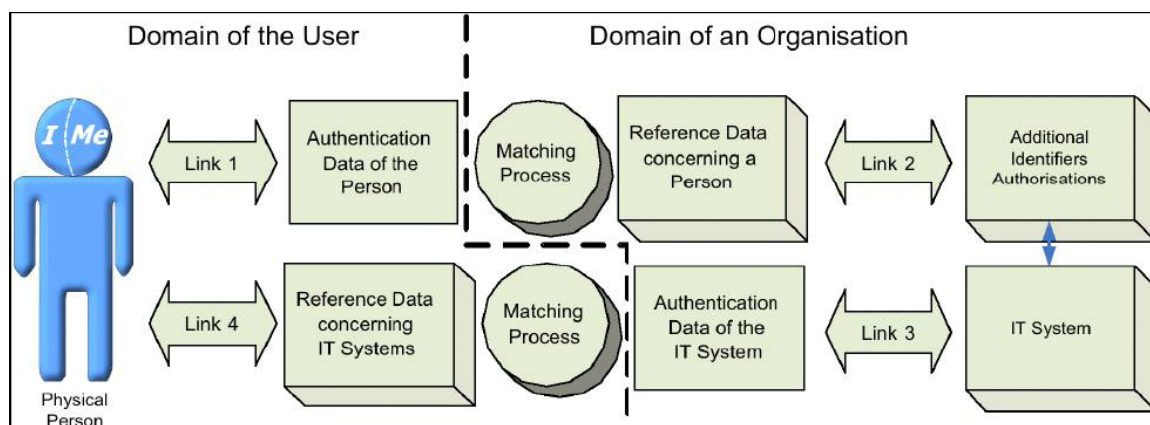


Figure 8. Authentication procedures between persons and IT Systems.

ANNEX 3 – DEFINITIONS OF MODUS OPERANDI IN THE ONLINE WORLD

Phishing (In computing) is the act of attempting to fraudulently acquire through deception sensitive personal information such as passwords and credit card details by masquerading in an official-looking email, IM, etc. as someone trustworthy with a real need for such information. It is a form of social engineering attack.

Pharming is the exploitation of a vulnerability in the DNS server software that allows a hacker to acquire the Domain Name for a site, and to redirect traffic to that web site to another web site. DNS servers are the machines responsible for resolving internet names into their real addresses- the "signposts" of the internet.

Phreaking is a slang term coined to describe the activity of a subculture of people who study, experiment with, or exploit telephones, the telephone company, and systems connected to or composing the Public Switched Telephone Network (PSTN) for the purposes of hobby or utility.

In the field of computer security, **social engineering** is the practice of obtaining confidential information by manipulation of legitimate users. A social engineer will commonly use the telephone or Internet to trick people into revealing sensitive information or getting them to do something that is against typical policies. By this method, social engineers exploit the natural tendency of a person to trust his or her word, rather than exploiting computer security holes. It is generally agreed upon that “users are the weak link” in security and this principle is what makes social engineering possible.

Botnet is a jargon term for a collection of software robots, or bots, which run autonomously. A botnet's originator can control the group remotely, usually through a means such as IRC, and usually for nefarious purposes. A botnet can comprise a collection of cracked machines running programs under a common command and control infrastructure. Individual programs manifest as IRC "bots". Botnets have become a significant part of the Internet, albeit increasingly hidden. Due to most conventional IRC networks taking measures and blocking access to previously-hosted botnets, owners must now find their own servers. Oftentimes, a botnet will include a variety of connections, ranging from dial-up, DSL, cable, educational, and corporate. Sometimes, an owner will hide an IRC server installation on an educational or corporate site, where high-speed connections can support a large number of other bots. Exploitation of this method of using a bot to host other bots has proliferated only recently, as most script kiddies do not have the knowledge to take advantage of it.

In cryptanalysis, a **brute force attack** is a method of defeating a cryptographic scheme by trying a large number of possibilities; for example, exhaustively working through all possible keys in order to decrypt a message. In most schemes, the theoretical possibility of a brute force attack is recognised, but it is set up in such a way that it would be computationally infeasible to carry out. Accordingly, one definition of "breaking" a cryptographic scheme is to find a method faster than a brute force attack.

In computer programming, a **buffer overflow** is an anomalous condition where a program somehow writes data beyond the allocated end of a buffer in memory. Buffer overflows usually arise as a consequence of a bug and the use of languages such as C or C++ that are not "memory-safe". One consequence of the overflow is that valid data can be overwritten as a result. Buffer overflows are also a commonly exploited computer security risk—since program control data often sits in the memory areas adjacent to data

buffers, by means of a buffer overflow condition the computer can be made to execute arbitrary (and potentially malicious) code that is fed to the buggy program as data.

Cryptanalysis is the study of methods for obtaining the meaning of encrypted information without access to the secret information which is normally required to do so. Typically, this involves finding the secret key.

Web site "**defacement**" is usually the substitution of the original home page by a hacker. The best-known defacement archive is www.zone-h.org which monitors web defacements but also web intrusion at any level (not only the homepage). Defacement is generally meant as a kind of electronic graffiti while recently it has become a means to spread messages from politically motivated "cyber protesters".

A **denial-of-service attack** (also, **DoS attack**) is an attack on a computer system or network that causes a loss of service to users, typically the loss of network connectivity and services by consuming the bandwidth of the victim network or overloading the computational resources of the victim system.

A **dictionary attack** refers to the general technique of trying to guess some secret by running through a list of likely possibilities, often a list of words from a dictionary. It contrasts to a brute force attack in which all possibilities are tried. The attack works because users often choose easy-to-guess passwords, even after being exhorted against doing so.

In a **distributed DOS attack**, the attacking computer hosts are often personal computers with broadband connections to the Internet that have been compromised by viruses or Trojan horse programs that allow the perpetrator to remotely control the machine and direct the attack, often through a botnet. With enough such slave hosts, the services of even the largest and most well-connected websites can be denied.

An **exploit** is a common term in the computer security community to refer to a piece of software that takes advantage of a bug, glitch or vulnerability, leading to privilege escalation or denial of service on a computer system.

Many exploits are designed to provide root-level access to a computer system. However, it is also possible to use several exploits, first to gain low-level access, then to escalate privileges repeatedly until one reaches root.

Flaming is the performance "art" of posting messages that are deliberately hostile and insulting, usually in the social context of a discussion board (usually on the Internet). Such messages are called flames, and are often posted in response to flamebait.

The term "**Hijacking**" is also used when spyware or a virus writes itself in a computer program in such a way that whenever that program starts to work, besides its normal duties it does other things too, which the creator of the virus or spyware meant it to.

SQL injection is a security vulnerability that occurs in the database layer of an application. Its source is the incorrect escaping of variables embedded in SQL statements. It is in fact an instance of a more general class of vulnerabilities that can occur whenever one programming or scripting language is embedded inside another.

Assuming the following code is embedded in the application, and a parameter "userName" that contains the user's name is given, SQL Injection is possible:

Spamming is the use of any electronic communications medium to send unsolicited messages in bulk. In the popular eye, the most common form of spam is that delivered in e-mail as a form of commercial advertising. However, over the short history of electronic media, people have done things comparable to spamming for many purposes other than the commercial, and in many media other than e-mail. In this article and those related, the term *spamming* is used broadly to refer to all of these behaviors, regardless of medium and commercial intent.

In cryptography, a **man in the middle attack (MITM)** is an attack in which an attacker is able to read, insert and modify at will, messages between two parties without either party knowing that the link between them has been compromised. The attacker must be able to observe and intercept messages going between the two victims.

A **spoofing attack**, in computer security terms, refers to a situation in which one person or program is able to masquerade successfully as another.

An example from cryptography is the man in the middle attack, in which an attacker spoofs Alice into believing he's Bob, and spoofs Bob into believing he's Alice, thus gaining access to all messages in both directions without the trouble of any cryptanalytic effort.

Many carelessly designed protocols are subject to spoof attacks, including many of those used on the Internet. Another kind of spoofing is "web page spoofing," also known as phishing. In this attack, a web page is reproduced in "look and feel" to another server but is owned and operated by someone else

Strictly defined, **spyware** consists of computer software that gathers and reports information about a computer user without the user's knowledge or consent. More broadly, the term *spyware* can refer to a wide range of related malware products which fall outside the strict definition of spyware. These products perform many different functions, including the delivery of unrequested advertising, harvesting private information, re-routing page requests to illegally claim commercial site referral fees, and installing stealth phone dialers.

In the context of computer software, a **Trojan horse** is a malicious program that is disguised as legitimate software. Trojan horse programs cannot replicate themselves, in contrast to some other types of malware, like viruses or worms. A Trojan horse can be deliberately attached to otherwise useful software by a programmer, or it can be spread by tricking users into believing that it is a useful program.

In computer security technology, a **virus** is a self-replicating program that spreads by inserting copies of itself into other executable code or documents. Thus, a computer virus behaves in a way similar to a biological virus, which spreads by inserting itself into living cells. Extending the analogy, the insertion of the virus into a program is termed *infection*, and the infected file (or executable code that is not part of a file) is called a *host*.

War dialing was a technique in the 1980s and 1990s by which a computer would repeatedly dial a number (usually to a crowded modem pool) in an attempt to gain access immediately after another user had hung up.

Wardriving is an activity consisting of driving around with a Wi-Fi equipped laptop or a PDA in one's vehicle, detecting wireless networks. Many wardrivers will use GPS

devices to find the exact location of the network found and log it on a website. Wardriving shares similarities to wardialing in name only.

A **computer worm** is a self-replicating computer program, similar to a computer virus. A virus attaches itself to, and becomes part of, another executable program; however, a worm is self-contained and does not need to be part of another program to propagate itself. They are often designed to exploit the file transmission capabilities found on many computers.

ANNEX 4 - SELECTED BIBLIOGRAPHY

Basel Committee on Banking Supervision, *General Guide to Account Opening and Customer Identification*, February 2003, attachment to Basel Committee publication n°5 "Customer Due Diligence for Banks" (www.bis.org/publ).

Binder and Gill, *Identity theft and fraud: learning from the US*, Perpetuity Research and Consultancy International, 2005 (www.perpetuitygroup.com/prci).

European Commission, *Communication from the Commission to the European Parliament, the Council and the Committee of the Regions - Towards a general policy on the fight against cyber crime*, COM(2007)267, 22 May 2007 (<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0267:EN:NOT>).

European Commission Staff Working Document, *The application of Directive 91/308/EEC on the prevention of the use of the financial system for the purpose of money laundering in relation to the identification of clients in non-face to face transactions and possible implications for electronic commerce*, SEC(2006) 1792, December 2006 (http://ec.europa.eu/internal_market/company/financial-crime/index_en.htm).

Koops (ed.), FIDIS network, deliverable 5.1, *A survey on legislation on ID theft in the EU and a number of other countries*, May 2005 (www.fidis.net).

Leenes (ed.), FIDIS network, deliverable 5.2b, *ID-related crime: towards a common ground for interdisciplinary research*, May 2006 (www.fidis.net).

Owen, Keats and Gill, *The Fight Against Identity Fraud: a Brief Study of the EU, the UK, France, Germany and the Netherlands*, Perpetuity Research & Consultancy International, June 2006 (www.perpetuitygroup.com/prci).

Pascoe, Owen, Keats, Gill: *Identity Fraud: What about the Victim?*, CIFAS – Perpetuity Research & Consultancy International, March 2006 (www.perpetuitygroup.com/prci).

UN Commission on Crime Prevention and Criminal Justice, Sixteenth session, *Results of the second meeting of the Intergovernmental Expert Group to Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity*, doc. E/CN.15/2007/8, April 2007 (www.unodc.org/unodc/en/crime_cicp_commission_session_16.html)

UK Cabinet Office, *Identity Fraud: a Study*, July 2002 (http://www.identitycards.gov.uk/downloads/id_fraud-report.pdf).

UK Joint Money Laundering Steering Group, *Prevention of Money laundering/combating the financing of terrorism – Guidance for the UK financial sector*, March 2006 (<http://www.jmlsg.org.uk/>).

US, the President's Identity Theft Task Force, *Combating Identity Theft, a Strategic Plan*, April 2007 (www.idtheft.gov).

For a selection of **identity theft/fraud related sites**, see the relevant page in the FPEG website: http://ec.europa.eu/internal_market/fpeg/identity-theft_en.htm

For **other reports of FPEG**, see: http://ec.europa.eu/internal_market/fpeg/work_en.htm