Carleton University
Sprott School of Business

Sprott Letters

Working Papers ☐ Occasional Reports ■ Article Reprints ☐
Frontiers in Business Research and Practice ☐

Research

Collaboration in Combating Identity Fraud

Vinod Kumar, Uma Kumar, and Danuta de Grosbois

November 2007 SL 2007-034

Abstract

The problem of identity theft is complex, spans the boundaries of many organizations, companies and countries, and affects numerous entities in different ways at different times. However, given the nature of the problem, it is extremely difficult and costly for an individual or an organization to fight it on its own. An increasing number of practitioners and researchers have started to indicate that the success of identity theft management relies on joint efforts of different stakeholders. Collaboration, generally defined as 'working together to some end' is believed to have the potential of delivering numerous benefits to its participants when properly executed. This paper discusses different aspects of collaboration efforts undertaken by organizations in order to fight identity theft.

About the authors

Vinod Kumar is Professor of Technology and Operations Management at the Sprott School of Business (Director,1995-2005). He is the recipient of two Scholarly Achievement Awards and three Research Achievement Awards and is Carleton University's nominee for the Premier's 2007 Discovery Award.

Uma Kumar is Professor of Management Science and Technology Management and Director of the Research Centre for Technology Management at the Sprott School of Business. She has published over 150 refereed articles and has won ten best paper awards, two Research Achievement Awards and the Scholarly Achievement Award.

Danuta de Grosbois recently completed her Ph.D. program at the Sprott School of Business and has joined Brock University. Prior to coming to Sprott she held a university teaching position in Poland.

Sprott Research Program
research@sprott.carleton.ca
Sprott School of Business • Carleton University • 1125 Colonel By Drive • Ottawa • Canada • K1S 5B6

Carleton University
Sprott School of Business

710 Dunton Tower
1125 Colonel By Drive
Ottawa, ON K1S 5B6 Canada
Tel: (613) 520-2388
Fax: (613) 520-4427
www.business.carleton.ca

Sprott Letters
Working Papers

Collaboration in Combating Identity Fraud

Vinod Kumar, Uma Kumar, and Danuta de Grosbois
Sprott School of Business, Carleton University

SL 2007-034
Ottawa, Canada ▪ November 2007

Acknowledgement
This research has been partially funded by the Ontario Research Development Challenge Fund (ORDCF) through the Ontario Research Network in e-Commerce (ORNEC).

Contact author: Dr. Vinod Kumar, vinod_kumar@carleton.ca

Sprott Letters (Print) ISSN 1912-6026
Sprott Letters (Online) ISSN 1912-6034

Sprott Letters includes four series: *Working Papers, Occasional Reports, Article Reprints*, and *Frontiers in Business Research and Practice*.

For more information please visit "Faculty & Research" at http://sprott.carleton.ca/.

COLLABORATION IN COMBATING IDENTITY FRAUD

Introduction

Identity theft is fast becoming one of the most serious and fastest growing crimes affecting millions of individuals and organizations every year. The problem became so widespread that it has lead to the creation of numerous companies offering 'identity theft insurance services' to individuals who are looking for ways of protecting themselves from the results of personal information abuse.

Although there is a lack of a common definition of identity theft, it is widely understood as the use of victims' personal information to impersonate them and illegally access their existing accounts, create new accounts, obtain or extend credit, take out loans in the victim's name, obtain accommodation, or otherwise engage in transactions by masquerading as the victim. Identity theft is also considered to include the acquisition or transfer of personal information as an instrument to commit these crimes in the future (Cavoukian, 2005).

The problem of identity theft is complex, spans the boundaries of many organizations, companies and countries, and affects numerous entities in different ways at different times. Despite significant advances in identity theft and fraud detection technologies and legal environment, many industries, including telecommunications, banking and finance, health care, Internet merchants, brokerage and securities and many others continue to incur high identity theft losses. The costs of identity theft are also passed on to society in the form of increased customer inconvenience, opportunity costs, unnecessarily high prices for goods and services, and criminal activities funded by the fraudulent gains.

The already high and rapidly growing number of identity theft cases, together with the very high costs associated with most of them, lead to the recognition by both individuals and organizations that there is a significant problem that needs to be systematically addressed. Numerous articles have been written discussing the steps that individuals can take to minimize the risk of theft of their identity and how to manage in case one becomes a victim of identity theft. Other literature provides guidance for organizations regarding 'identity theft management' or 'identity fraud management' encompassing all the activities, processes, procedures and practices that can be applied by an organization to manage and reduce the impact of identity theft activity.

However, given the nature of the problem, it is extremely difficult and costly for an individual or an organization to fight it on its own. An increasing number of practitioners and researchers have started to indicate that the success of identity theft management relies on joint efforts of different stakeholders. Collaboration, generally defined as 'working together to some end' (Fowler and Fowler, 1964) is believed to have the potential of delivering numerous benefits to its participants when properly executed. Among others, by working together, individual entities can pool scarce resources and minimize duplication of services in order to achieve objectives that would not otherwise be possible to obtain by separate actors working independently.

The need for collaboration in the context of identity theft is becoming widely recognized, but collaborative efforts aimed at identity theft management are still relatively rare and face numerous barriers hindering their creation and widespread adoption. These barriers originate, among others, from legal environment, prohibiting unlimited data sharing between different organizations, but also from the attitudes of managers in organizations affected by identity theft. Many companies are unwilling to share their security strategies and solutions but treat them as a way of gaining

competitive advantage over competitors. Even if they are interested in collaboration, companies face many difficulties and challenges. In order to put in place successful collaboration it is important to understand identity theft and distinguish between its different types and their impact. It is also important to identify all the stakeholders and their interests, strengths and threats, and understand different activities that can be undertaken to combat identity theft. Numerous questions also have to be answered, such as with whom to collaborate on which activities, how close the relationships need to be, and how to implement the collaborative structures and policies successfully.

The objective of this paper is to discuss different aspects of collaboration efforts undertaken by organizations in order to fight identity theft. Section 2 will be devoted to specifying in more detail the identity theft context, i.e. issues such as identity theft definition, interests of different stakeholders and identity theft management practices will be presented. The next two sections will be devoted to collaboration. First, the existing literature on collaboration in general will be summarized and different definitions of collaboration will be compared. Second, the dimensions of collaboration relevant for identity theft management will be identified and illustrated with examples of existing collaborations. The two final sections will offer conclusions and list of references.

1. Identity Theft Context

In order to investigate collaborative initiatives aiming at combating identity theft, it is first necessary to specify the problem domain of such collaborations, to identify all the affected stakeholders and to identify the activities that can be undertaken in order to combat identity theft.

1.1. Problem Domain

Problem domain of a collaboration is commonly defined as the general problem the participants of collaboration intend to address. In the context of identity theft, defining the problem domain of collaboration requires therefore defining 'identity theft'. Unfortunately, there is a significant confusion in the literature and media as to what is exactly meant by 'identity theft'. For different practitioners, government agencies or researchers, the label 'identity theft' covers different activities, and there is a lack of precision when it comes to distinguishing among different related concepts such as identity theft, identity fraud, account fraud or identity crime. This confusion exists despite the fact that research on identity theft would unquestionably benefit from the adoption of one definition to provide some consistency across studies and serve as a reference point for the collection of data.

Sproule and Archer (2006) conducted an extensive review of existing definitions of identity theft, identity fraud and identity crime and proposed four conceptual models that explain the relationships among these three constructs. For the purpose of this paper the model of identity theft as a precursor to identity crime is adopted and the following definitions proposed by Australasian Centre for Policing Research (ACPR) are used in a slightly modified form:

Identity Theft

> Identity theft is the theft or unauthorized acquisition, possession and/or assumption of a pre-existing identity (or a significant part of it) for criminal purposes.

Identity theft may involve an individual's identity (whether a person is deceased or alive), or the identity of a business. It generally occurs without the person's consent but also can include cases when the personal information was given willingly. It is usually associated with individuals and involves adoption of such items as name, date of birth, address, driver's licence number etc. As a result, an individual falsely represents himself or herself as another real person. Obtaining personal information can occur in many ways, ranging from careless sharing of personal information to intentional theft of purses, wallets, mail, or digital information, to dumpster diving. For an extensive discussion of the different ways in which identity theft can be accomplished see for example Gerard *et al.* (2004) and Liberty Alliance (2005).

Identity Crime

> Identity crime is any offence involving the use of a false identity.

It is important to clarify that false identities can be established in the following ways: the creation of a fictitious identity; the alteration of one's own identity; or the stealing or assumption of a pre-existing identity (identity theft). Therefore identity crime is the use of false identifiers, fraudulent documents, or a stolen identity (personal information) in the commission of a crime. The use of false identities has been linked to a range of offences, including major crimes such as people smuggling and trafficking, drug trafficking, terrorism and money laundering, but is most commonly seen in the form of identity fraud.

Identity Fraud

> Identity fraud is the gaining of money, goods, services, other benefits or the avoidance of obligation through the use of a false identity.

In other words, identity fraud is the use of fraudulent and/or stolen documentation and/or identity information to deceive a third party for a benefit or the avoidance of obligations. Examples of identity fraud include:

- the use of stolen credit cards or credit card numbers to access credit card accounts
- counterfeiting credit cards
- fraudulently obtaining money, loans, finance and credit (accessing existing bank accounts, opening new bank accounts, establishing new credit cards accounts, obtaining personal or car loans etc.)
- accessing telephone accounts
- fraudulently obtaining benefits, pensions or entitlements
- evading the payment of taxes, levies or other debts
- obtaining employment, social benefits
- filing for a bankruptcy

It is important to note that identity fraud encompasses fraud committed with the use of stolen identity of somebody else as well as fraud committed with the use of fictitious identity or modified identity. Therefore, identity theft can occur without identity fraud, if someone accesses information but does not use it, and identity fraud can occur without identity theft, if someone uses fictitious identity for fraudulent purposes.

The relationships among the three constructs (identity theft, identity crime and identity fraud) are shown in Figure 1 which is a modification of the model of identity theft as precursor of identity crime proposed by Sproule and Archer (2006).

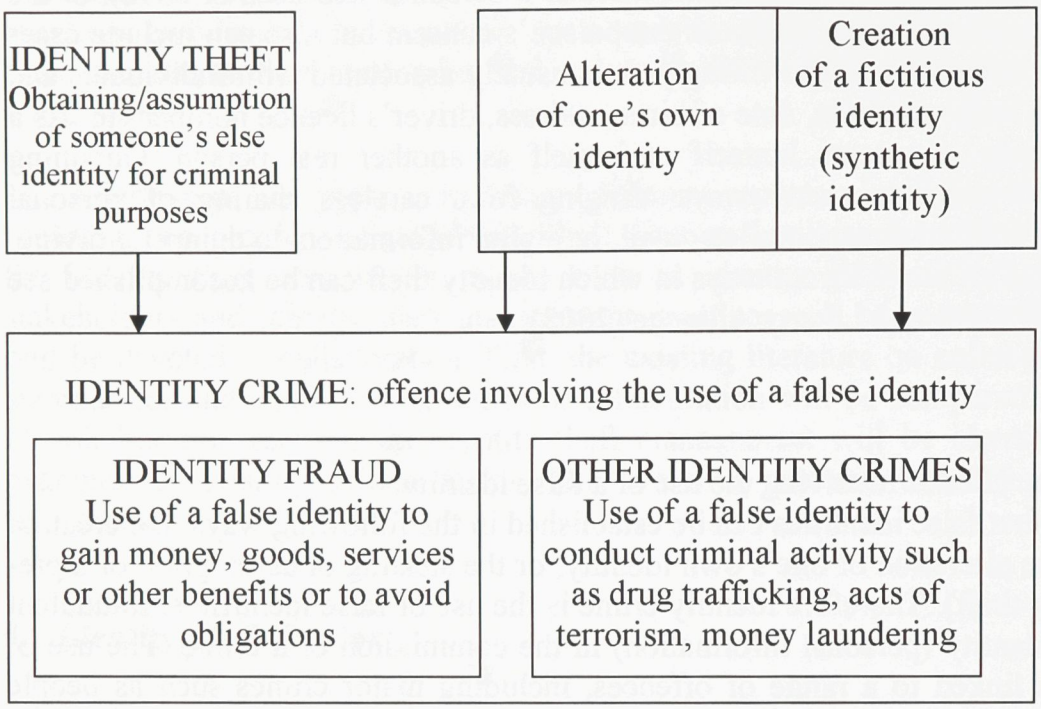


Figure 1 Relationships among identity theft, identity crime and identity fraud. Adapted from: (Sproule and Archer, 2006)

In the light of the definitions presented above, the scope of this paper encompasses collaboration efforts aimed at fighting:

- Identity theft, including both individual identity theft and corporate identity theft, and
- Identity fraud (but only committed with the use of stolen identity, not with the use of synthetic or altered identity).

For the simplicity and due to a lack of better terminology, the term 'identity theft' will refer to both the categories mentioned above in the rest of the paper. Given this problem domain definition, potential victims of identity theft are at risk of either having their identities stolen (or having the personal data of their customers, employees etc. stolen from them) or of being a victim of fraud committed with the use of the stolen identities.

The exact understanding of the scope of identity theft, crime or fraud requires specifying what constitutes a person's 'identity', i.e. what identifying information (means of identification) can be obtained by identity thieves. Means of identification include any name or number that may be used, alone or with conjunction with any other information, to identify a specific individual. The types of personal information most often considered in existing definitions of identity theft include: a person's name and address, birth date, driver's licence number, health card number, social insurance number/social security number, credit report, credit card information, bank account information, passwords and other information that can be presented on different documents such as birth certificate, personal cheques, mail, property ownership documents, tax returns etc. However, in some interpretations the identity is limited only to actual personal

information and exclude for example credit card number or debit card number. In those instances, card skimming will not be part of identity theft and subsequently identity fraud, but will represent either credit card fraud or account fraud, depending on which card was stolen.

In common language and in quite a few papers and documents identity theft is simply equated with the subset of identity fraud that is executed with the use of somebody's stolen personal information. An example of such definition is the definition proposed by the United States Federal Trade Commission (FTC) stating that identity theft is a fraud that is committed or attempted using a person's identifying information without authority.

Yet more narrow definition of identity theft is often being used by financial institutions who define it also as fraud committed using someone's else personal information but encompassing only two types of such frauds:

- 'True name' identity theft occurs when the thief obtains personal information and uses it to open new accounts, for example to open a new credit card account, to establish cellular phone service or to open a new checking account to obtain blank cheques.
- Account takeover occurs when the thief obtains personal information and uses it to gain access to the victim's existing accounts (credit card frauds, debit card frauds).

In some cases the definition of identity theft states that it is only the fraud that occurs when someone's identity is used to fraudulently establish new accounts. This definition excludes cases when a criminal uses someone's personal information to perform fraudulent activity on the existing accounts (these cases are referred to as 'account fraud', not 'identity theft').

Distinction between different types of identity theft and identity fraud is very relevant from the perspective of collaborative efforts, because different collaborative initiatives can be aimed at different types of identity theft or fraud. In order to prevent or address different types of identity theft different actions are required. Ability to distinguish between different types of identity theft can therefore guide organizations in fighting identity theft more effectively by choosing the best partners in collaboration and best actions against the given type of identity theft. The knowledge about different types of identity theft can also help to determine what type of crime is most common or most costly and needs to be addressed in the first place. In this way better understanding of different types of identity theft can help organizations to make most use of their resources devoted to combating identity theft by directing them to the most costly type of crime in first place. Therefore, it is agreed that the knowledge about different types of identity theft and their scale can guide actions aimed at preventing and addressing this problem more effectively both in terms of individual action and even more so in case of collaborative action.

1.2. Stakeholders

There are numerous entities affected by identity theft. Each has different perspective, interest, needs and understanding of the problem. There are several ways of classifying stakeholders. One of them is functional approach adopted by Wang et al. (2004) who identified the following four types of stakeholders: Identity Owners, Identity Checkers, Identity Issuers, and Identity Protectors. In this paper, stakeholders will be classified based on their main area of activity/business. This classification is chosen because the objective of this paper is to formulate guidance for any given organization on how to take advantage of collaboration with other organizations in order to fight identity theft. In this paper the following stakeholders will be discussed: individuals, financial service providers (including utility companies), other businesses

collecting and storing personal data, retail vendors, credit rating agencies, government agencies, law enforcement agencies, and technology and security support companies.

Individuals

All individuals are at risk of having their personal information stolen and falling victim to identity thieves. In case it happens they lose their good credit and reputation and are forced to spend time, money and emotional capital to restore their identity.

Victims of identity theft experience various costs as a result of the crime. These costs include lost wages or vacation time, diminished work performance, increased medical problems, impact on family and friends, financial and other costs. Also, victims suffer from so-called secondary wounding, which refers to the treatment received from various public and private agencies with which they must interact. It takes place because of the extended impact of an artificially altered credit score (due to the identity theft) or a criminal history misreported as belonging to the victim. Even after the thief stops using the information, victims struggle with the impact of identity theft. That might include increased insurance or credit card fees, difficulty in obtaining credit, clearing accounts, holding or finding a job, higher interest rates and battling collection agencies and issuers who refuse to clear records despite substantiating evidence of the crime. This "tail" may continue for more than 10 years after the crime was first discovered. Victims have difficulty to clear negative records for several major reasons. They report that the most important is related to credit agencies who either put negative information back in records or do not remove it in the first place. The next most prominent reason for not being able to clear the records quickly is victims' fraud alerts being ignored and information sold to collection agencies even though cleared by the original creditor.

As a result, identity theft costs consumers $5 billion annually in out-of-pocket costs; victims typically spend 600 hours repairing the problem; the emotional impact of identity theft has been found to parallel that of victims of violent crimes (Identity Theft Resource Center, 2004). Identity Theft Resource Center in their survey of victims of identity theft also indicated that there is still a need for improving interactions between victims and law enforcement agencies, credit reporting agencies, collecting agencies, utility companies, financial institutions, and other credit granting institutions.

Financial service providers

Financial service providers including institutions such as banks, credit unions, mortgagers, cell phone carriers, car leasors, credit card companies, insurance companies, investment companies, public utilities, and retail credit issuers, are at risk of three main types of identity theft:

- their identity being compromised (when for example a false web site is created or somebody is posting as their representative and conducting business/contacting clients)
- personal data about their customers, employees or other individuals they store being stolen
- identity-theft related financial fraud

Identity-theft related financial fraud can include categories such as: credit card fraud (new accounts and existing accounts), bank fraud (existing accounts, electronic bank transfer, new accounts), loan fraud (business/personal/student; auto; real estate), investment fraud and in general unauthorized access to all financial services.

Financial services industry incurs three main categories of costs: direct fraud losses, staffing and operating cost of fraud departments, and loss of consumer confidence in online commerce/banking. According to classification of fraud used by MasterCard and VISA, the identity theft-related fraud include account takeovers and fraudulent applications (although the fraudulent applications category can have components that do not involve identity theft). Additional fraud losses (considered to be non related to identity theft) include categories such as lost and stolen cards, never-received cards, counterfeit cards, and mail order/telephone order fraud.

Businesses outside finance industry

All organizations that collect, assemble, process, store, and retrieve information about individuals are at risk of identity theft in the form of the personal information about customers, employees etc. that they store being stolen. Organizations that do not take proactive steps to minimize the likelihood of identity theft risk increase liability exposure. Since identity theft victims are not likely to recover from thieves, they are increasingly looking to various third parties, including employers and other record keepers, for recovery for failure to protect their personal information. Failing to secure personal information kept by companies can create enormous legal liability as well as reputation risk. Therefore, the burden on corporations to protect their customers' and employees' personal information is going to increase dramatically.

According to the FTC report, identity theft losses to businesses and financial institutions amounted to $47.6 billion in 2004.
The damage to the business can be very diverse in its nature. Liberty Alliance identified the following areas:

- Brand damage: identity thieves impersonate trusted organizations, creating false emails and Web sites to steal personal information. After this activity is discovered, credibility of a organization suffers
- Costly customer account repair: corporations that issue credit to people whom they believe have good credit rating, but in reality do not pay off their debts, typically bear the cost of credit extended.
- Systems failure: in situation when a computer system is breached, organizations have to incur costs of system replacement/safety features improvement in order to prevent future attacks.
- Legal costs: this group of costs is becoming more important, as consumers who have suffered from identity theft are increasingly undertaking legal actions against organizations that have compromised their personal data to try to gain compensation for those losses.

Merchants (retail vendors)

Merchants are a specific subgroup of organizations affected by identity theft. the rules established by Visa and MasterCard, merchants are usually not liable for the loss if the fraudulent transaction was made in person. However, if the transaction was made on line or over the phone in what is known as "Card Not Present" transactions, retailers incur numerous costs: they lose the merchandise if it is not recovered; they incur the cost of processing and shipping the items; they do not receive the payment for their merchandise, because the payment is usually reversed; and they often pay a fee to the credit card company when the chargeback is made.

Credit rating agencies

Credit rating agencies are companies that assign credit rating for issuers of certain types of debt obligations. In most cases, these issuers are companies, cities, non-profit organizations, or national governments. Agencies that issue credit scores for individual borrowers are generally called credit bureaus or consumer credit reporting agencies. A credit score helps lenders assess credit worthiness, the ability to pay back a loan and can affect the interest rate applied to loans. Credit bureaus collect personal financial data on individuals from financial institutions with which they have a relationship. The data are aggregated and the resulting information is made available on request to contributing companies for the purposes of credit assessment. In the United States most credit history information is collected and kept by the three national credit bureaus, Experian (which purchased the files and other assets of TRW), Equifax, and TransUnion. Credit rating agencies play an important role in dealing with identity theft. They are responsible for keeping accurate credit rating records, and individual victims of identity theft have to deal with credit bureau to clear their accounts of fraudulent activities. In the United States, under the Fair Credit Reporting Act (FCRA), both the credit bureau and the organization that provided the information to the credit bureau (the "information provider"), such as a bank or credit card company, are responsible for correcting inaccurate or incomplete information in a given person's report.

Government agencies

Government agencies, including all administrative units of governments and law enforcement agencies in particular, are one of the most important stakeholders in the identity theft problem. Their responsibility includes formulating the law and developing national policies to deal with the identity theft problem, protecting the safety and privacy of the citizens, enforcing the law, and prosecutions of the offenders. Law enforcement agencies play a particular role among the government agencies. They are responsible for insuring obedience to the laws and in case a crime occurs, they are tasked with the collection of physical evidence, interviewing witnesses, and preparing reports that are presented to prosecutors, magistrates, judges, and juries. The effectiveness of their work depends to large degree on the input of other stakeholders in the identity theft problem.

Technology and security support companies

Technology and security support companies are important stakeholders who work on developing technological and best practice solutions to identity theft threats.

1.3. Identity Theft Management

The occurrence of identity theft forces both individuals and organizations to get involved in actions aimed at reducing its impact, i.e. to get involved in identity theft management activities. Identity theft management encompasses all the actions, activities, processes, procedures, organizational designs, economic analysis, and intra-entity exchanges necessary to manage and reduce the impact of identity theft activity.

Although organizations cannot directly influence the actions of identity thieves, they can implement procedures and programmes that can reduce the likelihood or opportunities for identity theft (Gerard et al., 2004). They include: analyzing the control structure, enhancing manual controls (control the paper trail, destroy outdated records), establishing employee controls (instituting effective background checks, requiring mandatory vacations, establishing a hotline, creating and enforcing an information security and privacy policy), enhancing computer system identity theft controls and considering insurance as a risk management tool. They are discussed further in Gerard et al., 2004. Widespread implementation of the controls outlined by Gerard et al. (2004) would accomplish two objectives: first, it is likely that the frequency and severity of occurrences of identity theft would both be reduced. Secondly, organizations would diminish their potential liability exposure, both criminal and civil, for loss of confidential personal information and subsequent identity theft events.

Therefore, there are numerous actions organizations can undertake to fight identity theft and literature is rich in prescriptions on how to deal with identity theft, directed both at individuals and organizations. However, most of the research provides just a list of possible activities but is not all encompassing and does not provide a comprehensive identity theft management framework. The frameworks existing in the literature originate mostly from fraud management research and practice. An example is work by Wilhelm (2004) who has identified eight stages of Fraud Management Lifecycle encompassing all the possible actions that companies can undertake to fight fraud. However, these frameworks do not help to identify the strengths and weaknesses of the existing systems, are not flexible, and do not analyze the fraud itself in detail. In this paper we would like to propose Action-Event Model of Identity Theft Management addressing all of the above mentioned issues.

In the Action-Event Identity Theft Management Framework (see Figure 2), identity theft is viewed as a process involving four events: threat, attempt, occurrence, and loss (they are represented by circles). Taking an example of identity theft from a perspective of an individual, the threat represents a risk or possibility that personal information of that individual can be obtained by an unauthorized person and used fraudulently. The threat becomes an attempt when a potential thief tries to obtain this information (can take place in many different ways such as an attempt at security breach at organization that is in possession of the individual's personal information, dumpster diving, stealing mail, phishing etc.). If the attempt succeeds, the occurrence of identity theft takes place: the information is in hands of the unauthorized person and can be used in different ways. The incident can lead to loss for one or more stakeholders. In case of an individual whose identity is compromised, the loss can include for example poor credit rating, refusal of additional credit, or criminal record, depending on how his or her personal information is used. The proposed model also recognizes that the actual occurrence can lead to new threats and therefore start new processes of identity theft (for example once personal information of an individual is in possession of an unauthorized person there emerges a threat that it will be used to obtain a loan, commit a crime, or open an account).

In the example of identity theft (or more precisely identity fraud) in the form of a new banking account opening (from a bank perspective), the threat represents a risk that a person can open an account in someone else's name. The treat becomes an attempt when a fraudster approaches a bank and applies for an account. The attempt is followed by actual occurrence of identity theft if the requested account is opened by the bank. This incident can lead to a loss incurred by the bank (for example when funds are withdrawn from the account) or to new threats of identity theft.

In response to the identity theft events, organizations or individuals can undertake a series of different actions. In the proposed framework there are seven distinct groups of actions (represented by rectangles):

- ***Deterrence:*** includes activities intended to stop an identity theft before it is attempted, that is, to discourage even the attempt at identity theft through, for example, card activation programs. In the view of the proposed model, deterrence stops the identity theft to move from a threat to an attempt.
- ***Prevention:*** includes activities intended to prevent identity theft from occurring, i.e. to make any attempt at identity theft unsuccessful.
- ***Detection:*** includes activities intended to reveal the occurrence of the identity theft, for example through statistical monitoring programs etc.
- ***Mitigation:*** includes activities intended to stop losses from occurring or continuing to occur and to stop a fraudster from continuing or completing his or her activity.
- ***Analysis:*** includes activities intended to explain how the identity theft happened, what failed, etc.
- ***Policies and Procedures Amendment:*** includes activities intended to improve policies and procedures to increase the efficiency and effectiveness of identity theft management.
- ***Recovery and Prosecution:*** includes activities intended to recover assets and convict the fraudster.

Every action has an outcome, on a spectrum from success to failure, which is dependent upon its strengths and weaknesses that are linked with people, processes, and technology involved in that activity. Examples of strengths and weaknesses related to the three factors include:

Strengths

- ***Technology strengths:*** multi-factor authentication, antivirus software, cards with internal chip
- ***Human factor strengths:*** banking call center employee not authorizing transaction or access to account based on his conversation with the caller; individual's knowledge about identity theft threats that prevents him or her from becoming a victim of social engineering
- ***Process strengths:*** process requiring two or more pieces of identification when opening a new banking account; contacting credit bureau by bank to verify information provided by the applicant for a new account

Weaknesses

- ***Technology weaknesses:*** signatures on credit cards, although they are an important safety feature, wear off after frequent use (bank's responsibility); not safe online banking authorization protocols (bank's responsibility); not protected databases at different companies
- ***Human factor weaknesses:*** employees selling customer information in possessions of their companies; retail clerks who do not verify the signature on a credit card with the signature of the person presenting the card; individuals who do not protect their personal information, but for example write down PIN numbers and keep them with debit cards; people falling victims of social engineering
- ***Process weaknesses:*** the requirement imposed on banks forcing them to open an account for anyone who supplies necessary documentation; telebanking process (asking certain questions

to verify identity of a caller but without compromising too much of his convenience); companies asking individuals to provide their social insurance numbers in order to access their services

It is important to recognize that in every case of identity theft process, the weaknesses and strengths that allow it to progress from a threat to losses or that stop it, are not within the authority of only one stakeholder. Different stakeholders can be involved in different events and actions. An individual's personal information can be obtained from the company he is employed at; it can be then used to open an account and obtain a credit card at a bank; then the credit card can be used for an online purchase (card not present transaction) which will lead to a loss incurred by the retail vendor. The stakeholders involved in this scenario include the individual, his employer, bank and retail vendor. Given this multi-stakeholder nature of identity theft, the strengths and weaknesses that exist along the process, also are not in control of one stakeholder but are composite of numerous stakeholders. If a thief attempts to use a stolen credit card at a store, different strengths can make his attempt unsuccessful, for example store clerk who verifies the signature of the person trying to make the purchase and the signature on the card or the existing limit on the account posted by the real user of the card. However, weaknesses of different stakeholders can lead to attempts becoming successful.

Similarly, the actions within the identity theft management can be undertaken not by one stakeholder, but by a number of stakeholders. Individuals can find out that they are victims of identity theft either on their own or when they are notified by other organization; in order to respond to it, they need to contact different creditors, credit rating agencies, possibly utility companies and with their help restore the individuals' original credit and names. They might also involve law enforcement agencies in order to prosecute the offender.

The model also recognizes that there are numerous relationships among the stakeholders (credit card agreements between banks and individuals; relationships between banks and vendors accepting the banks' payment cards).

The proposed model provides a framework for systematic assessment of the identity theft problem. A given organization willing to analyze a given threat of identity theft (for example takeover of an existing account) can model this kind of identity theft with the proposed process approach. It will enable identification of all involved stakeholders and their existing and potential role in the process:

- people, process and technology strengths associated with each stakeholder
- people, process and technology weaknesses associated with each stakeholder
- the role of each stakeholder in conducting different actions to manage identity theft

Identification of all the roles of involved stakeholders will determine the areas where different stakeholders can contribute and therefore the areas for potential collaboration.

2. Defining Collaboration

In situations in which working alone is not sufficient to achieve a desired end, collaboration with other entities is the most widely recommended approach. In a general sense, collaboration means "working together to some end" (Fowler and Fowler, 1964; Huxham, 1996, Jordan and Michel,

2000). Definitions of collaboration provided by different dictionaries include the following: "working together", "a joint venture", "working jointly with others", "joining forces", "working in partnership", and "pooling resources". From these sources, collaboration appears to signify just about any relationship between individuals or organizations working together towards a common aim. As described by Gray (1989) collaboration can be used effectively to pool scarce resources, minimize duplication of services, resolve conflict or advance shared visions, where stakeholders recognize the potential advantages of working together.

Given the fact that collaboration is receiving widespread attention in several research disciplines, especially in social sciences and organizational research, also the academic literature provides vast conceptualizations of collaboration, explains the need for it and identifies the factors that influence the quality and success of collaboration. In general, there is lack of consensus on the definition and understanding of dimensions of collaboration. Smith et al. (1995) pointed out that "one difficulty in interpreting the theory and research on cooperation stems from the numerous definitions of cooperation scholars have offered without making much attempt to reference other usage of the term". Unfortunately, the literature is very confusing and often the same words are used to express different meanings or the same concepts are given different names by different authors. Examples of the academic definitions state that collaboration is:

- 'Taken to imply a very positive form of working in association with others for some form of mutual benefit' (Huxham, 1996).
- 'A distinct mode of organizing, implies a positive, purposeful relationship between organizations that retain autonomy, integrity and distinct identity, and thus, the potential to withdraw from the relationship' (Huxham, 1996).
- 'A number of companies linked to create and support a service or product for its service life including final disposal' (Jordan and Michel, 2000).
- 'A focus on joint planning, coordination and process integration between supplier, customers and others partners in a supply chain. Also involves strategic joint decision making about partnership and network design' (McLaren et al., 2000).
- 'A process in which organizations exchange information, alter activities, share resources and enhance each other's capacity for mutual benefit and a common purpose by sharing risks, responsibilities and rewards' (Himmelman, 1992 cited in Huxham, 1996).
- "A process of joint decision making among key stakeholders of a problem domain about the future of that domain" (Gray, 1989).
- "A cooperative, interorganizational relationship that is negotiated in an ongoing communicative process and that relies on neither market nor hierarchical mechanisms of control" (Lawrence et al., 2002).

Apart from the extensive number of different definitions of collaboration, different terms are commonly applied interchangeably in the literature to describe the notion of individuals or organizations working together to accomplish a specific task. Among them are: collaboration (Trist, 1977; Jassawalla and Sashittal, 1998; Lawrence and Lorsch, 1967), coordination (Argote, 1982; Van De Ven *et al.*, 1976), cooperation (Schermerhorn, 1975; Pinto *et al.*, 1993), integration (Gupta et al., 1986), and interaction (Moenaert and Souder, 1990), and more specifically in inter-organizational context: joint ventures, consolidations, networks, partnerships, coalitions, collaboratives, alliances, consortiums, associations, councils, etc.

All the above presented constructs refer to a similar and overlapping idea of joint behaviour toward some goals of common interest; however, by many researchers they are not treated as equal (Todeva and Knoke, 2005; Peterson, 1991; Gajda 2004). Literature on collaboration and strategic alliance development strongly supports opinion that there are varying degrees and types of linkages that develop between agencies that seek to work together in some capacity. Most collaboration theorists argue that collaborative endeavors fall across continuum of low to high integration depending on the intensity of the collaboration's process, structure, and purpose. Valuable distinction is provided by, among others, Peterson (1991) who in his research on strategic alliances postulated that there is a following three point continuum of interaction among partners:

(1) **cooperation**, whereby fully independent groups share information that supports each others organizational outcomes,

(2) **coordination**, whereby independent parties align activities or co-sponsor events or services that support mutually beneficial goals,

(3) **collaboration**, where individual entities give up some degree of independence in an effort to realize a shared goal.

For the purpose of this paper collaboration is defined as the process of working together of different individuals, groups or organizations towards a common aim (Huxham, 1996; Bittitci et al., 2004; Song et al., 1997; Souder and Moenaert, 1992) and encompasses all the three levels of interaction discussed by Peterson (1991). This definition of collaboration is inclusive enough to encompass a wide range of collaborative arrangements (for instance, consortia, alliances, joint ventures, round-tables, networks, and associations). The definition proposed here encompasses wide range of joint efforts, whether they involve only information sharing or more activities such as joint decision making or joint strategy development.

3. Collaborations Addressing Identity Theft

During the last ten years, numerous collaborative efforts were started to address different identity theft or fraud-related issues. They have very different origins, memberships, objectives, and had to overcome significant challenges to operate successfully. The next sections will present comparisons of some major collaborative initiatives. The detailed descriptions of all the collaborations mentioned in this section can be found in the Appendix B.

3.1. Origin

The existing collaborations aimed at addressing identity theft and fraud originated from very different sources. A significant number of them were initiated by governments or law enforcement agencies of different levels. These collaborations include the Financial Services Information Sharing and Analysis Center (FS/ISAC), Internet Crime Complaint Center (IC3), Consumer Sentinel and InfraGard in the United States; and the Reporting Economic Crime Online (RECOL) in Canada. The FS/ISAC was launched as a result of presidential directive requesting the public and private sectors to create partnerships to share information about physical and cyber threats, vulnerabilities, and events to help protect the critical infrastructure of the United States. Internet Crime Complaint Centre was created jointly by the National White Collar Crime Centre (NW3C) and the Federal Bureau of Investigation (FBI). Its equivalent in Canada, the Reporting Economic Crime Online, was initiated by the National White Collar Crime Centre of Canada (NW4C) and the Royal Canadian Mounted Police (RCMP). Consumer Sentinel is an international

joint project of law enforcement agencies from Australia, Canada and the United States. Finally, InfraGard was initiated by the Cleveland Field Office of the Federal Bureau of Investigation.

Other stakeholders, especially the financial services industry, have also shown significant initiative to collaboratively respond to the identity theft problem. The financial services industry in the U.S. (represented by members of the Financial Services Roundtable and BITS) has formed the Identity Theft Assistance Corporation in order to provide identity theft victim assistance services. The financial services industry in the United Kindgom has created Credit Industry Fraud Avoidance Scheme. Another collaboration, the PCI Security Standards Council, was founded jointly by American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International. Stakeholders from other industries also have shown initiative and initiated several collaborations to address the identity theft issues. For example, security solutions providers have created their own alliance to address identity theft issues: the Cyber Security Industry Alliance.

Still more collaborative efforts were created jointly by organizations from different private sectors and sometimes government or law enforcement agencies. An example is the Liberty Alliance Project which is a global alliance of more than 150 companies, mostly banks, telecommunication companies, service providers and vendors; and non-profit organizations and government agencies. Another example of a global multi-industry association focused on eliminating the identity theft and fraud is the Anti-Phishing Working Group, with more than 2400 members worldwide. Members of the APWG include financial institutions, online retailers, ISPs, law enforcement agencies, security solutions providers and research institutions.

3.2. Membership

Most of the collaborations do not limit their membership only to the founding organizations. However, they introduced very different policies for companies that are eligible for the membership.

For example, the Identity Theft Assistance Corporation originally allowed only members from the financial services sector. However, after less than two years, its membership was opened also to retailers and utilities. To join ITAC, a company must have an ongoing business relationship with individual consumers, and be able to authenticate the consumer's identity and verify the existence of identity theft. Similarly, CIFAS has member companies from different industries, including finance and leasing organizations, banks and credit cards, building societies and mortgage lenders, discounters, insurers, companies specializing in telecommunications, energy supply, mail order, share dealing and fund management. Membership of CIFAS is open to all consumer and commercial/corporate credit grantors; e.g. loan providers, credit card issuers, mortgage lenders; deposit takers; e.g. banks etc.; leasing and hire companies; motor finance providers; insurance companies; other providers of products, services and facilities; e.g. telecommunication service providers, factors and discounters, mail order, stockbrokers etc. Membership is not open to intermediaries, such as brokers, independent financial advisers, or loss adjusters, or to debt collection agencies, tracing agents and private investigators. The FS/ISAC, on the other hand, allows strictly firms in the financial services sector to become members and Consumer Sentinel – only law enforcement agencies.

Other collaborations allow very different stakeholders to become members. Members of the Anti-Phishing Working Group include financial institutions, online retailers, ISPs, law enforcement agencies, security solutions providers and research institutions from all over the world. Similarly, the Liberty Alliance Projects has members including banks, telecommunication companies, service providers, vendors and government agencies.

Several of the collaborations use multiple tiers of memberships, with different services available to different members. Usually these collaborations also require their members to pay annual fees, depending on the type of membership. Examples include, among others, the FS/ISAC and the APWG.

3.3. Organization and Management

Collaborations devoted to combating identity theft can take different organizational forms, ranging from sub-committees or working groups created within existing associations or trade unions to new separate organizations created jointly by a number of stakeholders, either already collaborating within an existing association or working together for the first time.

For example, the Identity Theft Assistance Corporation is an independent non-profit industry consortium created by the Financial Services Roundtable and BITS. The financial institutions that created the Identity Theft Assistance Corporation were therefore already grouped within the Financial Services Roundtable and BITS, representing 100 of the largest integrated financial service companies in the U.S and had experience with working together on other issues. These issues include public policy initiatives (Financial Services Roundtable) and development of electronic financial services and e-commerce (BITS), as well as experience in facilitating cooperation with other stakeholders, including government organizations, technology providers and third-party service providers. Similarly, the Financial Services Information Sharing and Analysis Centre is an independent private partnership of major banks, insurance companies and utilities.
The PCI Security Standards Council is a limited liability corporation.

CIFAS is a non-profit association of consumer and commercial/corporate credit grantors. Similarly, Information Technology Association of America, Anti-Phishing Working Group, and Messaging Anti-Abuse Working Group are trade associations representing different industries, either nationally or multinationally.

Cyber Security Industry Alliance and Libery Alliance Project are global alliances .
Other types of collaborations aimed at combating identity theft take a form of partnerships where stakeholders together establish not an independent organization but conduct a project: for example law enforcement agencies contrubuting to the Identity Theft Data Clearinghouse.

Identity Theft Data Clerainghouse was created within the Consumer Sentinel project bringing together more than 1000 law enforcement agencies from Australia, Canada and the US. It is managed by the Federal Trade Commission. The collaboration has a form of a database to which all the members contribute and which all of them can use. It is not a separate organization.

They can be created as a totally new entity or as a part of an existing collaboration, aimed at addressing other things that started to recognize the importance of identity theft policy and either

included identity theft in its mandate or created a separate sub-committee or organization devoted solely to identity theft.

For example, in 1999, the U.S. Department of Justice established the Sub-committee on Identity Theft in the Attorney General's Council on White-Collar Crime. The Sub-committee, which includes representatives of federal law enforcement and regulatory agencies, as well as representatives of state and local law enforcement, meets monthly to share information and facilitate coordination among all levels of law enforcement on identity theft issues. Similarly, the Prevention of Crime in Industry Committee (PCIC) is a sub-committee of the Canadian Association of Chiefs of Police that provides a forum for discussion and collaboration with Canadian police executives, government policy advisors and key private sector corporations on emerging criminal trends and corresponding remedial actions. The PCIC has a working group focused specifically on identity theft.

The Canada-United States Cross-Border Crime Forum determined that it would be appropriate to conduct a threat assessment of identity theft and its impact on cross-border criminality. It directed the Canada-United States Working Group on Cross-Border Mass-Marketing Fraud,
the Identity Theft Data Clearinghouse within the Consumer Sentinel.

3.4. Scope and Objectives

All of the analyzed collaborations work towards elimination of the identity theft problem. However, they significantly differ in their scope and objectives. Some of them address only a narrow subset of the identity theft domain. For example, most of the collaborations originating from financial sector, either address the financial fraud in general or they address the identity theft defined as solely the creation of a fraudulent new account in a consumer's name or the takeover of an existing legitimate account. Their objectives are usually either to assist the victims or to help the members protect themselves from losses related to identity theft. Collaborations serving the law enforcement community have a much wider scope and often address all cases of identity theft understood as any unauthorized use of false identity (Consumer Sentinel) or even address economic crime in general (RECOL). These collaborations focus on providing victims with the possibility to report the crime to the police and have their case referred to the appropriate law enforcement or regulatory agency. They also provide law enforcement with data and tools to analyze trends and prosecute offenders. Industry associations led by software companies focus on a given aspect of identity theft and work on finding technological and best practices solutions to that problem. For example, the objective of APWG is to eliminate identity theft and fraud that result from the growing problem of phishing and email spoofing and the spread of crimeware that automatically mines consumers' personal data from their computers.

3.5. Collaborative Activities

Activities performed by a collaboration differ significantly in its nature and the level of its members' involvement.

One of the most common joint activities of collaboration's members is data collection, sharing and analysis. Data collection and data sharing that takes place in the collaborations aimed at addressing identity theft can be of very different scope. It depends on the data possessed by the membership organizations and on the data collected by the collaboration itself. For example, the

ITAC collects data on identity theft cases that took place at member companies and then shares the data with its members, with the Consumer Sentinel Database run by the FTC and with the U.S. postal service. The collection and sharing of data lead to the development of the collaborative databases such as:

- Identity Theft Data Clearinghouse (part of Consumer Sentinel project): database of consumer fraud and identity theft complaints submitted by victims to the FTC and to over 100 different U.S. and Canadian federal, state, and non-governmental organizations. Access to the data is provided to the members of Consume Sentinel network (i.e. law enforcement agencies from the U.S., Canada and Australia)
- Internet Crime Complaint Center: database of complaints related to Internet crime filed by victims. Access to the data is provided to law enforcement and regulatory agencies in the U.S.
- Reporting Economic Crime Online: database of complaints related to economic crime, including everything from credit card fraud to major corporate corruption
- The ITAC database includes identity theft cases detected by member companies. Data is shared with all members, the Consumer Sentinel Database run by the FTC and the U.S. postal service.
- FS/ISAC has a database of cyber and physical security threats faced by the financial services sector. Data only available to members, not shared with government agencies.

An example of a very special and unique system of data sharing is represented by the CIFA's Fraud Avoidance System. Members of CIFAS are required to operate effective in-house procedures to enable fraud or attempted fraud to be identified and the cases placed into classifications known as the CIFAS categories. Basic information on each case is filed on the CIFAS database. The information is then transferred electronically to all agencies. When an address against which a fraud has been filed, is searched, by any other .member, through any participating agency, the searching member is made aware of the need to investigate through a warning, followed by the CIFAS category, and the identity of the Member filing the data.

Other activities conducted by the members of collaborations include analysis of the data stored in databases in order to identify trends and patterns in identity theft,; providing of the best practice guidance, training and networking opportunities for the members; providing of services directed to the general public (e.g. providing information for consumers on identity fraud, both as a leaflet and at a website; providing advice for consumers on what to do if they believe they may have fallen victim to identity fraud or impersonation), and organizing different events and conferences.

Several collaborations have undertaken initiatives that are very unique and one-of-a-kind,. They include, among others, the following projects:

- Victim Assistance Service: The Identity Theft Assistance Corporation offers free assistance to victims of identity theft if they are customers of member companies (uniform affidavit to report fraud only once, assistance in dealing with credit reporting agencies, notification of the affected creditors). It also assists victims of identity theft in correcting the damage caused by the crime
- Crisis Alerts: FS/ISAC gathers threat, vulnerability, and risk information about cyber and physical security risks faced by the financial services sector. Sources of information include commercial companies who gather this type of information, government agencies, law

enforcement, CERTs, academic sources, and other trusted sources. After analysis by industry experts, urgent and crisis alerts are delivered to participants based on their level of service

- PCI Security Standards: PCI council develops and maintains a global, industry-wide technical data security standard for the protection of payment account information;
- Identity Fraud Index: CIFA, the first UK Identity Fraud Index developed from data supplied by its members in order to identify the business sectors being mostly targeted by fraudsters and organised crime

4. Conclusions

In the authors' observation, collaborative forms for identity theft management are a relatively new and emerging field of study. There are two main perspectives when investigating collaborations aimed at fighting identity theft. The first perspective focuses on organizations created or projects undertaken by a group of stakeholders in order to address the given problem related to identity theft. In this case, a particular collaboration effort is the unit of analysis. This paper followed this approach by identifying and comparing different organizations, collaborative in nature, aimed at addressing the problem of identity theft. However, another way of looking at the collaboration in combating identity theft is to take a perspective of a single organization, for example a bank, and identify all the collaborative efforts this organization is part of, what are the benefits from participation and identify what kind of collaboration, with whom and on what would be the most beneficial. In this case a particular company or organization is the unit of analysis. However, even if it can be determined what portfolio of collaborative efforts is best for a given company, there are still numerous difficulties faced by it when the collaboration is being implemented and executed. Future questions to be answered based on the empirical studies are therefore:

- identify facilitators to collaboration for identity theft management through empirical research
- identify potential inhibitors and problems that may arise during collaboration and identify appropriate actions to resolve them
- identify collaboration practices adopted in practice
- identify what are the activities that would benefit from collaboration
- investigate the stages and implementation of the collaboration process, with attention paid to the development of appropriate structures for ongoing management of identity theft (sharing information practices etc)
- investigate how collaboration improves effectiveness of identity theft management activities
- investigate and identify organizational forms most suited to fight identity theft

5. References

[1] Bielski, L. (2001). Identity theft, ABA Banking Journal, 93 (1).

[2] Bittci, U., Martines, V., Albores, P., and J. Parung (2004). Creating and managing value in collaborative networks, International Journal of Physical Distribution and Logistic Management, 34 (3/4), 251-268.

[3] Childerhouse, P., Disney, S.M., Lockami, A. III, McCormack, K. and D.R, Towill (2003), Proven BPR trajectories for effective supply chain change management, in Spina, G., Vineli, A., Cagliano, R., Kalchschmidt, M., Romano, P. and F. Salvador (Eds.), Proceedings of the 1st International Joint Conference EurOMA (European Operations

Management Association Conference) – POMS (Production and Operations Management Society): The Challenges of Integrating Research and Practice, Vol. II, pp. 71-80.

[4] Hemphill, T. (2001). Identity theft: A cost of business? Business and Society Review, 106 (1).

[5] ID Theft Tops FTC Complaints for 2005, Information Management Journal, 40 (3), 19.

[6] Lepofsky, R. (2004). Preventing identity theft, Risk Management, 51 (10).

[7] Smith, J., and J. Frisby (2004). A five-step plan for comprehensive information security and privacy, Bank Accounting & Finance.

[8] Sproule, S., and N. Archer (2006). Defining Identity Theft – A Discussion Paper, McMaster eBusiness Research Centre (MeRC), McMaster University.

[9] Wang, W., Y. Yuan, et al. (2004). A Theoretical Framework for Combating Identity Theft; MeRC Working Paper No. 12. McMaster eBusiness Research Centre (MeRC). Hamilton, ON, McMaster eBusiness Research Centre (MeRC), McMaster University.

[10] Wesley, K. (2004) The Fraud Management Lifecycle Theory: A Holistic Approach to Fraud Management, Journal of Economic Crime Management, 2 (2), 1-38.

6. Appendix A: Comparison of Major Collaborations Addressing Identity Theft

Collaboration	Year Established & Founders	Members	Mission	Scope	Activities
The Identity Theft Assistance Corporation	January 2004 Financial Services Roundtable and BITS, USA	Financial service companies; since October 2005 also retailers and utilities	To provide a free victim assistance service for customers of member companies	Identity theft defined as the creation of a fraudulent new account or the takeover of an existing account	• Manages the Identity Theft Assistance Center • Uniform affidavit to report fraud used by all members • Free assistance for victims of identity theft: customer reports fraud only once on the uniform affidavit provided, then ITAC notifies the affected creditors (both members of ITAC or non-members) and places a fraud alert with the credit bureaus • ITAC shares data on identity theft cases with its members, the Consumer Sentinel Database run by the FTC and with the U.S. Postal Inspection Service
Financial Services Information Sharing and Analysis Center	1999 President's Commission on Critical Infrastructure Protection & financial industry	Firms eligible for membership include the firms in the financial services sector	To disseminate trusted information to increase sector wide knowledge about physical and cyber security risks faced by the financial services sector.	All cyber and physical security risks faced by the financial services industry	• Gathers information about cyber and physical security risks faced by the financial services sector • Delivers normal, urgent and crisis alerts with a description of the threat or vulnerability, its severity, and recommendations for solutions to participants • Delivers of DHS and Treasury alerts in times of crisis • Conducts member meetings, conference calls, customized analysis, best practices information sharing
PCI Security Standards Council	Sept, 2006 American Express, Discover Financial Services, JCB, MasterCard and Visa International	merchants, payment devices and services vendors, processors, financial institution and others are invited to participate	To enhance payment account data security by fostering broad adoption of the PCI Security Standards	Financial fraud	• owns, develops, maintains and distributes the PCI Data Security Standard (DSS). • promotes its broad industry adoption • defines qualifications for Qualified Security Assessors (QSAs) and Approved Scanning Vendors (ASVs); and trains, tests and certifies QSAs and ASVs • provides the tools needed for compliance with the standard, including audit guidelines, scanning vendor requirements, and, a self assessment questionnaire
Credit Industry Fraud Avoidance	1988 major retail credit lenders in the UK	over 240 member companies Membership open to all	To protect the interests of CIFAS members from the actions of criminals	Financial fraud	• providing a data sharing scheme (fraud avoidance system) enabling financial services and other companies to share information on fraud cases they prevent or detect

23

Scheme		consumer and commercial/corporate credit grantors; but not intermediaries	by pooling information on fraud and attempted fraud		• providing best practice guidance, training and networking opportunities for its members • 'Protective Registration' service for victims to protect their identity from misuse • launching the first UK Identity Fraud Index developed from data supplied by its members
Identity Theft Data Clearing-house	November 1999	Part of Consumer Sentinel project with members including more than 1000 law enforcement agencies from Australia, Canada and the United States	To provide identity theft victims with a central place in the federal government to report their problems and receive information	Identity theft	• It is the federal government's database for tracking identity theft complaints submitted by victims to the FTC • through data sharing agreements it includes not only consumer fraud and identity theft complaints received by the FTC, but also complaints from over 100 different U.S. and Canadian federal, state, and non-governmental organizations provides both U.S. and Canadian members of the Consumer Sentinel network with direct, online and secure access to the consumer complaints
Internet Crime Complaint Center (IC3)	May 2000 the National White Collar Crime Center (NW3C) and the FBI	international, federal and state law enforcement agencies, regulators and selected commercial organizations	to serve as a vehicle to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cyber crime	fraud committed over the Internet	• Provides, in a central point, a convenient and easy way for Internet crime (including identity theft and fraud) victims to report the possible crime • provides a central repository for complaints related to Internet crime, available to law enforcement and regulatory agencies • refers all fraudulent activity identified on the Internet to the appropriate federal, state, local, or international law enforcement agency • analyzes received Internet crime complaints in order to identify patterns and current trends in Internet crime • shares its Internet fraud and identity theft complaint data with the FTC for inclusion in the Identity Theft Data Clearinghouse
Reporting Economic Crime Online (RECOL)	October 2003 National White Collar Crime Centre of Canada	international, federal and provincial law enforcement agencies, regulators and	To provide Canadians with a single point of entry to make a complaint on any economic crime including fraud	Economic crime	• gives citizens a single Web site for reporting everything from credit card fraud to major corporate corruption • Crime complaints filed at the RECOL site are prioritized automatically and forwarded to the relevant RECOL partners selected by the complainant • for improved communication between law enforcement

	(NW4C) and the RCMP	selected commercial organizations	like identity theft, fraudulent letter or telemarketing scams and other white-collar crimes		jurisdictions • provides data pertaining to trends, as well as information relating to consumer education, prevention and awareness of economic crime
Liberty Alliance Project		more than 150 members, including banks, telecommunications companies, service providers, vendors and government agencies	to establish technical, business and policy standards for digital identity management and Web services; to serve as a hub for a global effort against identity theft and will be attacking issues from multiple perspectives in a collaborative, open and vendor-neutral environment	Identity theft	•
Anti-Phishing Working Group		open to qualified financial institutions, online retailers, ISPs, law enforcement agencies, security solutions providers, and research institutions; more than 2400 members	to eliminate the identity theft and fraud that result from the growing problem of phishing and email spoofing and the spread of crimeware that automatically mines consumers' personal data from their computers	Identity theft and fraud resulting from phishing	• collaborative technology development to facilitate the rapid deployment of a solution to e-mail phishing scams • prepared a report on 'crimeware' – software that performs illegal actions unanticipated by a user running the software • Together with the Messaging Anti-Abuse Working Group (MAAWG), the APWG jointly developed set of best practices for ISPs to combat phishing, a major cause of online idenitiy theft and fraud. • provides forum to discuss phishing issues, trials and evaluations of potential technology solutions, and access to a centralized repository of phishing attacks

7. Appendix B: Case Studies

Canadian Collaborations

7.1. Canadian Bankers Association (CBA)

Origin and Membership
The Canadian Bankers Association was established in 1891 to represent all banks in Canada.

All chartered Canadian banks can become members of the Association, and foreign banks that operate in Canada are also members of the Association.

Organization and Management
In terms of governance, the Canadian Bankers Association has an Executive Council that functions like a Board of Directors. Representatives from the six largest domestic banks, other Canadian and foreign banks sit on the Executive Council. There is the Executive Committee to which various Senior Committees report.

Scope and Objectives
The Canadian Bankers Association's mission is to help develop public policy that benefits the financial services sector, and to ensure that the legal and regulatory framework in which banks operate is effective, efficient, and fair. The Association also organizes activities to promote greater understanding of the Canadian banking industry among the public, government agencies, international bodies, various interest groups and the media.

Collaborative Activities
In terms of efforts on combating identify theft and related crimes, the Associations sets up the Bank Crime Prevention and Investigation Office (BCPIO). The BCPIO works to protect bank customers from financial crimes. The BCPIO is also designated under the federal Personal Information Protection and Electronic Documents Act as an investigative body, and that is overseen by the Privacy Commissioner of Canada.

7.2. Federal/Provincial/Territorial (FPT) Council on Identity

Origin and Membership
With increased incidents of entitlement fraud in publicly-funded programs, a rise in identity theft, and in the aftermath of the 2001 terrorist attacks, the security and integrity of identity documents have become a major concern. Federal, provincial and territorial ministers agreed that current Canadian identity policies require review and that a new approach to identity should be considered. The FPT Council on Identity was established and tasked with reviewing Canada's current identity policy; developing a consensus among jurisdictions on a comprehensive approach to identity including common definitions, best practices and standards.

Organization and Management
The FPT Council is chaired by Foreign Affairs Canada and has representatives from all Canadian jurisdictions and various program areas

Scope and Objectives
The Council is tasked with drafting an identity policy framework for further consideration.

Collaborative Activities

7.3. PhoneBusters National Call Centre (PNCC)

Origin and Membership
PhoneBusters was established in January 1993 as a national anti-fraud call centre that collects information on telemarketing fraud. The PNCC is a joint operation by the Ontario Provincial Police and the Royal Canadian Mounted Police.

Organization and Management
The call centre is operated by the OPP and the RCMP, but it has other funding partners. The Competition Bureau of Canada and the Visa Canada both work with PhoneBusters to combat telemarketing frauds.

Scope and Objective
PhoneBusters plays a key role in educating the public about specific fraudulent telemarketing pitches. The PNCC also plays a vital role in the collection and dissemination of victim evidence, statistics and documentation. PhoneBusters's original mandate was to prosecute key individuals in Ontario and Quebec who were involved in telemarketing fraud under the Criminal Code of Canada. Its new mandate has included facilitating prosecution by the United States agencies through extradition, and by Industry Canada under the Competition Act.

Collaborative Activities
Although it has email capacity, most complaints are phoned in to the PNCC. The information is then disseminated to the appropriate law enforcement agencies. Due to the ever-increasing number of complaints about identity theft, PhoneBusters started an Identity Theft project in 2002. The data collected at PhoneBusters is a valuable tool in evaluating the effects on the public of various types of fraud. It also helps to prevent future similar crimes from taking place.

SeniorBusters is another program specifically created to educate and protect seniors from telemarketing frauds. Recognizing that seniors are more vulnerable because they are more trusting of people who sound friendly on the phone, the program works with local police agencies, senior groups and family members to equip elderly with the necessary knowledge and tool to fight the crime. The program also provides support to seniors who are victims of telemarketing frauds.

7.4. Reporting Economic Crime Online (RECOL)

Origin and Membership
The Reporting Economic Crime Online (RECOL) is a RCMP-led web-based initiative that involves an integrated partnership between international, federal and provincial law enforcement agencies, as well as regulators and private commercial organizations that have a legitimate investigative interest in receiving a copy of complaints of economic crime, including identity theft. RECOL also provides data pertaining to trends, as well as information relating to consumer education, prevention and awareness of economic crime.

The formation of RECOL was announced on October 3, 2003 by the National White Collar Crime Centre of Canada (NW4C)[1] and the RCMP. The NW4C is a major partner in the RECOL initiative and is actively engaged in fostering private-sector participation. Other partners in the development of RECOL include the Ontario Provincial Police and the U.S. Federal Bureau of Investigation.

Scope and Objectives

RECOL is an Internet-based tool for reporting domestic economic crimes. It aims to offer Canadians a single point of entry to make a complaint on any fraud such as identity fraud and telemarketing scams, and other white-collar crimes, allowing them to take immediate actions against these crimes through submitting complaints on the Internet. RECOL also aims to raise awareness of economic crimes, as well as to improve communication among domestic and international law enforcement jurisdictions.

Collaborative Activities

RECOL handles complaints from Canadians on identity theft. Once complaints are made, they are prioritized and then directed to the appropriate law enforcement agencies and other organizations concerned with white-collar crime according to the wishes of the user. There is free information flow between RECOL and its partners. In this way, RECOL allows for improved communication between law enforcement jurisdictions, helping eliminate barriers and stopping criminals who might otherwise evade investigation and prosecution.

Support for individuals filing complaints to RECOL is provided by the PhoneBusters National Call Centre (1-888-495-8501), which was established 10 years ago to combat deceptive telemarketing.

Between October 2003 and March 2004, more than 1,054 fraud complaints have been filed with RECOL.ca and consumers valued the crimes they reported at more than $481.9 million

RECOL's major partners are the RCMP and PhoneBusters. Its other partners include the Ontario Provincial Police, the U.S. Internet Fraud Complaint Center, MasterCard Canada and the Canadian Health Care Anti-Fraud Association.

7.5. The Fraud Prevention Forum

Origin and Membership

The Fraud Prevention Forum is formerly known as the Deceptive Telemarketing Prevention Forum. It is organized by a concerned group of private sector firms, consumer and volunteer groups, government agencies and law enforcement organizations in Canada that are committed to fighting fraud aimed at consumers and businesses.

Membership in the Forum has grown considerably over the years. At the initial launch in 2004, there were 22 members. Today, there are over 80 of them, ranging from government agencies to financial institutions to trade associations to corporations.

---

[1] NW4C is a not-for-profit corporation established to help combat and prevent economic crime through partnership with the private, public and law enforcement sectors.

The Fraud Prevention Forum model has been adopted around the world. Twenty-nine countries have

Organization and Management
The Forum is chaired by the Competition Bureau, which is primarily responsible for investigating anti-competitive activities such as deceptive telemarketing and

Scope and Objectives
Through its partners, the Forum, which is chaired by the Competition Bureau, works to prevent Canadians from becoming victims of fraud by educating them on how to "**Recognize it. Report it. Stop it.**"

Collaborative Activities
In March 2004, the Competition Bureau, as chair of the Fraud Prevention Forum, unveiled an anti-fraud public education campaign in Toronto. This campaign is the first international effort of its kind to combat the growing epidemic of fraud targeted at consumers and businesses by helping Forum partners educate consumers. The Federal Trade Commission is adapting the campaign's material for use throughout the United States. The Office of Fair Trading in the UK is supportive of the campaign and is looking for its own opportunities to use the material to educate its citizens.

In 2006, the Competition Bureau partnered with Shred-it to launch the first national Fraud Prevention Community Shredding Event in 20 Canadian cities. Canadians were encouraged to come out for the day and shred any unwanted personal documents, and the event resulted in a total of 122,066 pounds of paper being shredded.

In every March, the Forum organizes a month-long campaign to raise awareness and educate consumes about the dangers of fraud and to help prevent the occurrence of frauds and ensure confidence in the marketplace, the Forum organizes a month-long education campaign each March to improve consumers' awareness and understanding about the dangers of fraud.

To gauge Canadians' awareness and understanding, the Strategic Counsel conducted a post-Fraud Prevention Month survey in 2006 of one thousand Canadians, aged 18 years and older. Some of the results were:

- **17%** were the victim of identity theft
- **31%** were the victim of mass marketing fraud (by phone, mail or email)
- **41%** were motivated to change their behaviour based on the anti-fraud messages
- **53%** said public education is the most effective approach to combating mass marketing fraud and identity theft in Canada

American Collaborations

7.6. Anti-Phishing Working Group (APWG)

Origin and Membership

The APWG is a global industry association that focused on eliminating the identity theft and fraud that result from the growing problem of phishing and e-mail spoofing. The working group was founded by Tumbleweed Communications and a number of financial service institutions and e-commerce providers. The APWG held its first meeting back in 2003 in San Francisco, California.

Membership for the APWG is open to qualified financial institutions, online retailers, internet service providers (ISPs), the law enforcement community, security solutions providers, and research institutions. There are currently over 1,600 organizations participating in the APWG and more than 2,600 members worldwide as of November 2007. Eight of the top 10 banks and four of the top five ISPs in the United States are members of the APWG.

APWG members pay annual fees to financially support the organization. Membership dues cover the general expenses of the organization, including websites, mailings and communications, portions of the APWG meetings and more. There are several types of membership, including special (non-profit, academic, government, law enforcement and NGO), basic (annual fee of $50), individual ($500), corporate ($5000), sponsoring vendor ($7,500), premium ($15,000) and sustaining ($50,000).

Organization and Management

APWG is a voluntary organization that brings together groups from diverse fields to work towards eliminating Internet scams and fraud.

Scope and Objectives

The objective of APWG is to eliminate the identity theft and fraud that result from the growing problem of phishing and email spoofing and the spread of crimeware that automatically mines consumers' personal data from their computers.

The APWG also aims to offer resources, technology, vision, and expertise to facilitate the rapid deployment of a solution to e-mail phishing scams. It provides a forum for the public, business and law enforcement agencies to discuss phishing issues, trials and evaluations of potential technology solutions, and access to a centralized repository of phishing attacks

Collaborative Activities

On December 12, 2003, the APWG published a white paper titled "Proposed Solutions to Address the Threat of E-mail Spoofing Scams" that provides a brief overview of e-mail spoofing scams and offers four solutions. The recommended solutions are stronger web site authentication, mail server authentication, digitally signed e-mail with desktop verification and digitally signed e-mail with gateway verification.

The APWG publishes phishing activity trends reports in which it analyzes phishing attacks reported to the organization via its website or email. It also offers a news service called APWG eCrime Newswire, where the latest news on anti-phishing activities and efforts are posted on the website and updated four times a day. That way, businesses, law enforcement agencies and the general public are informed of what is happening out there.

Other than doing work on its own, the working group also collaborates with a handful of other organizations.

The APWG and the Financial Services Technology Consortium (FSTC) have agreed to work together to identify and evaluate solutions to phishing. The FSTC is a consortium of leading North American-based banks and other financial institutions that sponsors collaborative technology development.

Together with the US Department of Homeland Security and SRI International Identity Theft Technology Council, the APWG prepared a report in October 2006 on "crimeware," a piece of software that performs illegal actions unanticipated by a user running the software. The distributor of the software then gains financial benefits as a result of that.

In addition, the APWG has worked with the Messaging Anti-Abuse Working Group (MAAWG) to develop a set of best practices to combat phishing, which is a major cause of online idenitiy theft and fraud. The recommendations will help ISPs and mailbox providers better guard their infrastructures and filter traffic traversing their networks. APWG's Chairman Dave Jevans said that these best practice recommendations are a result of collaboration between ISPs, security companies and government agencies. He also said that "this kind of ongoing collaboration is crucial, as phishing and crimeware are constantly evolving security threat." The joint efforts between the two groups and their respective technical and governance committees began in the fall of 2005. The final document was reviewed and approved at a co-located June 2006 meeting of the APWG and MAAWG in Brussels.

7.7. Coalition on Online Identity Theft

Origin and Membership

The Coalition on Online Identity Theft was founded by a group of leading financial services, information technology and ecommerce companies in September 2003. The coalition was organized by the Information Technology Association of America (ITAA), which represents companies from the information technology industry in the United States. Among the founding members of this organization were Microsoft Corp., RSA Security Inc., eBay Inc., Amazon.com Inc., VeriSign Inc., Zone Labs Inc., Cyveillance Inc and several other technology companies.

Organization and Management

The ITAA serves as the secretariat of the coalition, leading member organizations to fight against online fraudulent activities. There were efforts dedicated to combating online identity fraud before the coalition was formed, and the establishment of the coalition helped formalize such efforts[2].

Scope and Objectives

The Coalition aims to reach out to other companies and organizations that are interested in seeking educational, legal and technical solutions to protect consumers and companies from online fraud and safeguard the future of e-business. It also coordinates its efforts with the Federal Trade Commission, the Department of Justice and other federal, state and local law enforcement agencies. Consumers can turn to the coalition to learn more combating online fraud[3].

Collaborative Activities

---

[2] http://query.nytimes.com/gst/fullpage.html?res=9C0DE7D8163BF93BA3575AC0A9659C8B63
[3] http://query.nytimes.com/gst/fullpage.html?res=9C0DE7D8163BF93BA3575AC0A9659C8B63

The coalition works primarily on four main areas in combating online fraud. It expands public education campaigns against online identity theft to protect consumers, as well as helping promote technology and self-help approaches for preventing and dealing with online identity theft. The coalition also shares documents and non-personal information regarding emerging trends of fraudulent activities to stay on top of things. Working with government agencies allows the coalition to help protect consumers and businesses and ensure the effective enforcement of rules and regulations against online fraud.

7.8. Financial Services Information Sharing and Analysis Center (FS/ISAC)

Origin and Membership

The FS/ISAC works under the auspices of the President's Commission on Critical Infrastructure Protection[4]. It is one of the fourteen ISACs created as a result of US Presidential Decision Directive 63 (PDD-63) in 1998. The directive requested the public and private sectors to create a partnership to share information about physical and cyber threats, vulnerabilities, and events to help protect the critical infrastructure of the United States. PDD-63 was updated in 2003 with Homeland Security Presidential Directive/HSPD-7 to reaffirm the partnership mission. Today there are ISACs for 14 critical infrastructures, such as Financial Services, Electric, Energy and Surface Transportation. The FS/ISAC was launched in 1999 to help members prepare for Y2K and establish an anonymous information sharing capability within the financial services industry.

The FS/ISAC uses multiple tiers of membership. Firms eligible for membership include the firms in the financial services sector: banking firms and credit unions, securities firms, insurance companies, credit card companies, mortgage banking companies, financial services sector utilities, financial services service bureaus, and appropriate industry associations. The present members make up the majority of banking assets and securities transactions in the United States. The membership requires fees to be paid. Pricing varies depending on the type of membership: Basic Participant (no fee), Core Membership (annual fee: $750); Standard Membership (annual fee: $5,000); Founding Membership, and Affiliate Membership (annual fee: $25,000). Names of member firm are not released without the members' permission and no data is ever attributed to an individual member without that member's permission.

FS/ISAC membership is recommended by the U.S. Department of the Treasury, the Office of the Controller of Currency, the Department of Homeland Security, the United States Secret Service, and the Financial Services Sector Coordinating Council. In fact, both Treasury and DHS rely on the FS/ISAC to disseminate critical information to the financial services sector in times of crisis.

Scope and Objectives

The FS/ISAC's objective is to disseminate trusted and timely information to increase sector wide knowledge about physical and cyber security risks faced by the financial services sector. The goal is to deliver urgent and crisis alerts to 99% of the sector by 2006.

Organization and Management

---

[4] The President's Commission on Critical Infrastructure Protection was created on July 15, 1996, by Executive Order 13010 to bring the public and private sectors together to assess and develop strategies to address infrastructure vulnerabilities. The banking and finance sector was identified as one of eight critical infrastructures requiring review and assurance strategies.

The FS/ISAC is a private partnership of major banks, brokerages, insurance companies, and utilities and is managed by a board of managers elected by the FS/ISAC membership. The U.S. Department of Treasury is the official government sponsor and has provided substantial project funding to meet the requirements of the FS/ISAC. The FS/ISAC Board of Directors determines member eligibility, enforces member eligibility verification through trusted third parties, and oversees the operation of the FS/ISAC. The Board of Directors is elected by members to serve a three-year term. The FS/ISAC is for the private sector and is managed by the private sector and funded by members for all operations.

Collaborative Activities

The FS/ISAC gathers threat, vulnerability, and risk information about cyber and physical security risks faced by the financial services sector. Sources of information include commercial companies who gather this type of information, government agencies, law enforcement, CERTs, academic sources, and other trusted sources. After analysis by industry experts, delivering urgent and crisis alerts are delivered to participants based on their level of service. Members may create a profile on the FS/ISAC website to identify specific areas of interest or receive all alerts. For both physical and cyber events, alerts contain a description of the threat or vulnerability, its severity, and recommendations for solutions.

Members of the FS/ISAC receive trusted and timely expert information that increases sector-wide knowledge of physical and cyber security threats. Based on level of service, FS/ISAC members take advantage of a host of important benefits, including early notification of security threats and attacks, anonymous information sharing across the financial services industry, regularly scheduled member meetings, and bi-weekly conference calls.

Examples of services for members include:

- Access credentials for up to 10 of a given firm's employees
- Access to the FS/ISAC restricted Web site except for member submissions
- Delivery of normal, urgent and crisis alerts, except for member submissions
- Delivery of DHS and Treasury alerts in times of crisis
- Customized alert profile developed by a given member firm
- Multimedia alert delivery capabilities through CINS
- 24/7 access to a fully staffed FS/ISAC watch desk
- Participation in crisis-management conference calls
- Access to customized analysis
- Attendance at FS/ISAC member meetings
- Ability to submit both anonymous and attributable information to FS/ISAC membership
- Information sharing best practices

The following two examples illustrate the nature of alerts provided by FS/ISAC and their benefits. The first example is *Russian Keylogger in July 200, an.*email scam on retail financial services customers. Website installed keystroke monitoring software on the victim's computer to capture account information. 16,000 keystroke logs of consumer information were found on dump-site and provided to FS/ISAC. FS/ISAC provided list of compromised accounts to member institutions. Accounts were legitimate and were locked by the bank to protect against fraud. Victim account owners were notified by bank. Worked closely with ISC, DHS, USSS and FBI on investigation. As a result of FS/ISAC banks were saved from direct financial losses. Another

example is *Keylogger in March 2005*. Massive DDoS paralized ISP. Investigation discovered a server with a large file of apparent bank account information. ISP contacted the FS/ISAC and delivered the file. FS/ISAC analysis found 19,000 keystroke logs on customer bank account information from more than 20 institutions. Accounts were legitimate and were locked by the banks to protect against fraud. Victim account owners were notified by bank.

No government agency of any type or law enforcement agency has any access to member-submitted events. The FS/ISAC has and will provide the appropriate government departments with summary sanitized data based on a need-to-know basis. The current FS/ISAC database has thousands of threats, vulnerabilities, and events dating back to 1999. The FS/ISAC analysts use the database to establish trends and do research and investigations. Only members with the appropriate credentials have access to the database. Basic Participants have no access to the database, Core Members have limited access to the database, and Standard Members and higher have access to all features and benefits of the database. Over time the FS/ISAC is expecting to offer advanced analytics to members to study multiple firm IDS data and other programs to predict the likelihood of events.

7.9. Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC)

Origin and Membership

Established in June 2002, the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC) consists of more than 30 private-sector firms and financial trade associations. The FSSCC was founded by the private sector and it gets recognition from the U.S. Treasury.

The FSSCC now have 34 members, and they include the American Insurance Association, the Investment Company Institute and New York Border of Trade and many other organizations from the financial services sector.

Organization and Management

The FSSCC works with the U.S. Department of Treasury, which is directly responsible for infrastructure protection and homeland security efforts for the financial services sector. It also works under the guidance of the Department for Homeland Security.

The Council is chaired by George S. Hender with Shawn Johnson being newly appointed as vice-president.

Scope and Objectives

The FSSCC's scope is on critical infrastructure protection and homeland security (CIP/HLS). Its goal is to foster and facilitate the coordination in the financial services sector to organize voluntary activities and initiatives to help improve CIP/HLS.

More specifically, the Council aims to provide broad industry representation for CIP/HLS and related matters for the financial services sector and for voluntary sector-wide partnership efforts, as well as identify voluntary efforts where improvements in coordination can foster sector preparedness for CIP/HLS. It also helps identify barriers to and recommend initiatives to improve sector-wide voluntary and timely sharing/ dissemination of CIP/HLS knowledge and critical

information. More importantly, the FSSCC works to improve sector awareness of CIP/HLS issues, available information, sector activities/initiatives and opportunities for improved coordination[5]

Collaborative Activities

In terms of collaboration, the FSSCC represents organizations in the financial services sector and works with the public sector on their behalf.

7.10. Financial Services Technology Consortium (FSTC)

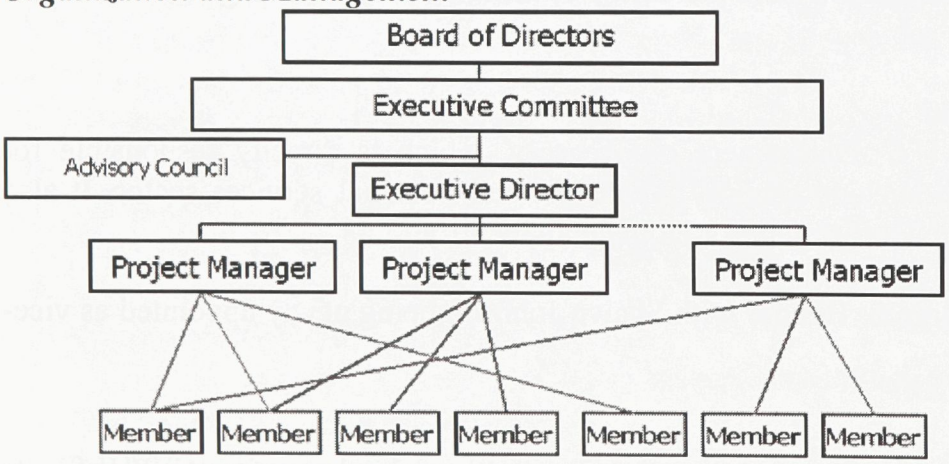
Origin and Membership

The Financial Services Technology Consortium was created in 1993 by a group of leading organizations in the financial services sector in the United States. The FSTC aims to unite individuals in the industry to work collaboratively in solving problems and challenges they face, as well as to work towards the next-generation of financial services technologies.

The FSTC currently has more than 100 members from financial institutions, technology companies, academic institutions and government agencies. Any organization interested in contributing to the technological development of the financial services industry is encouraged to become a member of the FSTC. Members can participate in the FSTC's Advisory Committee, where they can play an active role in proposing and sponsoring research projects, participate in different special interest groups and work with various standing committees of the FSTC.

There are three types of membership. Companies can choose to become Principal, Associate or Advisory Members based on the nature of their businesses. Members pay dues to financially support the Consortium.

Organization and Management



The FSTC is overseen by a Board of Directors, to which the Executive Committee reports. There is an Advisory Council, which consists of four Standing Committees. They are the Business Continuity Standing Committee, which focuses on financial services continuity and risk management; the Security and Infrastructure Standing Committee, which helps members of the FSTC to anticipate and cope with problems and challenges they may face; the Payments and Check Imaging Standing Committee, which handles issues of the payment trends; and the

[5] https://www.fsscc.org/about/default.jsp

Enterprise Architecture Standing Committee, which helps with networking among members to share best practices on enterprise architecture and technology.

Scope and Objectives

The FSTC conducts noncompetitive collaborative research and develops inter-bank technical projects that impact the financial services industry. Its mission is to assist its members in collaborating on the technical and business aspects of technologies. That helps bring innovations to the industry and to customers.

Collaborative Activities

The FSTC is actively involved in research pertinent to technologies employed by the financial services sector.

It publishes a series of reports, together with Meridien Research, on a bi-monthly basis to investigate different topics that are of interest to its members. Bi-annual member meetings are held to discuss emerging technologies in the field and members can take the opportunity to network with one another.

Recently, the FSTC has been working on a project that deals with sharing real-time information on fraud cases and patterns. Such information sharing will help organizations in the financial services sector to better protect themselves against fraudulent activities and mitigate the impact of these activities if they do happen. This research also looks at how the data gathering and disseminating process can be integrated into a financial services institution's operations and its customer processes.

7.11. Identity Theft Assistance Center (ITAC)

Origin and Membership

The Identity Theft Assistance Center (ITAC) is a cooperative initiative founded by the financial services industry in the United States to provide a free victim assistance service for customers of member companies. The ITAC is run by the Identity Theft Assistance Corporation, a not-for-profit membership corporation based in Washington, DC, sponsored by The Financial Services Roundtable[6] and BITS[7].

The ITAC was formed in September 2003, and it began operation in August 2004[8]. The objective of this non-profit industry consortium was to pilot the Identity Theft Assistance Center. The ITAC

---

[6] The Financial Services Roundtable represents 100 of the largest integrated financial service companies providing banking, insurance, and investment products and services to the U.S. consumer. It is a public policy group that promotes the interests of member companies in legislative, regulatory and judicial forums.

[7] BITS is a nonprofit, CEO-driven industry consortium whose members are 100 of the largest financial institutions in the United States. It was created in 1996 to foster the growth and development of electronic financial services and e-commerce for the benefit of financial institutions and their customers. BITS facilitates cooperation between the financial services industry and other sectors of the nation's critical infrastructure, government organizations, technology providers and third-party service providers. BITS shares its membership with its sister organization, The Financial Services Roundtable.

[8] http://pdfdownload.randomlypoked.com/pdf2html.php?url=http%3A%2F%2Fwww.identitytheftassistance.org%2Fresources%2FFact%20Sheet_final.pdf&images=yes "Fact Sheet"

was initially founded as a one-year pilot, but given its success, the board of directors voted to permanently establish the ITAC as a service to customers of the ITAC member companies.

Originally membership in the ITAC was open only to financial services companies, but in October 2005 it was opened also to companies operating in other industries frequently targeted by identity thieves, including retailers and telecommunications companies. At the moment, eligible companies include financial services companies, retailers and utilities. To join the ITAC, a company must have an ongoing business relationship with individual consumers, and be able to authenticate the consumer's identity and verify the existence of identity theft.

The ITAC builds on the "Fraud Reduction Guidelines: Strategies for Identity Theft Prevention and Victim Assistance," announced by the Roundtable and BITS in July 2003. The guidelines provide for (1) a single point of contact at financial service companies to whom victims can report cases of identity theft, and (2) the use of a uniform affidavit to record information about the fraud.

Members have access to a comprehensive range of fraud detection and prevention services through ITAC including customer notification and credit monitoring in the event of an information security breach. They are eligible for ITAC Risk Management Services. These services can serve in lieu of, or as an extension of, existing fraud operations, and include information breach mitigation, credit monitoring, expanded victim's assistance and ITAC database queries.

Scopes and Objectives

The ITAC works with its members who come from the financial sectors and other industries that are often targeted by identity theft perpetrators as well as individual consumers. Members of the ITAC state that fraud reduction and victim assistance are not a competitive issue. As a result, the ITAC's mission is to assist victims of identity theft in correcting the damage caused by the crime; help member companies detect and prevent identity theft from occurring; share information with the Federal Trade Commission and with law enforcement agencies to help them investigate, prosecute and convict criminals; and analyze the identity theft data.

According to the ITAC's definition, identity theft is the creation of a fraudulent new account in the consumer's name or the takeover of an existing legitimate account. Unlike the more common kinds of financial fraud, such as unauthorized use of a credit card, which typically can be resolved quickly, identity theft often involves multiple companies and can be difficult to resolve.

Organization and Management

ITAC is run by the Identity Theft Assistance Corporation, a not-for-profit membership corporation based in Washington, DC. The Identity Theft Assistance Corporation is governed by a Board of Directors elected by the members.

Collaborative Activities

- ***Victim Assistance Service***

The ITAC serves individuals who live in the United States and who have an account relationship with a member for personal, family or household use. The process begins at an individual ITAC member company. If a consumer suspects a problem with an account - for example, funds are missing from an account - the consumer contacts the company that holds that account. Next, the

customer works with the member to resolve any issues at that particular company. The member gathers information about the event using the Uniform Affidavit. Information in the Uniform Affidavit can be shared with departments and business units within the company and, with the customer's consent, other companies. This sharing reduces the burden on the victim who otherwise would have to tell his or her story repeatedly and complete multiple forms. If the member determines the problem involves identity theft, it offers the victim use of ITAC free of charge. With the victim's consent, the contents of the Uniform Affidavit is transmitted to the ITAC. ITAC then obtains the victim's credit report and reviews the file with the victim to see if there is evidence of accounts that have been taken over or fraudulent accounts that have been created. ITAC notifies the affected creditors (whether they are members of ITAC or non-members) and places a fraud alert with the credit bureaus if the victim has not already done so. At the beginning of the process, consumers are informed about ITAC's partnership with law enforcement and asked to consent to the sharing of their information with law enforcement in order to help them determine investigate and prosecute identity theft.
Between August 2004 and May 2006 ITAC has helped more than 6,000 consumers restore their financial identities (Wallace, 2006)

Important feature of ITAC is the Uniform Affidavit. For the victim, one of the most frustrating aspects of identity theft is having to complete a different affidavit at each company where suspicious activity occurred. All members of ITAC have agreed to use the same form and to share the contents of the Uniform Affidavit among themselves. The ITAC Uniform Affidavit replaces the proprietary fraud forms that many companies use today. The Uniform Affidavit allows different departments of the same company to share information and, with the consumer's consent, it can be shared with other companies. This means the victim will give details about the incident once instead of repeating it to multiple companies

- ***Data Sharing Agreements***

In 2005, the ITAC signed a data sharing agreement with Federal Trade Commission and since then, has forwarded its data on identity theft cases to the Consumer Sentinel Database run by the Federal Trade Commission. The ITAC also works with the FBI and the Secret Service who have 24-hour-a-day online access to the ITAC data via the FTC's database. In 2005, the ITAC also signed a data sharing agreement with the U.S. Postal Inspection Service under which the ITAC provides, on a weekly basis, information about the victim and the identity theft incident which is next added to the Financial Crime Database. The database is used by postal inspectors all over the country. In May 2006, the ITAC signed a data sharing agreement with the regional Identity Theft Network which was developed and is led by the US Attorney – EDPA. This project includes federal agencies (U.S. Postal Inspection Service, FBI, Secret Service, DHS and State Department), as well as the Pennsylvania Attorney General and District Attorneys in Philadelphia County and surrounding counties.

7.12. Identity Theft Resource Center (ITRC)

Origin and Membership

The Identify Theft Resource Centre (ITRC) is a national non-profit organization that focuses exclusively on identity theft. Originally named VOICES (Victims of Crimes Extended Services), the ITRC was founded in December 1999 by Linda and Jay Foley. While its national office is

based in San Diego, CA, the ITRC has representatives working with its program throughout the United States.

Organization and Management

Since its inception in 1999, the ITRC has gone through continuous organizational expansion and growth. The center has created a full strategic plan, mission statement and updated company structure. Its structure includes a team management process, improved communications efficiency, and internal checks and balances needed to grow the center in
all aspects.

ITRC has audited financials (2004) and reviewed financials (2005). In addition, it has critical financial controls in place, as well as real time bookkeeping and asset management. Furthermore, critical server, computer, network and software systems have been installed, standardized, and stabilized, giving the company enhanced ability to handle current and anticipated growth in calls, data tracking, and reporting. The 3,300-square foot San Diego facility houses administrative offices, call center, and server/communications center.

The ITRC management team meets formally at least once per week and approves all decisions that affect the agency. This management method provides a thoughtful decision process that produces consistent and reliable company policies, both with the ITRC staff and with entities outside the agency.

Scope and Objectives

The ITRC's mission is to provide best in class victim assistance at no charge to consumers throughout the United States, to educate consumers, corporations, government agencies and other organizations on best practices for fraud and identity theft detection, reduction and mitigation, as well as to provide enterprise consulting and outsourced services related to information breach, fraud and identity theft.

The ITRC fundamentally believes that both consumers and businesses are victims of identity theft and fraud and that prevention and reduction of identity theft will require education and cooperation between consumers, businesses, law enforcement agencies, and legislators. The resource centre also believes that support and education of businesses has a strong positive impact on the restoration of victims' lives, and the prevention of further identity theft.

Meanwhile, the ITRC has consciously avoided legal advocacy as a method of forwarding its mission.

Collaborative Activities

The ITRC works with law enforcement agencies, businesses and consumers in combating identity fraud.

It works closely with the U.S. Attorney General and various national law enforcement agencies to provide them with resources in combating identity theft, as well as with the Office of Victims of Crime on various programs.

The ITRC provides victim assistance training through the Office for Victims of Crime Training and Technical Assistance Center (OVC-TTAC) program. It also serves as advisor to many other

organizations including the San Diego District Attorney, San Diego Police Department, the San Diego County Sheriff's Department, the FBI Cyber Crimes Division, the San Diego CATCH team, the AUDIT program for CAUSE, IPSA, and the National Association of Attorneys General.

7.13. InfraGard

Origin and Membership

InfraGard is a Federal Bureau of Investigation (FBI) program is an information sharing and analysis effort serving the interests and combing the knowledge base of a wide range of members. It began in the Cleveland Field Office in 1996 and was later expanded to other FBI Field Offices. It is a partnership between the FBI and the private sector. It is an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to protect critical information systems and prevent hostile acts against the United States. InfraGard Chapters are geographically linked with FBI Field Office territories.

Each InfraGard Chapter has an FBI Special Agent Coordinator assigned to it, and the FBI Coordinator works closely with Supervisory Special Agent Program Managers in the Cyber Division at FBI Headquarters in Washington, D.C.

While under the direction of NIPC, the focus of InfraGard was cyber infrastructure protection. After September 11, 2001 NIPC expanded its efforts to include physical as well as cyber threats to critical infrastructures. InfraGard's mission expanded accordingly.

In March 2003, NIPC was transferred to the Department of Homeland Security (DHS), which now has responsibility for Critical Infrastructure Protection (CIP) matters. The FBI retained InfraGard as an FBI sponsored program, and will work with DHS in support of its CIP mission, facilitate InfraGard's continuing role in CIP activities, and further develop InfraGard's ability to support the FBI's investigative mission, especially as it pertains to counterterrorism and cyber crimes.

In terms of membership, since InfraGard is an organization dedicated to the protection of the United States and the American people, all applicants undergo a background check performed by the FBI in order to maintain a level of trust within the membership. For this reason InfraGard membership is currently limited to United States citizens. Applications are then screened according to a defined criteria and then passed to the local chapter for final acceptance (individual chapters may have more strict criteria).

Organization and Management

InfraGard members are represented nationally by an elected board of seven representatives called the InfraGard Board of Directors. Elections are held annually at the InfraGard National Congress for voluntary two-year terms. The Board is responsible for representing the membership in the partnership with the FBI. They conduct weekly conference calls to address a variety of issues that face the organization. Board members travel to various chapter activities and attend conferences promoting InfraGard and other issues pertinent to the program.

The Board has established several committees to address issues such as membership, incorporation, and partnerships with other private sector associations/organizations. Special Interest Groups (SIGs) have also been established to meet the challenges America faces in protecting against criminal, terrorist, and intelligence threats. One such SIG involves InfraGard, the National Institute of Standards and Technology (NIST), the Small Business Administration, and the FBI.

Scope and Objectives

The goal of InfraGard is to "improve and extend information sharing between private industry and the government, particularly the FBI, when it comes to critical national infrastructures". Critical infrastructures include these physical and cyber-based systems essential to the minimum operations of the economy and government.

Another goal of InfraGard is to promote ongoing dialogue and timely communication between members and the FBI. InfraGard members gain access to information that enables them to protect their assets and in turn give information to government that facilitates its responsibilities to prevent and address terrorism and other crimes.

The relationship supports information sharing at national and local levels and its objectives are as follows:

- Increase the level of information and reporting between InfraGard members and the FBI on matters related to counterterrorism, cyber crime and other major crime programs.
- Increase interaction and information sharing among InfraGard members and the FBI regarding threats to the critical infrastructures, vulnerabilities, and interdependencies.
- Provide members value-added threat advisories, alerts, and warnings.
- Promote effective liaison with local, state and federal agencies, to include the Department of Homeland Security.
- Provide members a forum for education and training on counterterrorism, counterintelligence cyber crime and other matters relevant to informed reporting of potential crimes and attacks on the nation and U.S. interests.

Collaborative Activities

Infragard is an information-sharing and analysis resource serving the interests and combining the knowledge base of a wide range of members. Members include businesses, academic institutions, state and local law enforcement agencies, and others dedicated to sharing information and intelligence to prevent hostile acts against the United States. Each Infragard Chapter has an FBI special agent coordinator assigned to it, coordinating with the Cyber Division at FBI headquarters. Government organizations and their representatives are eligible for Infragard membership, and several FDIC regional offices participate. Infragard chapters are located across the United States and are linked with FBI field office territories. InfraGard provides formal and informal channels for the exchange of information about infrastructure threats and vulnerabilities.

- ***Local Chapter Activities***

Each FBI Field Office has a Special Agent Coordinator who gathers interested companies of various sizes from all industries to form a chapter. Any company can join InfraGard. Local executive boards govern and share information within the membership. Chapters hold regular meetings to discuss issues, threats and other matters that impact their companies. Speakers from public and private agencies and the law enforcement communities are invited. The local chapters

may also offer training and education initiatives, a local newsletter, a Contingency Plan for using alternative systems in the event of a successful large scale attack on the information infrastructure

7.14. Internet Crime Complaint Center (IC3)

Origin and Membership

The Internet Crime Complaint Center (IC3) is an alliance between the National White Collar Crime Center (NW3C) and the Federal Bureau of Investigation (FBI). IC3 began operation on May 8, 2000 to address fraud committed over the Internet. Originally known as the Internet Fraud Complaint Center (IFCC), the IC3 was renamed in December 2003 to better reflect its growing scope that encompasses different, often overlapping, Internet crimes and to minimize the need for consumers to distinguish "Internet fraud" from other crimes.

Organization and Management

The IC3 is a partnership between the FBI and the NW3C.

Scope and Objective

IC3's mission is "to serve as a vehicle to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cyber crime[9]". It was created to serve as a means to receive Internet related criminal complaints and to further research, develop, and refer the criminal complaints to federal, state, local, or international law enforcement and/or regulatory agencies for any investigation they deem to be appropriate. The IC3 was intended to serve the broader law enforcement community including federal, as well as state, local, and international agencies, which are combating Internet crime and, in many cases, participating in Cyber Crime Task Forces.

Collaborative Activities

The Internet Crime Complaint Center conducts a number of different activities, which include providing a convenient central point for Internet crime (including identity theft and fraud) victims to report the possible crime and to alert an appropriate agency on-line at www.ic3.gov. The Centre also serves as a central repository for complaints related to Internet crime and the information is available to law enforcement and regulatory agencies. Once complaints are received, the IC3 will refer the fraudulent activity identified on the Internet to the appropriate federal, state, local, or international law enforcement or regulatory agencies for appropriate actions to be taken. Every complaint that is referred is sent to one or more law enforcement or regulatory agencies that have jurisdiction over the matter. This way IC3 aids in preventive and investigative efforts. On top of that, the IC3 analyzes Internet crime complaints in identifying patterns and current trends in Internet crime, as well as helping the development of law enforcement training to address identified Internet crime problems, and facilitating networking and data sharing among law enforcement and regulatory agencies

Supplemental to partnering with law enforcement and regulatory agencies, IC3 has established numerous alliances with industry in order to leverage its partners' intelligence and subject matter expert resources. A number of agencies have collaborated with the IC3 and provided added value to its work in the form of staffing, recommendations, and other support. Among IC3's partners are the Business Software Alliance (BSA), the Direct Marketing Association (DMA),

[9] http://www.ic3.gov/about/

EBay/PAYPAL, the Federal Trade Commission (FTC), the financial services industry, the Merchant Risk Council (MRC), Microsoft, the National Cyber-Forensics & Training Alliance (NCFTA), the Nigerian Economic and Financial Crimes Commission (EFCC), Reporting Economic Crime Online (RECOL), and United States Postal Inspection Service (USPIS).

Together, The IC3 and its partners have launched a public website (www.lookstoogoodtobetrue.com) to educate the public on online fraudulent activities so that they do not become a victim.

The IC3 also shares its Internet fraud and identity theft complaint data with the Federal Trade Commission (FTC) for inclusion in the Identity Theft Data Clearinghouse. It cooperates with the Financial Institution Fraud Unit (FIFU) and members of the Financial Services Roundtable (FSR) to ensure it is receiving, interpreting, and leveraging financial institution data in the most effective manner.

7.15. Merchant Risk Council (MRC)

Origin and Membership

The Merchant Risk Council (MRC) was formed in 2002, as the Merchant Fraud Squad collaborated with the Internet Fraud Roundtable. The Merchant Fraud Squad was set up in September 2000 by American Express, ClearCommerce and Expedia with the goal to educate online businesses on how they can prevent fraud. Founded by Hewlett-Packard and ClearCommerce in 2001, the Internet Fraud Roundtable brings large industry retailers together twice a year in person to share best anti-fraud practices among them, and there are monthly conference calls among these retailers.

Three levels of membership are offered by the Merchant Risk Council. Companies can choose to become Platinum Merchant Members, Silver Members or Law Enforcement Members. Companies enjoy access to different information according to the level of membership they get involved in, and they also pay different amounts of fees based on their membership status. For example, in order to become Platinum Merchant Members, companies have to be involved in non-face-to-face transactions and have a focus on e-commerce. Only are Platinum Merchant Members allowed to sit on the Board, although Silver Members can participate in committees of the MRC.

Companies can also choose to become sponsor members, ranging from Primer to Signature to Elite members, if they are willing to pay an annual between $15,000 and $40,000.

Organization and Management

The MRC consists of a Board of Directors and there are a number of Board Advisors, as well as different committees.

Scope and Objectives

The MRC strives to foster a safe environment and improve operational relationships between merchants and all constituents. It goal is to realize the promise of e-commerce and to make the Internet a place where individuals prefer when engaging in shopping and selling activities.

Collaborative Activities

Companies can subscribe to the MRC's website to gain access to the most up-dated information on technological products that help combat fraud. Subscribers also have access to analyses of different fraud prevention tools. These subscribers together share the common goal of protecting and encouraging the thriving online commerce industry by establishing best practices for cyber-fraud prevention.

The MRC also works with deferral and local enforcement agencies such as the Federal Bureau of Investigation, Secret Service, the U.S. Department of Justice, and the U.S. Postal Inspectors to help catch and prosecute cyber criminals.

Every year, it hosts an Internet Fraud Prevention Conference, where experts from major Internet retails, credit card associations and law enforcement agencies get together and discuss the latest development in fraud prevention.

7.16. PCI Security Standards Council

Origin and Membership

The PCI Security Standards Council is an open global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection.

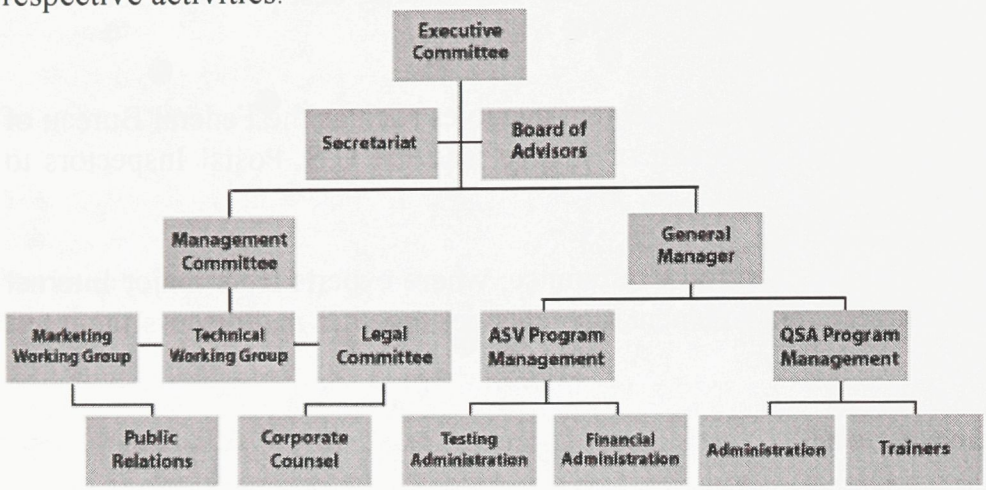
A Limited Liability Corporation (LLC) chartered in Delaware, USA, the PCI Security Standards Council was founded by American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International on September 7, 2006. All five payment brands share equally in the council's governance, have equal input to the PCI Security Standards Council and share responsibility for carrying out the work of the organization. Other industry stakeholders are encouraged to join the group and review proposed additions or modifications to the standards.
The Council is an independent organization designed to manage the ongoing evolution of the Payment Card Industry (PCI) Data Security Standard, which focuses on improving payment account security throughout the transaction process. By establishing the independent Council to manage the PCI Data Security Standard for the payments industry, the founding members intent to develop a system that is more accessible and efficient for all stakeholders including merchants, processors, point-of-sale (POS) vendors and financial institutions.

The PCI Security Standards Council invites all parties with a role to play in securing payment account data - including merchants, payment devices and services vendors, processors, financial institution and others - to participate in this organization. Participating organizations will be able to recommend changes, provide input on future initiatives, have access to and the ability to comment on drafts of potential changes to security standards in advance, as well as influence the organization's overall direction. In addition, participating organizations will be able to elect or serve as a member of the PCI Security Standards Council's Board of Advisors. The PCI Security Standards Council will serve as an advisory group and manage the underlying PCI security standards, and each payment card brand will remain responsible for its own compliance programs.

Organization and Management

The PCI Security Standards Council is led by a policy-setting Executive Committee, composed of representatives from the founding payment brands. Operational decisions are made by a

Management Committee, also from the payment brands. An Advisory Board, drawn from Participating Organizations, provides input to the organization and feedback on the evolution of the PCI Data Security Standard. A Marketing Working Group, Technical Working Group, and a Legal Committee, whose participants are drawn from the payment brands, deal with their respective activities.



Scope and Objectives

The PCI Security Standards Council's mission is to enhance payment account data security by fostering broad adoption of the PCI Security Standards.

The PCI Security Standards Council owns, develops, maintains and distributes the PCI Data Security Standard (DSS). To improve compliance and reduce costs and lead times for implementation of the standard, the PCI Security Standards Council also defines qualifications for Qualified Security Assessors (QSAs) and Approved Scanning Vendors (ASVs); and trains, tests and certifies QSAs and ASVs.

The PCI Security Standards Council will maintain and evolve the PCI Data Security Standard, while working to promote its broad industry adoption, and while providing the tools needed for compliance with the standard. These tools include critical documents such as audit guidelines, scanning vendor requirements, and, in a few months, a self assessment questionnaire. These functions are as important as the promulgation of the standard itself.

All of the five founding members have agreed to incorporate the PCI DSS as the technical requirements of each of their data security compliance programs. Each founding member also recognizes the QSAs and ASVs certified by the PCI Security Standards Council as being qualified to validate compliance to the PCI DSS.

Collaborative Activities

Specifically, the PCI Security Standards Council develops and maintains a global, industry-wide technical data security standard for the protection of accountholder account information. It works to reduce costs and lead times for Data Security Standard implementation and compliance by establishing common technical standards and audit procedures for use by all payment brands. In addition, the Council provides a list of globally available, qualified security solution providers via its Web site to help the industry achieve compliance. It leads training, education, and a streamlined process for certifying Qualified Security Assessors (QSAs) and Approved Scanning Vendors (ASVs), providing a single source of approval recognized by all five founding members, as well as providing a transparent forum in which all stakeholders can provide input into the ongoing development, enhancement and dissemination of data security standards.

7.17. The President's Task Force on Identity Theft

Origin and Membership
The President's Task Force on Identity Theft was formed in May, 2006. It was established because U.S. President George W. Bush recognized the threat identity theft had posed to Americans and thus saw a need to improve collaboration at the federal level to combat this problem.

The Task Force has 17 members, and they are representatives from 17 government agencies. They are the Attorney General, the Federal Trade Commission, the Department of Treasury, the Department of Commerce, the Department of Health and Human Services, the Department of Veterans Affairs, the Department of Homeland Security, the Office of Management and Budget, the United States Postal Service, the Federal Reserve System, the Office of Personnel Management, the Federal Deposit Insurance Corporation, the Securities and Exchange Commission, the National Credit Union Administration, the Social Security Administration, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision.

Organization and Management
In terms of management, the Task Force is chaired by the Attorney General and co-chaired by the chairperson of the Federal Trade Commission.

Scope and Objectives
The Task Force's goal is to craft a strategic plan to ensure that various government agencies work collaboratively in an effective and efficient manner in raising awareness of, preventing, detecting, and prosecuting identity theft.

Collaborative Activities
The Task Force works with enforcement agencies to investigate and prosecute individuals and parties who engage in identity theft crimes. It also surveys existing education efforts put out by government agencies and the private sector, as well as collaborating with federal agencies to strengthen the safeguarding of personal data.

International Collaborations

7.18. Canada-United States Working Group on Cross-Border Mass-Marketing Fraud

Origin and Membership
Since 1997, the Bi-national Working Group on Cross-Border Mass Marketing Fraud has provided an important mechanism for bi-national coordination and cooperation on a wide variety of mass marketing fraud issues. This Working Group has previously highlighted the problem of identity theft through its 2003 report on mass marketing fraud and its involvement in the preparation of joint public advisories on identity theft for consumers and retailers in both countries.

Organization and Management
This Working Group functions as a sub-group of the Canada-United States Cross-Border Crime Forum, and it reports to the Forum annually. The Cross-Border Crime Forum was created in 1997, and it is a joint effort between Public Safety and Emergency Preparedness Canada

(formerly as the Department of the Solicitor General of Canada), the Department of Justice Canada and the U.S. Department of Justice.

Scope and Objectives
The Working Group deals mostly with fraudulent activities in the mass marketing context. Its goal is to establish work relationships between the Canadian and the American governments to prevent and limit cross-border mass marketing fraud.

Collaborative Activities
In 2003, the Canada-United States Cross-Border Crime Forum determined that a threat assessment of identity theft and its impact on cross-border criminality needed to be conducted. Therefore, it directed the Canada-United States Working Group on Cross-Border Mass-Marketing Fraud, to prepare such an assessment. The assessment was a product of many agency and individual participants in the Working Group from the United States and Canada. It was prepared jointly by the United States Department of Justice (DOJ) and Public Safety and Emergency Preparedness Canada (PSEPC). The report was presented in October 2004 during Cross-Border Crime Forum and provided information and recommendations for policy makers, law enforcement, consumers and the private sector. This threat assessment report aims to define the nature, scope and impact of identity theft. It includes trends, statistics and an examination of the factors surrounding identity theft to increase understanding of the nature of the crime as well as current and potential responses to the problem.

7.19. Consumer Sentinel and Identity Theft Data Clearinghouse

Origin and Membership
Consumer Sentinel is an international, multi-agency joint project with members including more than 1,000 law enforcement agencies from Australia, Canada and the United States. It has been in operation since 1997.

The Identity Theft Data Clearinghouse is the federal government's database for tracking identity theft complaints. It was created pursuant to the Identity Theft and Assumption Deterrence Act of 1998, and began operation on November 1, 1999. The Federal Trade Commission (FTC) established the Identity Theft Toll-Free Hotline (1-877-IDTHEFT/438-4338) and the ID Theft Web site to provide identity theft victims with a central place in the federal government to report their problems and receive information. Complaints received from victims through the hotline or online complaint forms are entered into the Identity Theft Data Clearinghouse. Through data sharing agreements, the Clearinghouse includes not only consumer fraud and identity theft complaints received by the FTC, but also complaints from over 100 different U.S. and Canadian federal, state, and non-governmental organizations, including the Social Security Administration's Office of the Inspector General.

In terms of membership, only law enforcement agencies are allowed to join Consumer Sentinel. In order to do that, interested agencies have to sign a confidentiality agreement to show that they understand the access privileges they enjoy and the confidential rules to which the agencies have to adhere. Applications are then filled out by individual users within a participating law enforcement agency. Once they become members of Consumer Sentinel, law enforcement agencies have immediate and secure access to complaints made on identity theft, fraud and other matters of a similar nature.

Organization and Management

Both Consumer Sentinel and the Identity Theft Data Clearinghouse are managed by the Federal Trade Commission.

Scope and Objectives

Consumer Sentinel aims to serve as a one-stop, secure investigative tool and complaint database, on a separate restricted-access secure web site, that provides hundreds of law enforcement agencies immediate access to Internet cons, telemarketing scams and other consumer fraud-related complaints. It also gives consumers a way to voice their complaints about fraud to law enforcement officials worldwide.

Consumer Sentinel understands that sharing information makes law enforcement stronger and more effective, and it also works to enhances cross-border consumer education and prevention efforts.

The Clearinghouse's objective is to support its members in detecting trends in consumer fraud and identity theft.

Collaborative Activities

Consumer Sentinel has a database that is maintained by the Federal Trade Commission. The database now contains more than one million consumer fraud complaints that have been filed with federal, state, and local law enforcement agencies and private organizations. The data can be accessed through an encrypted website by hundreds of law enforcement organizations, including more than 90 federal law enforcement organizations, and over 1,000 state-run and local fraud fighting agencies. Various Canadian and Australian law enforcement organizations can access the data as well. In offering a variety of tools to law enforcers, Consumer Sentinel helps facilitate investigations and, if necessary, prosecutions.

In addition to the complaint database, Consumer Sentinel features include data analysis to identify fraud trends, an index of fraudulent telemarketing sales pitches available from the National Tape Library, alerts about companies under investigation, a contact list, and how-to information to help agencies coordinate effective joint action. Consumer Sentinel's data helps law enforcement to pinpoint trends and developments in consumer fraud.

Data is contributed to Consumer Sentinel by a range of organizations either in the law enforcement community or in the private sector. Some leading data contributors are the FTC, Better Business Bureaus, the National Fraud Information Center, and Canada's PhoneBusters.

For the Clearinghouse, it provides both U.S. and Canadian members of the Consumer Sentinel network with direct, online and secure access to the consumer complaints that the FTC has received. Law enforcement officers can search the Clearinghouse database for complaints based on the location of a suspect, a victim or a particular company involved in the misuse of the identities, or many other key elements of the crime. Currently, more than 1,000 law enforcement agencies have direct online access to almost 700,000 identity theft complaints through the Clearinghouse. The diversity of data sources gives Consumer Sentinel users a broader, more complete picture of current trends in consumer fraud and identity theft.

The Clearinghouse, an integrated part of the Consumer Sentinel system, contains more than 279,000 complaints as of January 1, 2003.

Information stored within the Clearinghouse is shared electronically with other law enforcement agencies nationwide via Consumer Sentinel. Such information provides law enforcement agencies with a broad range of complaints, allowing them to spot patterns of illegal activity. The information also enables policy makers to get a sense of the extent of identity theft and how it's taking place (e.g., credit card vs. phone fraud, latest scams, etc.). At the same time, the Clearinghouse provides information to some private entities to enable them to better protect consumers from identity theft.

7.20. Credit Industry Fraud Avoidance Scheme (CIFAS)

Origin and Membership

CIFAS is a fraud prevention service in the United Kingdom. It is a non-profit association dedicated to the prevention of financial crime in general. Established in 1988 by major retail credit lenders in the U.K.'s consumer credit industry, CIFAS was developed as a result of a rapid rise in fraud losses in the 1980s. Retail lenders were severely affected, and a number of them met to discuss the situation in 1987. At the same time, the police advised the credit industry to accept that fraud prevention was a non-competitive issue and that co-operation and communication was necessary among lenders to successfully reduce frauds funded by the financial services industry. The CIFAS concept was founded after a series of meetings among the retailers and CIFAS became operational by late 1988.

CIFAS was initially established as an association under the auspices of the Consumer Credit Trade Association. CIFAS grew rapidly in the early years and was incorporated as an independent company limited by guarantee on February 22, 1991.

Currently, CIFAS has over 240 member companies from different industries, including consumer and commercial/corporate credit grantors, deposit takers, leasing and hire companies, motor finance providers, insurance companies, and other providers of products, services and facilities. However, intermediaries such as brokers and independent financial advisers are yet to be granted membership.

In order to become members of CIFAS, organizations have to register under the Data Protection legislation to hold data for crime prevention and prosecution of offenders. They need to specify how their data may be shared among CIFAS members and are willing to identify frauds and share details with other members in exchange for being able to access other members' fraud data. At the same time, organizations wishing to become members need to be a client of a Participating Agency within CIFAS, and these Agencies are Callcredit and/or Equifax and/or Experian and/or MCL Software Ltd. Furthermore, these organizations have to agree to receive training and be visited by CIFAS annually to confirm that they are complying with the membership rules.

Organization and Management

A Board of Directors is responsible for CIFAS. It includes elected non-executive directors from the membership together with independent non-executive directors, non-voting Observers from the Police and National Consumer Council. The Board is primarily responsible for the direction

and future strategy of CIFAS. There are also a number of elected Management Committees that deal with operational and other matters

Scope and Objectives

Being the world's first non-profit fraud prevention data sharing scheme, CIFAS serves to safeguard interests of CIFAS members by pooling information on fraud and attempted fraud. It ensures that victims of fraud are not prejudiced by misuse of their identities and documentation, as well as to expand crime prevention data-sharing to encompass both the private and public sectors in the public interest[10].

Collaborative Activities

CIFAS has undertaken a number of key collaborative activities. They include providing a data sharing scheme to share information on fraud cases among financial services providers and other companies. Other schemes modelled on CIFAS have been set up in South Africa, Ireland and Germany.

CIFAS represents its members to government, the media and the business community, and it provides members with best practice guidance, training and networking opportunities.

Information services are offered to the general public, as they can learn more about identity fraud through a leaflet created by CIFAS or the consumer information website. Consumers are given advice on what actions they should take should they believe they may have fallen victim to identity fraud or impersonation, and there is a 'Protective Registration' service for victims to protect their identity from misuse.

In addition, CIFAS has created the CIFAS Organised Fraud and Intelligence Group, which organizes quarterly regional meetings involving local members, and Police/Public Sector contacts. CIFAS also organizes different events and conferences, as well as having launched the first UK Identity Fraud Index developed from data supplied by its members in identifying business sectors that are often targeted by fraudsters and organised crime. The average index figure is 100. Higher index figures indicate the business sector is being targeted more than average, whereas an index below 100 means the opposite.

Meanwhile, members of CIFAS are required to operate effective in house procedures to enable fraud or attempted fraud to be identified and the cases placed into classifications known as the CIFAS categories. Basic information on each case is filed on the CIFAS database. The information is then transferred electronically to all the agencies. When an address against which a fraud has been filed, is searched, by any other member, through any Participating Agency, the searching member is made aware of the need to investigate through a warning, followed by the CIFAS category, and the identity of the member filing the data. CIFAS membership therefore involves both responsibilities and benefits. Members have a responsibility to contribute information by identifying, categorising and filing fraud cases on the database. In return for doing so, they receive the benefit of system generated warnings previously filed by other Members. In all impersonation cases, CIFAS Members are obliged to send a mandatory letter to the innocent victim if their current address is known, advising of the CIFAS warning and how it will prevent

[10] http://www.cifas.org.uk/default.asp?edit_id=563-73

further impersonation activity. A CIFAS warning against an innocent victim warns other CIFAS members to seek confirmation of identity to confirm they are not dealing with the fraudster.

7.21. Cyber Security Industry Alliance (CSIA)

Origin and Membership

Founded in 2004, Cyber Security Industry Alliance (CSIA) is an advocacy group created by security solutions providers, who share the technical expertise, depth and focus to encourage a better understanding of security issues.

The CSIA welcomes organizations involved with the provision of internet security hardware, software, and services to join the alliance, as well as law, consulting and accounting firms and educational institutions.

Members of the CSIA pay different amounts of membership dues depending on the focus and revenues of a member company. In order to be part of the board of directors, a member organization has to be in the cyber security industry.

Organization and Management

The CSIA is an independent legal entity, consisting of a board of directors and three working committees. They are the Coordinating committee, the Europe Advisory Committee and the Public Relations Committee. Eight directors currently sit on the Board, and they are chairpersons or senior managers of companies in the Internet security sector. The Board oversees how well the organization is fulfilling its intended mission and it selects officers to run the organization.

Scope and Objectives

With offices in the United States and Belgium, the CSIA deals mostly with its members in the U.S. and the European Union. The organization is dedicated to ensuring the privacy, reliability and integrity of information systems through public policy, technology, education and awareness. Members of the CSIA strive to enhance cyber security through public policy initiatives, public sector partnerships, corporate outreach, academic programs, and alignment behind emerging industry technology standards and public education.

Collaborating Activities

The CSIA has worked with government agencies in developing data breach legislation. It has fought with the U.S. Department of Homeland Security to have the position of assistant secretary for cyber security created.

Every year, the CSIA partners with the Computer Security Institute (CSI) to hold a conference on computer crime and security issues. It also sponsors the annual Security World Development Conference, where the latest issues arising from secure software development and programming are discussed.

7.22. Liberty Alliance Project

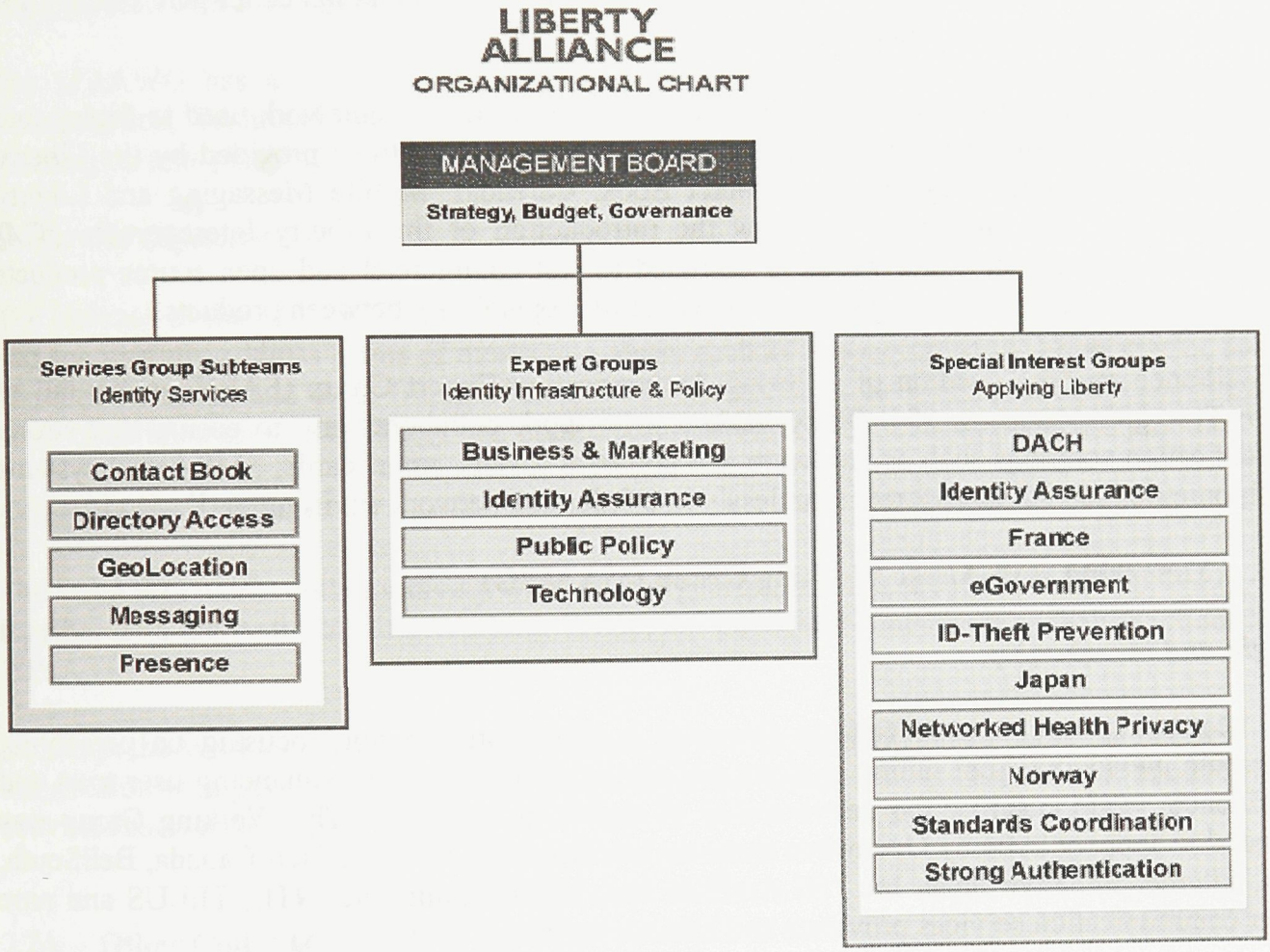
Origin and Membership

Formed in 2001 by about 30 organizations, the Liberty Alliance Project is a global alliance that aims to establish open standards, guidelines and best practices for federated identity management. This goal was met when the Alliance released Liberty Federation in 2002, which is the industry

standard for addressing authentication, privacy and security challenges faced by organizations and individuals involved in online identity management.

At present, the Alliance has nearly 150 members from various fields. Current members include banks, telecommunications companies, service providers, vendors and government agencies around the world. There are no specific criteria for becoming members of the Alliance, and companies interested in doing so are only required to fill out various forms. Once companies activate their membership, they enjoy numerous benefits, which include the ability to network with other members of the Alliance to work on identity management, to participate in different special interest groups and to market the companies on different levels.

Organization and Management



The Alliance is governed by a Management Board that works on strategy and budget development and on governance. The Board is reported to by three groups. There are the Services Group Subteams, which focus on identity services. The Expert Groups are responsible for identity infrastructure and policy, and the Special Interest Groups work on applying liberty. Different sub-groups fall under the three groups.

Scope and Objective

The Liberty Alliance Project's objective is to establish technical, business and policy standards for digital identity management and Web services. According to its mission statement, the group is "designed to serve as a hub for a global effort against identity theft and will be attacking issues from multiple perspectives in a collaborative, open and vendor-neutral environment."

Collaborative Activities

The Liberty Alliance Project has formed a cross-organizational Liberty Alliance Identity Theft Prevention Group that focuses exclusively on combating identity theft. Its operational goals are to act as a business and technology forum to address identity theft on a holistic level – across industries and attack vectors; to leverage Liberty's tack record and capabilities in developing business and technical best practices; to work with existing ID theft-related organizations to bolster their efforts; and to make recommendations into Liberty Alliance Expert Groups for additional technical, policy and business work.

In 2003, the Alliance released the Liberty Web Services, an open framework used to deploy and manage a range of different identity-based Web services. Applications provided by the Liberty Web Services include Geo-location, Contact Book, Calendar, Mobile Messaging and Liberty People Service. The same year also saw the introduction of the Liberty Interoperable (TM) certification program in 2003, which is designed to test commercial and open source products against published standards to assure base levels of interoperability between products.

The Alliance saw the creation of a Strong Authentication Expert Group (SAEG) in the fall of 2005. This group consists of industry leaders, who work collaboratively to ensure that strong authentication solutions such as hardware and software tokens, smart cards, SMS-based systems and biometrics can be interoperate seamlessly in a federated network environment[11].

7.23. Messaging Anti-Abuse Working Group (MAAWG)

Origin and Membership

The Messaging Anti-Abuse Working Group is a global organization focusing on preserving electronic messaging from online exploits and abuse with the goal of enhancing user trust and confidence, while ensuring the deliverability of legitimate messages. The Working Group was founded in January 2004 by Openwave Systems Inc, Abranet, Adelphia, Bell Canada, BellSouth, Cox, Internet Initiative Japan Inc., IIJ America Inc., NII Holdings Inc, NTL, TELUS and nine other communication services providers and Internet service provider (ISPs).

With a broad base of ISPs and network operators representing over 600 million mailboxes, key technology providers and senders, the MAAWG works to address messaging abuse by focusing on technology, industry collaboration and public policy initiatives.

Service providers and vendors, as well as any company that wants to help address the messaging abuse problem are welcome to become members of the MAAWG. There are three levels of memberships at the MAAWG. Joining the organization as supporters, individuals are allowed to participate in working committees, attend meetings of the MAAWG and gain access to the

[11] http://www.projectliberty.org/liberty/about/history

documents and resources on the members-only section of our Web site. However, there are no voting rights at this level. The cost is $3,000 for a 12-month membership.

Individuals can choose to become full members, and they enjoy all the benefits listed above with the addition of voting rights. Also, full members may run for election to the Board of Directors. Two full members are elected to serve on the Board every 12 months. The cost is $12,500 for 12 months.

As sponsors, members get a seat on the MAAWG Board of Directors. At this time, all Board positions are filled except for openings for operators headquartered outside of North America. The cost is $25,000 per 12 months.

Organization and Management

The MAAWG has a Board of Directors and three main working committees, which are the Collaboration, Technical, and Public Policy Committees. There are also several subcommittees working on anti-phishing, zombie/botnets, sender best practices and initiatives.

Scope and Objectives

The purpose of the MAAWG is to bring the messaging industry together to work collaboratively and successfully address forms of messaging abuse such as messaging spam, virus attacks, denial-of-service attacks, and other forms of abuse. The MAAWG is developing initiatives in the three areas of collaboration, technology and public policy to resolve the messaging abuse problem[12].

Collaborative Activities

The MAAWG works collaboratively with other organizations. Recently, the Working Group, together with the Anti-Phishing Working Group, has published Anti-Phishing Best Practices for ISPs.

Although the Working Group does not lobby on government public policy issues, it shares information with government agencies. It also develops best practices for other anti-fraud activities such as anti-spam.

7.24. Other Collaborations

Proposed rulemaking

In July 2006, the five federal agencies that oversee the financial industry (Federal Reserve, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, the Office of Thrift Supervision and the Federal Trade Commission) published a Notice of Proposed Rulemaking seeking to better coordinate the battle against identity theft. One of the proposed rules would require credit and debit card issuers to assess the validity of a request for a new credit or debit card if it followed a change of address by 30 days or less. The agencies jointly propose regulations that would require each financial institution and creditor

[12] http://www.maawg.org/about/

to implement a prevention program that detects, prevents and mitigates identity theft in connection with account openings and existing accounts. They'll be asked to use guidelines listing patterns, practices and specific forms of activity that should raise a "red flag" signaling a possible risk of identity theft. Additional proposed regulations would require users of consumer reports to develop reasonable policies and procedures to apply when they receive a notice of address discrepancy from a consumer-reporting agency. (CardLine, 2006)

International identity theft conferences

The first-ever International Identity Theft Conference was hosted by the Ontario Provincial Police (Anti-Rackets), in Orillia, Ontario, from October 21 to 23, 2003. The conference was attended by more than 300 participants from government, police, law enforcement and the private sector from across Canada, the United States and as far away as Australia.

Law enforcement training

Since 2002, a group of U.S. federal law enforcement and regulatory agencies (including the Department of Justice, the Postal Inspection Service, the Secret Service and the Federal Trade Commission) has jointly sponsored a series of regional training seminars for state and local law enforcement authorities throughout the United States. To date, the participating agencies and the American Association of Motor Vehicle Administrators have conducted 18 one-day seminars. These seminars include practical guidance and information resources for state and local police, sheriffs, and prosecutors on how to respond to and investigate identity theft.

Consumer awareness campaigns

"Operation: Identity Crisis" was a national consumer awareness campaign organized by the U.S. Postal Inspection Service in conjunction with the U.S. Postal Service, Federal Trade Commission, U.S. Secret Service and various other governmental agencies and private companies associated with the Financial Industry Mail Security Initiative (FIMSI). The campaign, which took place in September 2003, focused on educating consumers about ways to protect themselves from various identity theft schemes. It also provided businesses with prevention tips to help them protect consumer data and ensure privacy.