MeRC

McMaster eBusiness Research Centre

A THEORETICAL FRAMEWORK FOR COMBATING IDENTITY THEFT

By

WenJie Wang, Yufei Yuan, Norm Archer

wenjiew@dhu.edu.cn
yuanyuf@mcmaster.ca
archer@mcmaster.ca

McMaster eBusiness Research Centre (MeRC)
DeGroote School of Business

MeRC Working Paper No. 12

September 2004

McMaster University

A THEORETICAL FRAMEWORK FOR COMBATING IDENTITY THEFT

By

WenJie Wang, Yufei Yuan, Norm Archer

MeRC Working Paper #12
September 2004

DeGroote School of Business
McMaster University
Hamilton, Ontario, L8S 4M4
Canada
wenjiew@dhu.edu.cn
yuanyuf@mcmaster.ca
archer@mcmaster.ca

ABSTRACT

Identity theft is not a new phenomenon, but due to the widening applications of the Internet that increases exposure of users to this threat, it is beginning to cause more and more damage to the economy and society in general. Therefore, research on identifying and combating ID theft is both imperative and urgent. In this paper, a theoretical framework is proposed to identify key stakeholders and their interactive relationships that play a role in combating identity theft. The identification and clarification of the responsibilities of the relevant stakeholders, along with related activities, will help to understand how to defend against identity theft in an efficient and effective manner. We also note the potential and urgency for future research on particular aspects of identity theft.

KEYWORDS

Identity theft analysis, theoretical framework, stakeholders and relationships, combating identity theft

TABLE OF CONTENTS

1. INTRODUCTION

Identity theft (ID theft or IDT), a crime resulting from unauthorized collection and fraudulent use of someone else's personal identity and other relevant information [1], is becoming a significant and growing problem in many countries. It is resulting in more and more damage to consumers, society, national economies, and national security. Every year, millions of individuals and organizations are victimized by identity thieves. Victims of ID theft suffer financial loss, damage to their reputations, emotional distress [2], and may even risk false arrest and having their (true) histories viewed with suspicion [3]. The estimated cost of identity theft in the U.S. was nearly US$ 53 billion in 2002 [4]. *Phonebusters*, a Canadian ID theft reporting agency, estimated a cost of about $ 21.5 million to Canadian consumers and businesses in 2003 [5]. However, the most dangerous aspect of the threat is its potential use by terrorists to breach national security.

ID theft is more than a significant problem – it's a growing problem. According to Tim Hudak, Ontario Minister of Consumer and Business Services, "In the past five years, identity theft has emerged as the fastest growing and most serious consumer crime in North America [6]." ID theft reports in the *Consumer Sentinel* database grew from 31,000 in 2000 to 86,000 in 2001 and then to 162,000 in 2002 [7]. Incidents of identity theft reported in 2003 were 214,905, up 33% from 2002 [8]. The U.S. Federal Trade Commission (FTC) reported in 2003 that ID theft was the top fraud complaint reported by consumers in 2000, 2001, and 2002. Forty-three percent of consumer fraud complaints to the FTC in 2002 involved identity theft [7]. An FTC survey of US adults concluded that almost 10 million Americans were victims of ID theft of some form in 2002, an 81% rise over 2001 [9,10]. According to *PhoneBusters*, more than 13,000 Canadians were victims of identity theft in 2003, compared with 8,180 in 2002 [3]. Americans are more concerned about identity theft than unemployment or corporate fraud, according to a survey of 2,000 people conducted by *Star Systems* [11]. A major reason for the growth in the identity theft problem is the explosive growth of Internet applications, making identity theft easier, and dramatically increasing the potential occurrence and impact of identity theft.

ID theft is now recognized as a social problem, whereas ten years ago the terms "identity theft" and "identity fraud" were virtually unknown and received very little attention. Consumers were not fully aware of the severe damage that it could cause and did not know how to protect themselves. Legislation was not and is not yet adequate for safeguarding potential victims and punishing identity thieves. Few researchers and institutions have studied identity theft issues. Combating identity theft and protecting consumers is of urgent importance if we are to maintain a healthy economy and stable society environment, and considerable research is needed to understand and respond to this threat.

Identity theft prevention is a very complex issue. It is not just a technical, but mostly an economic, social, and legal issue. It involves multiple stakeholders such as identity issuers, owners, checkers, and protectors that work together to combat ID theft criminals. It is thus important to study the roles of all the stakeholders as an interacting system, in order to address identity theft issues comprehensively and to propose effective ways to combat this problem.

In this paper, we analyze the nature and scope of ID theft in section 2 and develop a systematic

framework for combating identity theft. We identify the key stakeholders and their interactions in section 3. The roles and responsibilities of each stakeholder in the framework are discussed in section 4. Section 5 outlines identity information collection for the purpose of authentication and service provision, and section 6 describes possible identity fraud activities. How to prevent and detect identity theft and to protect identity theft victims by law are discussed in section 7. Finally, we propose some future research directions for combating identity theft.

2. IDENTITY THEFT

You have used your credit card for many years without any problem. But recently creditors you never heard of are repeatedly calling you and demanding payment for merchandise you never bought. Your credit history has always been perfect, but you are now being denied financing due to several delinquencies appearing on your credit report [12]. Today, these kinds of problems have happened to hundreds and thousands of victims of the crime known as "identity theft". The FTC has defined ID theft as "Identity theft occurs when someone uses your name, address, Social Security number (SSN), bank or credit card account number, or other identifying information without your knowledge to commit fraud or other crimes [13]." PIAC (Public Interest Advocacy Centre in Canada) uses the definition, "Identity theft is the unauthorized collection and fraudulent use of someone else's personal information. Victims of ID theft suffer financial loss, damage to their reputation, and emotional distress, and are left with the complicated and sometimes arduous task of clearing their names [1]." However, no uniform definition for ID theft has been adopted widely.

Besides basic information like names, addresses and telephone numbers, identity thieves look for Social Insurance Numbers (SIN, in Canada) or Social Security Numbers (SSN, in the U.S.), driver's license numbers, credit card or bank account numbers, as well as birth certificates, passports, bank cards, health cards, or telephone calling cards. The most common purpose of ID theft is financial gain. Other reasons for stealing personal information include ruining the reputation of another person [14], avoiding criminal prosecution, and starting a new life under a new identity. In the US, innocent ID theft victims have been arrested and jailed for crimes that imposters have committed [3]. Criminals, from local deadbeats to international terrorists, use false identification to escape detection by law enforcement officials, both before and after committing crimes. Imposters may also steal and use other identities in order to hide from abusive situations or to leave behind a poor work and financial history.

ID theft is a truly modern crime. It can be carried out internally to an organization by an employee, through physical theft from individuals, or by criminals working online from thousands of miles away through public communication networks. It relies on the commercial culture of ubiquitous personal information holdings, easy consumer credit, and the networking facilities of modern technology. It also relies on lax consumer security. ID thieves exploit business and government information leaks, credit industry excesses and unsafe practices, inadequate consumer control over trade in credit information, and the use of personal information for collateral uses. Government identification weaknesses, government ID "function creep", a lack of specific legal definitions of ID theft offences, uncoordinated law enforcement, and unfocussed privacy laws round out the list [1].

3. FRAMEWORK FOR COMBATING IDENTITY THEFT

Identity theft issues have been receiving a growing amount of attention from business, consumers, government, and the media. However, to the best of our knowledge, there have been few if any attempts to develop a general strategy and framework for research on ID theft problems. In this paper, we propose an abstract and systematic framework for studying and combating identity theft. This framework describes the major players involved, and their roles and interactions in the prevention, detection, and legal prosecution of ID theft. We present the framework in Fig. 1, where the major players are represented by nodes, and their interactions and information flows are indicated by arrows.

There are four main stakeholders involved in combating identity theft: (1) identity owners, who own and legally use various kinds of identities for different social and financial activities and wish to be protected from identity theft; (2) identity issuers, who authorize and issue identity to provide the owner the proof of identity and the right to acquire related social and financial services; (3) identity checkers, who verify the identity of the identity owner and permit related services; and (4) identity protectors, whose major duty is to safeguard the rights and interests of other stakeholders, including identity owners, identity issuers, and identity checkers, by finding and prosecuting thieves and setting guidelines for the issuers and checkers. A fifth stakeholder, who of course works against the goals of the other stakeholders, is the identity thief, who illegally or unethically steals and counterfeits true owner identities for financial or other purposes, and fraudulently abuses the rights of the owners by committing fraud.

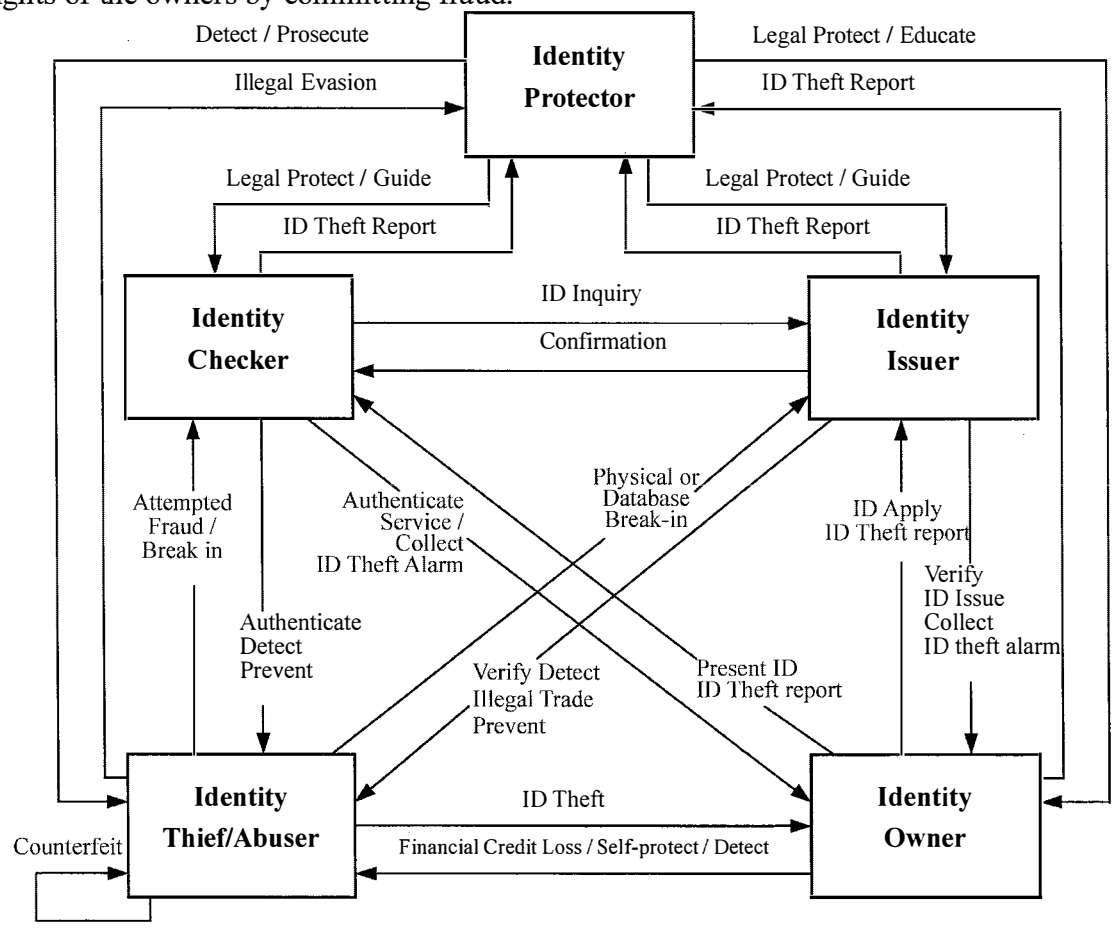

Figure 1. Theoretical Framework: Combating Identity Theft

The five stakeholders interact with each other through three main interrelated activities: (1) identity authentication and information collection activities; (2) identity fraud activities; (3) identity theft combating activities, which include identity theft prevention, identity theft detection, and identity theft victim protection and theft prosecution by law. To issue identity and provide confirmation for the checker, issuers (government agencies, financial institutions, and other trusted authorities) collect and authenticate personal identity information. Identity checkers, such as online merchant services, verify and hold personal identity information to ensure that they can provide service to real ID owners. Such sensitive information must therefore be secured and maintained at a high level by management and technology means. Perpetrators of identity theft obtain personal identities through illegal means and then use it to masquerade to gain financial or other benefits in various ways. Safeguarding personal ID is the ID owners' responsibility. Government legislation, business management, consumer awareness, and technology all play important roles in preventing, detecting, and prosecuting identity theft. All the stakeholders involved, including the ID protector, ID issuer, ID checker, and ID owner, must take part in a continuing joint effort to protect personal identity and to combat identity theft.

Vigorous activities, as reflected by this framework, to prevent, detect, and prosecute identity theft, are necessary to build a healthy economic and business development environment. Some potential uses of the framework include:

- Suggesting the most critical statistics for measuring and tracking ID theft
- Analyzing relationships among the various stakeholders involved in the identity management process
- Studying the impact of changes in one type of activity on the remaining activities and stakeholders
- Isolating weaknesses in the identity management process, and proposing ways to strengthen the process
- Examining the effectiveness of fraudulent activity prevention and detection
- Determining the return on investment for various types of technologies used to control ID theft
- Clarifying interactions among the stakeholders involved in building systematic and effective technical solutions
- Evaluating the balance between the need for privacy and the need for centralized databases of personal data to counteract ID theft
- Assessing ID theft risk and developing a systematic and efficient security strategy

In the following sections, we will examine the roles and responsibilities of each stakeholder and the relationships among them, by analyzing the activities involved in the proposed framework. This will help to establish a better understanding of how to properly protect identity in the rapidly

developing Internet and information environment. Based on this framework, we then extend the discussion to some potential research that will foster success in combating identity theft.

4. STAKEHOLDERS INVOLVED IN COMBATING IDENTITY THEFT

4.1 Identity Owners

Identity owners are the individuals who have the legal right to own and use their personal identity. Because of an identity's financial value and other useful benefits, identity owners become the target of identity thieves. The resulting damage and loss are a cause for concern by ID owners.

Many kinds of ID certificates are used as individual identifiers, including government-issued certificates, such as SSN or SIN cards, driver's licenses, passports and birth certificates, and business certificates, such as credit cards, debit cards, telephone cards, and digital certificates that are used in online transactions. In North America, SINs or SSNs and driver licenses are de facto identifiers, and are therefore the most valuable identifiers for ID thieves. As the Privacy Commissioner of Canada states, "Your SIN can be used to steal your identity." [15] Credit card numbers are another valuable form of identifiers that ID thieves pilfer for financial purposes.

Identity owners apply to various trusted issuers to obtain ID certificates for different purposes related to social activities and financial services throughout their lives. When babies are born, their parents apply for a birth certificate that serves as the child's original identity. From then on, based on that identifier, individuals apply for other kinds of ID certificates for the purposes of receiving welfare, driving qualifications, qualification for traveling abroad, all kinds of financial transactions, and so on. For example, individuals must obtain passport from their own governments before traveling internationally. Another example is the Canadian SIN, which serves as a client account number with the federal government for the administration of pension plans, employment insurance programs, and tax reporting purposes.

Since identities are the property of the ID owners, it is their responsibility to safeguard them. Although ID owners are increasingly concerned with the security of their identities, they must translate this into an awareness of the risk, and the need for active self–protection against ID theft and the resultant damage. This requires education in how to protect against ID theft, how to monitor their ID status, and how to report ID theft to ID protectors. Owners who are the victims of ID theft need to be able to clear the resulting damage to their reputations and any blemished records easily and quickly in order to reduce their financial and emotional losses. In addition, ID owners are responsible for using their ID legally and not abusing their rights by lending their identities to other persons (e.g. lending health cards to acquaintances), that may cause damage to ID issuers.

4.2 Identity Issuers

An identity certificate is used to identify a specific person (or organization) for a specific purpose over a specific period of time. An ID certificate usually consists of six information components: the certificate identifier, the certificate receiver (owner), the purpose of the certificate, the

certificate issuer, the validation time period, and the signature of the issuer. A certificate also contains information to verify the certificate holder, such as a photograph or fingerprint, and an identifier of the certificate authorizer such as a watermark, stamp, etc. An ID certificate can be represented by a physical token such as a passport or birth certificate, or in a digital form such as a digital certificate issued by a trusted authority such as VeriSign [16] on the Internet.

Identity issuers are trusted government or private institutions who issue the related identity certificates to prove or authorize a certain social and financial right to the ID owner. Governments issue ID certificates such as SSN or SIN cards, driver's licenses, passports, and birth certificates to eligible individuals. Private institutions may issue business ID certificates, such as credit cards, debit cards, telephone cards, and digital certificates. After verifying applicant identification, ID issuers give the related ID certificates to qualified applicants and reject unqualified applicants. The responsibility of an identity issuer is to verify the true identity of the receiver and to issue a certificate that can be used by an identity checker to verify this identity.

Identity certificates are often cross-referenced. The birth certificate, as the first identity certificate received by any person, is issued by a government after authenticating the birth documents provided by the hospital and a guarantor signature on the birth certificate application. From then on, a birth certificate is a basic requirement in applications for most government identification and services, including SINs or SSNs, health care, driver's licenses, passports, and social benefits [6]. During the passport application procedure, for example, the birth certificate and two other valid identifiers are required to verify the applicant's identification. Credit card issuers issue credit cards after verifying applicant identities by one or more identifiers and assessing credit worthiness through credit bureaus. Certificate application is a chain process, so a single breach may cause a series of problems or questions to arise concerning the true identity of the applicant.

ID certificates and related identity information are the main targets of most ID theft. ID issuers have the responsibility to issue secure ID certificates and to protect sensitive identity information that they hold in archives or databases. ID certificates need secure features that help to prevent counterfeiting and impersonation by ID thieves, in addition to verifying a certain right bestowed on the ID owner. ID issuers need to use secure technologies and strict internal management mechanisms to protect identity information against ID theft of such forms as computer hacker or insider abuse. Unlike the loss of a physical ID certificate, this type of identity theft is often difficult to discover. It is therefore critical to use appropriate physical and digital security mechanisms to protect issuer databases against identity theft. In addition, the identity issuer must also provide protection mechanisms for both the identity owner (such as timely cancellation of stolen ID and database breach security alarms) and the identity checker (such as cancellation notification of stolen ID). We will discuss the detection and protection process in detail later.

4.3 Identity Checkers

Identity checkers are the service providers who verify ID holders' authenticity and eligibility, and provide related services. Identity checkers, such as customs officers and traffic police, examine the contents of the ID certificate and compare them (including photo ID) with the physical appearance of the identity holders to verify identity. Credit card checkers, such as merchants, normally verify

credit card validity through electronic communication with the issuer and bank. The cardholder's signature, however, is usually not carefully verified. Such weak verification is not acceptable in other countries such as China where, in addition, a PIN (personal identification number) number must be provided.

The ID checker must assume that the ID holder may be either the real owner or a thief /abuser. The main responsibility of ID checkers is to detect ID abusers by authenticating holder identities. ID checkers therefore need to use strict authentication processes and execution mechanisms. The front-line ID checker must be trained to examine identity certification and holder identification according to a standard authentication process. Techniques used include recognizing fake identity with the help of advanced technology. ID authentication technologies continue to evolve in order to combat the increasing sophistication of ID thieves. For example, some mobile phones have fingerprint readers for payment authentication, and these may be widely accepted in the future [17].

Identity thieves commit fraud not only by attacking identity certificates, but also by trying to break into databases and archives where identity information is stored. For example, a large US retail chain was reported to be the target of a scheme to steal credit card numbers by taking advantage of the firm's unsecured Wi-Fi network [18]. ID checkers have the responsibility to protect identity information against such incursions, and to notify the identity owners if such a breach is discovered.

4.4 Identity Thieves

Identity thieves are individuals or organizations who try to steal and use identity illegally for financial or other purposes. Thieves may be individuals, crime rings, terrorists, or international crime rings. Some thieves steal identity information by traditional means, such as "dumpster diving", "shoulder surfing", or mail theft. The modern online identity thief attacks victims through the Internet, through techniques such as database hacking, spoofing (sending a message to a computer from a source that pretends the message is coming from the IP address of a trusted computer) or phishing (sending an e-mail message to a targeted individual, asking the individual to access a Web site that mimics a trusted institution and divulge private identity information).

Although many people think that identity theft is primarily carried out by faceless strangers, statistics show that the perpetrator is often someone known to the identity owner, such as a relative or a family friend, or a work colleague. Moreover, the thief is frequently somebody who works in an organization of which the victim is a customer. A recent study of over 1,000 identity theft arrests in the U.S. reveals that as much as 70% of the theft of personal data is carried out by a company by an employee, or surprisingly often by a business owner. Organized crime rings often place members in low-level clerical jobs at banks in order to commit identity theft and other crimes [19].

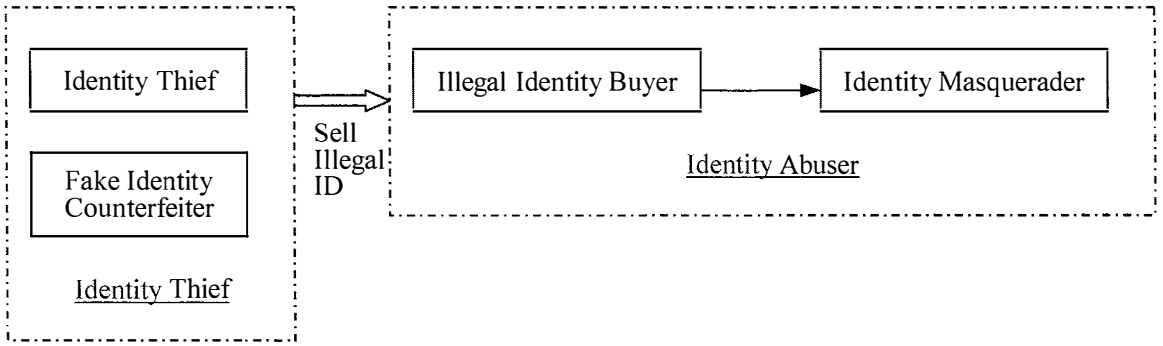

Figure 2. Different Roles in Identity Theft

When an identity thief commits fraud, two basic roles can be recognized, as shown in Fig. 2. One role is that of the identity thief who steals personal identity information or who counterfeits fake identity. The other is the identity abuser who masquerades as the targeted person in order to gain access to their finances or commit other crimes. Identity thieves, such as employees of financial institutions, may sell the personal identity information they acquire illegally to individuals or crime rings who use this information to commit offences. Sometimes, a bogus crime ring or individual will counterfeit fake identity, such as a passport or driver's license, to sell to individuals who then use it to impersonate the true owner, in order to become employed or start a new life elsewhere. In many cases the identity thief, identity counterfeiter, or identity abuser are the same individuals or organizations.

4.5 Identity Protectors

Identity protectors are individuals or organizations that work to protect individuals and businesses, including ID owners, ID issuers, and ID checkers, from attacks by identity thieves. Some may have legal powers to apprehend and punish the criminals. ID protectors can be government legislators, law enforcement agencies, and other public and private stakeholders. Government legislators, in concert with the Department of Justice (U.S.) and the Solicitor General's Department (Canada), enact laws to protect victims of ID theft and to punish the perpetrators. Law enforcement agencies, such as the RCMP (Royal Canadian Mounted Police) and FBI (Federal Bureau of Investigation), enforce laws to detect and prosecute violators and to give victims legal protection. In addition, there are some public and private organizations that contribute to the identity protection effort. In the U.S., the FTC was directed by the America Identity Theft and Assumption Deterrence Act of 1998 to establish procedures for educating the public, receiving complaints, and coordinating enforcement efforts with various investigatory agencies [3]. Credit bureaus, such as *Experian, TransUnion, and Equifax*, that serve retailers and other credit grantors by providing credit record information, also play a critical role in consumer protection by preventing and detecting ID theft. Various technology providers also contribute their efforts through technical solutions for the prevention and detection of ID theft. In summary, ID protectors can work to defeat identity theft through legislation, law enforcement, victim protection, education and guidance, and providing appropriate technology.

Table 1: Role and Responsibility of Main Stakeholders in Combating ID Theft

Main Stakeholders	*Role*	*Responsibility*
ID Owner	Legally own and use ID	• Safeguard ID • Fast victim recovery to reduce loss • Legally use ID
ID Issuer	Authenticate and issue ID	• Issue secured certificates • Protect ID certificate and information • Protect ID owner and checker
ID Checker	Authenticate ID and provide services	• ID authentication • Provide service to real ID owner • Protect ID information • Protect ID owner
ID Thief	Steal and abuse ID	• ID theft • ID counterfeit • ID abuse
ID Protector	Protect and prosecute	• Legislate • Enforce laws • Protect ID owners • Educate and guide • Provide technical solutions • Record and track complaints and detect trends

In support of identity protection, some law enforcement agencies have established ID theft call centers and statistical databases to record and track consumer and business complaints, and to provide education services for victims of identity theft. The *Consumer Sentinel* database, which is a national American database of ID theft statistics, contains more than one million consumer fraud complaints, and its members include more than 600 law enforcement agencies in Australia, Canada and the United States [20]. *PhoneBusters Canada* contributed seven percent of the 2002 ID theft complaints to the *Consumer Sentinel* database. This database can be used to build cases and detect trends in consumer fraud and identity theft [21].

Based on the discussion above, we can summarize the role and responsibility of five main stakeholders in combating ID theft, as in Table 1.

5. IDENTITY AUTHENTICATION AND INFORMATION COLLECTION

When ID owners use their identities to obtain services, their identities are authenticated by ID checkers, in order to gain confidence that people or things are who or what they claim to be. In this way ID issuers and checkers try to differentiate between real ID owners and ID abusers. Figure 3 shows the authentication process for ID owners only. The authentication and detection of ID abusers, although using a similar process, will be discussed in Section 7. ID issuers authenticate the identity of applicants in order to issue identity to the correct individuals. ID checkers verify the authenticity and validity of identity in order to give certain rights and to provide service to real ID owners. In some cases, such as credit card authentication, ID checkers communicate with the ID issuers to confirm identity information.

ID owners are required to present their identities or to enter a password or PIN (Personal Identification Number) to be authenticated. For example, passport applicants need to offer identities such as birth certificates in order to establish their true identity. Online transactions using credit or debit cards or other identification need reliable authentication to establish the user's identity through the use of a password or PIN. Unfortunately, identity exposure during presentation can increase the risk of theft. For example, "shoulder surfers" can steal identity by observing identity owners as they key numbers and passwords into public online terminals.

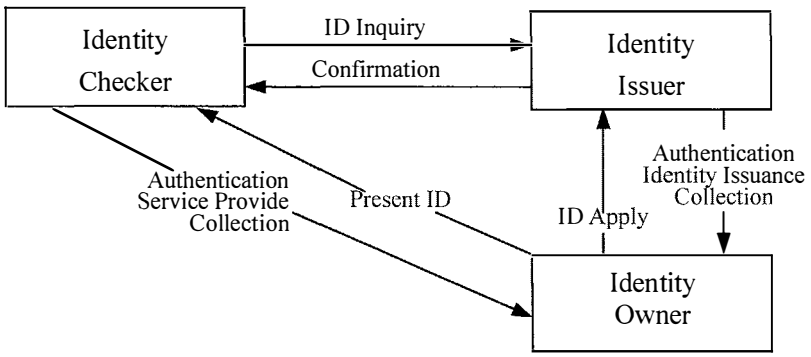

Figure 3. Identity Authentication and Information Collection Activities

For the purpose of recording, providing confirmation, retrieving, and renewing identity, ID issuers and checkers collect and store sensitive personal identity information, such as SINs, driver's license numbers, mother's maiden names, and bank account numbers, in archives and/or databases that will be used during authentication processes. These databases may be vulnerable to attack by ID thieves. In addition, sensitive personal identity information gathered for these purposes can compromise personal privacy, although any resulting loss of privacy must be balanced against the need for identity protection.

6. IDENTITY FRAUD

The two main targets of ID thieves are identity certificates and relevant identity information collected and/or exposed during authentication procedures. As shown in Fig. 4, identity fraud is directed towards ID owners, issuers and checkers by theft of identity information directly from the owner or by breaking into databases of issuers and checkers. For example, in March 2004, hundreds of consumer credit reports in the *Equifax Canada* database were accessed by criminals posing as legitimate credit grantors. The records included information such as SINs, bank account numbers, home and work locations, spouses' names, and up to six years of credit and banking history [22]. Employees of government issuing agencies have also been known to provide identity information illegally to private business, consequently exposing this sensitive information to the risk of ID theft. Insiders may also sell identity information for monetary benefit. Identity certificates are the other main targets of ID thieves, who may then use them to fake identity for fraudulent purposes.

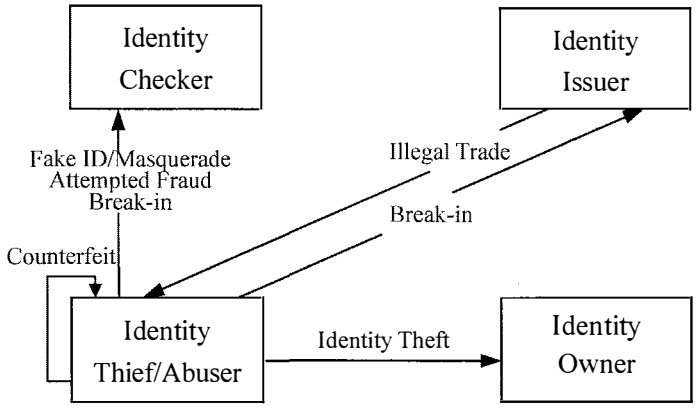

Figure 4. Identity Fraud Activities

ID theft and ID fraud concepts are interchangeable in most sections of this paper. However, they are used to indicate different activities in this section. Identity fraud describes the entire process of identity crime. It can be divided into two steps. The first step is identity theft or counterfeiting, and the second step involves identity abuse in the commission of crime, such as masquerading or illegally using fake identity. Identity theft, as one part of the identity fraud process, specifically refers to the activities where criminals steal identity and/or other relevant information. ID counterfeiters may then produce fake identity certificates for the identity abuser. ID abusers commit crimes that damage the ID owners or organizations with whom they interact, or compromises national security.

6.1 Identity Theft

There are many kinds of identity theft, which can be classified as traditional direct or electronic/online. Traditional theft activities include "dumpster diving" to retrieve personal data on old credit card or utility bills, stealing personal financial letters from mailboxes, stealing wallets and purses, "shoulder surfing" individuals enter personal identification numbers, bribing employees to hand over personal customer information, and physically stealing confidential files or computer hard drives from businesses or government [1], etc.. Some ID issuers may also sell identity information to private businesses for marketing purposes. For example the Canadian government recently acknowledged that one of its employees electronically stole personal data from about 200 Canadians, and may have passed the data on to other parties. The government informed the affected individuals that the information (which in this case did not include tax or financial data) may have been disclosed to a third party [23].

Identity theft has been described as the crime of the information age [24]. According to the U.S. Federal Trade Commission: "The Internet has dramatically altered the potential occurrence and impact of identity theft [2]." The Internet makes it easy for perpetrators to steal identity information just sitting in front of their computers at home. The explosion of financial services offered on-line, such as mortgages, credit cards, bank accounts, and loans, provides a sense of

anonymity to those potential identity thieves who would not risk committing identity theft in a face-to-face transaction. Online ID theft is becoming the fastest growing ID theft crime.

Online ID theft can be carried out by hacking into ID owners' personal computers or business servers and databases via the Internet, using spyware, or creating "phisher" websites. In phishing, the online thief, posing as a trusted Internet service provider, a digital certificate issuer, or even an "identity theft prevention" service provider, sends e-mails requesting that individuals enter personal information directly through dummy "phisher" websites. For example, on March 22, 2001, Microsoft issued security bulletin (MSO 1-017) alerting the Internet community that imposters were issuing fake *Verisign* digital certificates to individuals in Microsoft's name [16]. Some online thieves utilize phony "fraud alerts" to obtain personal information [25]. Spyware is a kind of program that is downloaded surreptitiously to run on Internet-connected PCs in order to steal data [26]. Email spam is another large and growing problem, indicated to represent up to 60% of e-mail traffic at a recent Brussels conference [27].

Despite consumer concerns about online fraud, electronic commerce has been booming. The US Census Bureau reported that retail electronic commerce sales for second quarter 2004 were $15.7 billion, up 23.1 percent from second quarter 2002 [28]. *VISA* reported that Canadians spent $772 million through 6.4 million online transactions during the 2002 Christmas season, up from $381 million a year earlier [29]. In order for the growth in Internet electronic commerce to continue, it is essential that online identity theft be understood well and effective strategies must be developed to combat it.

6.2 Identity Counterfeiting

Identity counterfeiters try to create fake certificates used to misrepresent one's identity. In 1993, an Egyptian citizen, Ahmed Abdullah al-Ashmouny, was indicted for counterfeiting thousands of visas on a color copier and selling them to other Egyptians, including followers of the accused terrorist leader Sheik Omar Abdel Rahman of Jersey City, enabling them to illegally enter the United States. According to Andrew Laney of the U.S. Department of State, the fakes were almost indistinguishable from actual visas [30]. Terrorists involved in the September 11th 2001 events also entered the United States with counterfeit passports and visa. These terrorists were able to use their fake IDs to get SSNs and driver licenses in the U.S. [31].

The major identity certificates that are valued by counterfeiters include passports, visas, birth certificates, driver's licenses, identification cards, social security cards, health cards, credit cards, bank cards and calling cards. Counterfeiters generally produce fake ID by swapping images on the certificates, altering the validation times or owner names on the certificates, or creating completely fake certificates in many cases [32]. Counterfeiters can be either individuals or crime rings. In the past, only skilled professionals with very sophisticated equipment, such as expensive engraving and printing equipment, could create counterfeit or altered ID documents. Today, however, casual counterfeiter can easily forge counterfeit identity certificates because sophisticated counterfeiting tools, such as PCs, scanners, card printers, image editing software, and desktop publishing technology, are readily available at decreasing costs [33]. The latest computer supported devices, such as embossers, encoders, and decoders, even allow counterfeiters to read, modify, and implant

magnetic strip information on credit cards [34]. With the advent of the Internet, templates of various documents are even for sale at Internet sites. Computer and Internet technology that makes identity counterfeiting easy makes it much more difficult to combat ID theft.

The aim of counterfeiting activities is to forge identity certificates, rather than attacking identity information. Therefore, in order to combat counterfeiting, it is necessary to focus on creating secure features for identity certificates to prevent forging. Certificate manufacturers must also be encouraged to keep information confidential that relates to anti-counterfeiting technology and production processes.

6.3 Identity Abuse

Identity abuse is the crime of unauthorized use of "stolen identity" to impersonate the identity owner to gain benefits, such as opening credit card accounts, getting loans or social benefits, opening telecommunications or utility accounts and more. In some cases, abusers have created and used an entirely new "fictitious identity" to fraudulently get employment, or start a new life, possibly in other countries. At the worst, criminals have committed crimes using "stolen or fake identity" to evade detection, investigation and arrest. This fraudulent abuse of identity can cause economic or emotional damage to victims or even society, as in the September 11th terror attack.

Table 2: How ID Theft Victim Information Is Abused (2002: 161,819 Victims)

Theft Type	*% of all Victims*
Credit card fraud	42
Phone or utilities fraud	22
Bank fraud	17
Employment related fraud	9
Government documents or benefits fraud	8
Loan fraud	6
Other identity theft fraud	16
Attempted identity theft	8

* Source: *Consumer Sentinel* and the *Identity Theft Data Clearinghouse*, 2003

** The percentages add to more than 100 because 22 % of victims reported more than one type of identity theft.

The U.S. FTC reported that the most common identity abuses are credit card, phone or utilities and bank fraud because of their great financial benefits. As shown in Table 2, these three kinds of abuse accounted for 81% of the total (161,819 victims) in 2002. Among them, credit card fraud accounts for the biggest proportion, at 42% [7,8]. It is apparent that credit card fraud should receive a high priority in combating ID theft. In addition, fraudulent travel document abuse should also receive considerable attention because of its potential disastrous damage to national security and social stability.

Understanding and analyzing ID theft is a very important and basic step for combating ID theft.

While ID theft problems can be more clearly understood through improved statistics gathering and analysis, research on preventing, detecting, and prosecuting actual ID theft is a top agenda item for the future.

7. COMBATING IDENTITY THEFT

Combating identity theft can be divided into three categories: prevention, detection, and legal protection and prosecution. Obviously, the best way to combat ID theft is prevention. However, if ID theft occurs, more damage accumulates if it is not detected very quickly. Moreover, ID theft detection provides the evidence necessary to punish criminals. Legislative and law enforcement agencies enact and execute laws to protect identity and victims of ID theft, and to prosecute violators.

Combating identity theft is a process that involves all five stakeholders, as shown in Figure 5. ID protectors play a key role in combating identity theft. Their major activities include preventing ID theft by educating ID owners, guiding ID issuers and checkers, detecting and prosecuting criminals, and protecting victim and identity information by law enactment and enforcement. ID owners must safeguard their identity and related information, check their credit status vigilantly, and report loss of identity to the relevant protector immediately, in order to minimize loss. ID issuers and checkers protect identity information held in databases and archives. When ID issuers and checkers detect ID theft they report the event to ID protectors and notify ID owners. ID issuers need to use advanced technology to prevent identity counterfeiting. ID checkers protect consumers from impersonation through advanced authentication technologies and restrictive checking policies. All stakeholders have their own responsibilities in combating ID theft. Any stakeholder's absence from this process will greatly increase the likelihood of ID theft and the loss if identity if theft occurs. An effective strategy to combat ID theft must involve a system that integrates all stakeholder contributions to the process.

7.1 Identity Theft Prevention

Identity theft prevention activities use measures and technologies to prevent ID theft. This is the best way to combat identity theft and protect possible victims. The main ID theft prevention activities, shown in Figure 5, can be classified into education and guidance, prevention technologies, and prevention mechanisms and policies. Public education and guidance activities help individuals and businesses to protect ID certificates and identity information. Advanced prevention technologies prevent ID counterfeiting, identity information theft, and abuse. Effective prevention mechanisms and policies help to prevent ID theft and to block ID abuse.

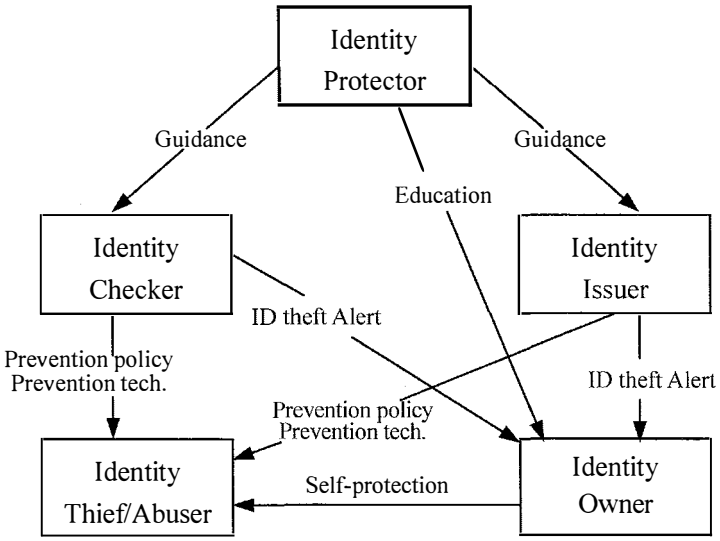

Figure 5. Identity Theft Prevention Activities

7.1.1 Education and Guidance

Education is an effective way to prevent ID exposure and ID theft. At present, ID theft prevention education can be classified into two categories: raising public awareness, and educating the public on self-protection. If the public is aware of possible severe damage from ID theft, they have an incentive to take measures to prevent it. ID protectors play a major role in public education, as do ID issuers and checkers who focus on customer education under the guidance of ID protectors. In North America, governments have presented TV specials that warn of potential damage from ID theft. Some companies have put ID theft alert messages on their websites and in advertising materials.

A key aspect of raising public awareness of ID theft is education on proper measures to protect identity and other relevant information. For example, government education materials and programs such as an Ontario government pamphlet on ID theft prevention [6] and an Australian Government National Crime Prevention Program [35]. These programs provide simple tips on preventing ID theft, such as destroying identifying information when disposing of private personal information, not giving out personal information to strangers over the phone or by e-mail, protecting against exposure when entering information into public online terminals, and using a separate bank account with a low credit limit for online transactions. Education on actions to take if consumers are victimized by identity theft is key to the process. Immediately informing police, credit bureaus, and financial institutions of such occurrences is important in order to minimize potential loss. In particular, financial institutions mitigate the risk by canceling existing credit cards, accounts, passwords and PINs, and replace them with new ones.

7.1.2 Prevention Technologies

Advanced prevention technologies are continually evolving, as they are used to protect identity and other relevant information from theft, counterfeiting, and abuse. Some prevention technologies, such as biometrics, smart cards, and special anti-counterfeit technologies, can be used to endow identity certificates with secure features that are hard to be counterfeited or fraudulently abused. PKI (Public Key Infrastructures) can be used to protect digital certificates and identity information in online transaction. Database security technology can prevent identity information theft. These technologies can be applied separately or jointly with identity protection activities. For example, storing biometric information on smart cards is a newer technique that can help to prevent ID theft.

Biometrics is seen as an identity protector [36] that can reduce ID theft [37] by accurately identifying the owner. Biometrics involves the use of unique human characteristics, such as fingerprints, voiceprints, or retinal eye scans [38,39] to accurately distinguish one person from another, even identical twins. An advantage of biometric authentication is that it requires the person being identified to be physically present at the point-of identification. This makes it difficult if not impossible to impersonate the ID owner. Moreover, authentication based on biometric techniques eliminates the need to remember a password, PIN, or carry a token, thus reducing identity information exposure [40].

Governments and businesses around the world have begun to use biometrics to prevent identity theft. The UN's International Civil Aviation Organization (ICAO), in May 2003, adopted a global and harmonized blueprint for the integration of biometric identification information into passports and other machine-readable travel documents. The United States now requires (as of October 2004) the inclusion of biometric identifiers in U.S. visas (digital photos and electronic fingerprints) and in the travel documents (digital photos) of 27 countries whose citizens do not currently require visas to travel to the U.S. [41]. The Canadian government has debated the use of a biometric Maple Leaf Card, that could be required for landed immigrants and other people who are not Canadian citizens [42,43] to live in Canada. The Canadian province of Ontario and the U.S. state of Colorado are also investigating the potential of biometrics for driver's licenses [44].

A smart card is a credit card-sized plastic card with an embedded IC (integrated circuit), which contains a microprocessor and enhanced memory to store information and processing capacity. Smart cards can be used in conjunction with other technologies to prevent ID theft. For example, smart cards can be used to store biometric information that serves to uniquely identify the owner and to deliver secure and accurate identity verification [46]. Moreover, smart cards are much more difficult to be counterfeited or altered than ordinary magnetic strip cards [47].

Digital certificates, often called online passports, work with PKI to help prevent online ID theft. PKI integrates digital certificates, public-key cryptography, and trusted online certificate authorities (CA) into a total network security architecture [45], which can create a secure online transaction environment for digital certificate owners. Smart cards can also be used to store and program private key and digital certificate confidentially with the help of PIN encryption to secure online transactions.

There are some advanced anti-counterfeiting techniques that can be used to protect identity, such as laid lines, watermarks and chemical voids, and optically variable ink, holograms, embossed characters and numbers, tamper-evident signature panels, magnetic strips with improved card validation technologies etc. [48]. These features make identity certificates hard to counterfeit or alter. For example, a watermark is an image formed by varying the thickness of the paper during its manufacture. The image becomes part of the paper and is difficult to reproduce, because it cannot be seen with reflective light--the kind used by scanners and copiers to make reproductions [30]. A Canadian passport has enhanced security features making it extremely difficult to be altered or forged. It uses five anti-counterfeiting techniques, including digital photos, holograms, optically variable inks, ghost photos, and digitally- printed information [49].

The development of advanced technology gives identity new and secure features to prevent ID theft. However, criminals can also take advantage of technological advances to steal identity and commit fraud. The result is a never-ending race between industry, in developing new security features for identity, and criminals attempting to compromise the technology and commit fraud.

7.1.3 Prevention Mechanisms

Effective mechanisms for preventing ID theft and abuse are often low cost. For example, internal theft is a major threat to identity information held by ID issuers and checkers. Internal screening and managerial mechanisms can minimize the risk of insider identity theft [44]. Online banks can remind consumers to prevent online spoofing and phishing by refusing to provide sensitive information when it is requested online. For example, the Industrial & Commercial Bank of China informs customer on its online homepage that the bank will never request an account number and password from a customer at any time by email, letter or telephone, except when the customer is logging in to its officially authorized site [50]. To prevent sensitive identity information exposure, credit bureaus and banks have stopped printing SINs and other identifying numbers on hard copy reports mailed out to customers, since the SIN is favored as a file identifier. Relevant laws, discussed in section 7.3, can prevent internal identity information theft by restricting their disclosure within the organization.

ID abuse can also be effectively prevented by other mechanisms. For example, the Canadian government has tightened its requirements for obtaining passports and SINs in order to prevent fraudulent applications. Illegal intrusion into identity information databases should result in immediate notification to affected consumers, to limit the ability of ID thieves to misuse any stolen personal information. In the U.S., certain laws have been enacted to require companies to warn customers of security breaches [44]. Certainly, it is not sufficient just to have a good policy in place to prevent ID theft. Front-line workers must also be trained, and proper procedures must be in place to implement the policy.

Although there are many ways to prevent ID theft, more research is needed to identify the techniques that work best in each particular circumstance. ID theft prevention education should also be encouraged and extended to more institutions and countries in order to broaden its impact on the public. Identity protection technologies, such as biometrics, digital certificates, and smart cards must continue to evolve and improved. More work needs to be done on technological

solutions, including their implementation, processes, policy, and management and control of data after it is collected.

7.2 Identity Theft Detection

Identity theft detection activities try to detect ID theft when or after it happens. ID theft is often not detected until long after it has occurred and has resulted in severe damage. The average time between the identity theft event and the date of discovery is 12 months, and the FTC reports that some ID theft victims were unaware of the theft for as long as 5 years [51]. The late detection of ID theft greatly increases the victim's potential for loss. Early detection of ID theft will clearly reduce potential loss. In addition, detection of ID theft can provide evidence that is essential to prosecute criminals.

ID owners, issuers, checkers, and protectors detect ID theft in various ways, as shown in Figure 6. Identity owners can detect ID theft by regularly checking their personal and financial information. ID issuers and checkers can detect attempted masquerades by strict authentication mechanisms, aided by advanced authentication technologies and other effective measures. ID protectors detect, pursue, and prosecute ID thieves.

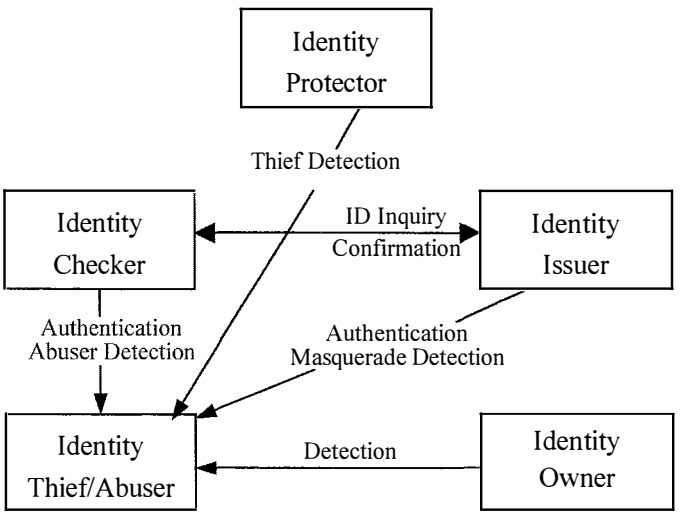

Figure 6. Identity Theft Detection Activities

Restrictive authentication is the key way to detect ID abuse. The general identity authentication process can be divided into three steps: identification, verification, and authentication. Identification checks personal information such as name, physical attributes or credentials such as social security cards, driver's licenses, passports, etc. Verification proves whether the credentials are genuine. The final step, authentication, associates an individual with a unique identifier, such as a password, physical token, or biometric attribute (fingerprint, voiceprint, retinal scan, etc.) that establishes the individual's identity as genuine [11]. Basically, online identity authentication is the same as any paper-based system [52], except that online authentication cannot check the physical attributes of the ID holder directly, and all the documents used are electronically formatted.

With restrictive authentication mechanisms and authentication technologies, ID issuers and checkers can detect potential theft at each step of the authentication process. For example, an imposter can be detected if signature or physical attributes (e.g. photo) do not match the identity document, when it is checked. Advanced technologies, such as biometrics, smart card technology, and PKI, as discussed in section 7.1.2, can also help to detect theft. For example, fingerprint scanning and matching at international customs entry ports can greatly increase the chance of detecting false visas and passports.

Some measures are also effective in detecting ID theft after it happens. Credit card fraud accounts for the greatest proportion of ID fraud, according to FTC statistics. Credit card providers monitor account activity with a view to identifying abnormal transactional patterns that suggest fraud. If such patterns are detected, cardholders are contacted in order to confirm transactions or to identify potential fraud at an early stage. Credit bureaus offer a number of services to help in fraud detection, including access to databases of potentially fraudulent information, and alerts to credit grantors of mismatches between input information and information on file. Credit card agencies allow merchants to verify the billing name and address of consumers who are presenting credit cards for payment on the Internet, or for mail order or telephone order purchases [1].

To prosecute criminals, law enforcement agencies must be able to gather evidence of criminal activities by the ID thief. ID thieves can be detected and their identities can be captured by monitoring measures when they use fake ID to obtain a certain right or financial benefit. For example, cameras can be used to monitor ATM users. However criminal evidence is difficult to gather in certain situations, such as data fraudulently copied from a database.

Early detection is critical to protect victims from heavy loss, and much more research is needed on ID theft detection. For example, comprehensive authentication processes must be developed and used to detect most instances of ID theft. The authentication process includes, not just adoption of the appropriate technologies, but proper training and management of front-line employees.

7.3 Legal Protection and Criminal Prosecution

If ID theft is not prevented, victims have to rely on protectors, issuers, and checkers to apprehend and punish the criminals and to recover their losses. Business victims also have to alert consumers of breaches that may result in illegal use of the their identities. The relationships among protector, checker, issuer, owner, and identity thief are depicted in Figure 7.

Certain laws have been enacted specifically to protect identity owners and relevant personal information and to punish ID thieves. In 1998, the U.S. Identity Theft and Assumption Deterrence Act was passed. This ensures that private consumers who fall victim to identity theft can stand as victims in federal criminal cases and force the courts to consider damage to these consumers by including them in restitution orders. The Act provides for stiffer penalties for perpetrators of this crime and implements certain procedures for investigation and enforcement as well [3]. In January 2001, PIPEDA (Canadian Personal Information Protection and Electronic Documents Act) was passed to protect personal information. This Act requires that organizations must protect personal information against loss or theft as well as unauthorized access, disclosure, copying, use, or

modification. The level of security should be appropriate to the sensitivity of the information. People with access to the information must sign confidentiality agreements [53]. For example, the U.S. Driver Privacy Protection Act makes it unlawful (subject to some exceptions) to disclose or obtain personal information from a motor vehicle record unless the subject expressly consents to such disclosure [54].

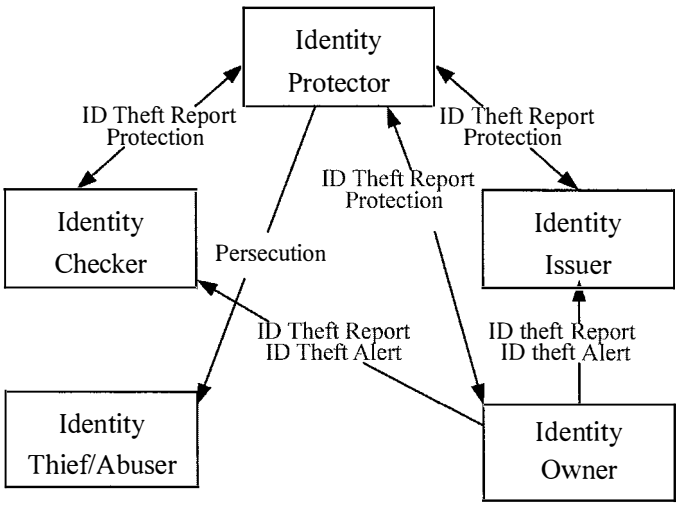

Figure 7. Legal Protection and Prosecution Activities

Although, as we have indicated, there are some laws that are specifically related to ID theft, stronger protection laws are needed in many jurisdictions for the protection of identity and victims, and to provide for criminal prosecution when such information is stolen and/or abused. For example, ID owners should be given certain rights to check their personal and financial information that is held by various institutions, in order to detect ID theft. In order to prevent identity information exposure, consumers should have the right to refuse to provide personal information that is not necessary for the requested service or transaction, without being denied the service or transaction in question, and without a reduction in the quality of service they receive. Excessive information requirements and illegal information use should be explicitly forbidden by law. Related laws should protect business victims of ID theft. However, strong laws are of little use if law enforcement agencies do not use them or don't have the resources to enforce them. Law enforcement agencies should therefore be given the resources needed for ID theft investigation, and the prosecution of related offences. Law enforcement agencies also must cooperate with their counterparts in other agencies and jurisdictions (including other nations) in order to pursue and convict identity thieves under existing criminal laws.

Finally, we summarize major interactive activities involved in combating ID theft in Table 3. Existing issues and prior potential research are also indicated in this summary table.

Table 3: Existing Issues and Potential Research in Combating ID Theft

Major Activities	*Tasks*	*Techniques*	*Issues*	*Potential Research*
Information Collection	Authentication		• ID exposure • ID information Databases	• Privacy protection
Identity Fraud				• Further analysis
• Identity theft	ID Loss	• Traditional direct ✓ ID certificate ✓ ID information • Online ✓ ID information	• Online theft	
• Identity counterfeiting	Fake ID	• Counterfeit ✓ ID certificate	• IT aided counterfeiting • Low cost • Easy access techniques	
• Identity abuse	Damage	• Impersonation	• Credit card fraud • Travel document abuse	
Combating ID theft				• Risk management • Multiparty coordination
• Prevention	Prevent ID theft before it happens	• Education and Guidance ✓ ID Theft • Prevention technology ✓ ID counterfeit ✓ ID abuse ✓ ID theft • Prevention mechanisms ✓ ID theft ✓ ID abuse	• Effectiveness • Application • Improvement	• Cost/benefit analysis
• Detection	Detect ID theft when or after it happens	• Restrictive authentication ✓ When it happens • Abnormal transaction patterns ✓ After it happens • Criminal evidence ✓ After it happens	• Front-line employees	
• Protection and Prosecution	Protect victims and prosecute criminals	• Legislation • Law enforcement	• Stronger protection laws • Law enforcement • Resources, cooperation	

8. CONCLUSIONS AND FUTURE RESEARCH

Within the framework described in Figure 1, we have systematically described an overall view of combating ID theft, including the roles and responsibilities of each stakeholder, and interaction activities among them. Many issues were revealed in the discussion of the framework that need to be addressed by further research. In the following section, we propose some potential research directions, including ID theft risk management, cost and benefit analysis of countermeasures, multiparty coordination, and privacy protection issues.

8.1 Risk Management

ID theft is a risk that businesses must manage. Unfortunately, most organizations do not know how

to manage the risk and, if they do, they do not put enough effort into it. Although our theoretical framework can help to clarify issues in the ID theft problem, an action plan to combat ID theft needs to be built on more general principles. Risk management is one such concept that would be very useful, to establish proper security policies and strategies to combat ID theft.

Risk management is the systematic application of management policies, processes, procedures, and technologies to the tasks of identifying, analyzing, assessing, treating, and monitoring risk [55]. The objective of risk management is to protect assets from all external and internal threats so that the costs of losses resulting from the realization of such treats are minimized [56].

Risk is determined by three primary factors including assets, threats, and vulnerabilities. After identifying a risk, the risk assessment process measures the risk by identifying and evaluating assets, identifying threats, and identifying vulnerability. Assets represent anything of value that is worth securing, such as identity, that can be relied on to access valuable services and privileges. Threats, which are any eventualities that represent a danger to an asset, can arise through any possibilities resulting in the theft of identity and relevant information that may be stolen, such as identity information exposure during an authentication process. Vulnerabilities are weaknesses existing in the identity safeguard system. A risk management strategy is developed on the basis of information derived from the risk assessment process. Countermeasures are then selected to prevent the assets from possible threats, depending on the relative likelihood of each threat. Based on this analysis, relevant security policies can then be developed to reduce all potential threats and vulnerabilities, in order to successfully reduce the overall risk of ID theft. Moreover, business managers must be given the information needed to separate acceptable and unacceptable risk events in the process of risk assessment. Resources are then invested rationally in order to prevent unacceptable and high probability risk events that can have a high impact on the business. Risk events with low probability and low impact are normally ignored.

It is important to study how to apply risk management in the context of combating ID theft, considering such aspects as ID theft risk assessment and security policy development and implementation. However, there has been little or no such research in this area. Research of this nature could provide answers for many questions. For example:

(1) What are the three risk factors in ID theft? Our framework would be very helpful in ID theft risk assessment, in identifying possible threats and vulnerabilities that exist in every aspect of ID theft risk management.
(2) What are acceptable and unacceptable risk events in ID theft? How should they be evaluated?
(3) What approach should be used to establish a practical and rational strategy for combating ID theft through the risk management concept? How should countermeasures and security polices for combating ID theft be evaluated and selected?

8.2 Cost and Benefit Analysis of Countermeasures

It is imperative to analyze costs and benefit of all kinds of ID theft countermeasures in order to achieve a reasonable and effective approach to security management. For example, PIN numbers

are used in the credit card authentication process in China. The cost and benefit analysis of this PIN or password countermeasure needs to be done in order to evaluate its cost and effectiveness in enhancing credit card security management. This would be helpful in determining if this measure could be adopted in the North American credit card system. The cost and benefit analysis of some new technologies, such as biometric and smart card technology, can also foster broader technical applications. Such financial analyses appear to be relatively rare for ID theft countermeasures. Research is needed in this area. For example:

(1) The effectiveness of ID theft countermeasures should be analyzed. For example, it appears that fingerprints will soon be used in US visas and passports [41] in order to more accurately identify ID owners and block ID abusers, especially terrorists. It is necessary to analyze the effectiveness of this biometric solution for combating ID theft, including the expected percentage of ID theft reduction through this solution.
(2) What are the direct and indirect costs of ID theft countermeasures? What is the ROI of each existing or potential technical solution? The U.S. has invested $380 million for fiscal year 2003 and more than $330 million for fiscal year 2004 in their new biometric US-VISIT (United States Visitor and Immigrant Status Indicator Technology) program [57]. These data show the direct cost of this program, but what are its indirect costs? How effective is this fingerprint-checking system in detecting terrorists? What is the ROI of the program?
(3) What are the cost and effectiveness of possible credit card ID theft prevention solutions, such as adding the owner's photo on the credit card or using a PIN or password in the credit card system?
(4) How can data be collected in order to analyze the costs and benefits of an ID theft countermeasure?

8.3 Multiparty Coordination in Combating ID Theft

The success in combating ID theft relies on joint efforts and coordination among all stakeholders, such as the ID owner, ID issuer, ID checker, and ID protector, in every relevant activity, such as prevention, detection, and prosecution. For example, in the process for issuing US biometric visas, fingerprints of the applicant are electronically compared with fingerprint records in criminal databases [58]. This comparison process requires coordination between the visa issuer (consular posts abroad) and protectors (DHS: Department of Homeland Security; FBI). Multiparty coordination among owners (fraud reports), issuers (status of credit cards), checkers (abuses), and protectors (investigation and prosecution), is also necessary in ID theft prosecution procedures.

Multiparty coordination is essential in combating ID theft. Many such coordination activities should be considered in various aspects of combating ID theft in the future. For example:

(1) In order to effectively block ID abusers (such as terrorists) through the US biometric visa and passport program, broad and deep coordination is required among all involved parties. For example, every consular post abroad and every landing port must install and operate the fingerprint-scanning device for issuing and checking visa. In addition, databases of criminal fingerprints in different countries must be linked with all such databases in the US in order to effectively prevent terrorists from crossing the border.
(2) International cooperation is required in combating ID theft. If US biometric visa or

passport abusers have not committed a crime in the United States, their criminal records could be in the archives or databases of their home countries. An effective biometric terrorist defense system requires a worldwide network that supports online fingerprint matching. Otherwise, the effectiveness of such a biometric system would be questionable.

(3) Coordination in credit card authentication should be studied to determine if it is more effective in combating online credit card theft by matching credit card records in various ID theft databases, such as the *Consumer Sentinel* or *PhoneBusters* databases.

8.4 Privacy Protection

Identity authentication requires identity presentation and the collection of identity information. However, excessive and inappropriate collection without the owner's consent may result in privacy violations and damage to customer trust, effectively driving customers away from the business [59]. In addition, applications of new technology for authenticating identity may bring privacy problems that will impact consumer acceptance. For example, potential abuses of biometric information such as tracking individuals and their transactions without their consent, are of concern with individual privacy violation [60] in the new US visa and passport application program.

Privacy protection should prevent non-permitted, illegal, and/or unethical use of private information [59]. Privacy protection must be balanced against the collection of identity information for authentication. Many organizations and governments are trying to deal with this issue, and laws have also been passed that attempt to address the problem. For example, the PIPEDA legislation bestows upon individuals the right to know what personal information about them has been collected, how it is being used, to whom it has been disclosed, and the ability to challenge the accuracy and completeness of the information and have it corrected (PIPEDA, 2004). However, this Act alone is not enough to address the privacy protection problem. More research is required on the relationship of identity management and the protection of personal privacy.

Combating ID theft requires a continuing effort among all the stakeholders involved. Research on ID theft is urgently needed if the rise in ID theft incidence is to be stopped. We hope the framework proposed in this paper will help to further that effort.

REFERENCES

[1] P. Lawson, J. Lawford, Identity Theft: The Need for Better Consumer Protection, Public Interest Advocacy Centre, Ottawa, Canada, November 2003, http://www.piac.ca/IDTHEFT.pdf.

[2] United States General Accounting Office, Identity Theft, Prevalence and Cost Appear to be Growing, March 2002, pp. 8-51, http://www.gao.gov/new.items/d02363.pdf.

[3] K. M. Saunders, B. Zucker, Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act, *International Review of Law Computers & Technology*, Vol. 13, No. 2, 1999, pp. 183-192.

[4] Federal Trade Commission, Identity Theft Survey Report (Synovate), September 2003, http://www.ftc.gov/os/2003/09/synovatereport.pdf .

[5] PhoneBusters, Statistics on Phone Fraud: Identity Theft Complaints, July 12, 2004, http://www.phonebusters.com/english/statistics_E03.html.

[6] Ontario Ministry of Consumer and Business Services, Keep Your Identity Safe: What you need to know to protect yourself, 2004, http://www.cbs.gov.on.ca.

[7] Federal Trade Commission, National and State Trends in Identity Theft, January-December 2002, January 22, 2003, p. 9, http://www.consumer.gov/sentinel/pubs/Top10Fraud_2002.pdf.

[8] Federal Trade Commission, National and State Trends in Fraud and Identity Theft, January-December 2003, January 22, 2004, http://www.consumer.gov/sentinel/pubs/Top10Fraud2003.pdf.

[9] Federal Trade Commission, Report – FTC Overview of the Identity Theft Program, October 1998-September 2003, September 2003, Fig. 1, http://www.ftc.gov/os/2003/09/timelinereport.pdf.

[10] Gartner Inc., Gartner says identity theft is up nearly 80 percent, *News Release*, July 21, 2003.

[11] S. Marlin, Personal Protection, *Bank Systems & Technology*, New York, Vol. 40, Issue 6, June 2003, p. 26.

[12] A. Cavoukian, *Identity Theft: Who's Using Your Name?* Information and Privacy Commissioner (IPC), Ontario, June 1997.

[13] Federal Trade Commission, Understanding Identity Theft, July 10, 2004, http://www.consumer.gov/idtheft/understanding_idt.html#1.

[14] M. Frank, Identity Theft: Who's Helping the Innocent Victims?, White-Collar Crime Fighter, May 1999, http://www.identitytheft.org.

[15] Privacy Commissioner of Canada, Fact Sheet-Social Insurance Number, July 9, 2004, http://www.privcom.gc.ca/fs-fi/02_05_d_02_e.asp.

[16] R. Forno, W. Feinbloom, PKI: A question of trust and value, Association for Computing Machinery, *Communications of the ACM*, New York, June 2001, Vol. 44, Issue 6, p.120.

[17] Y. Suzuki, Panasonic System Solutions Company, Matsushita Electronic Industrial Co., Ltd., Personal Identification Techonologies on Ubiquitous World, *AIC (Asian Info-communications Council) Conference*, 1st - 5th December 2003, Tokyo, Japan.

[18] K. Poulsen, Wardriver pleads guilty in Lowes Wi Fi hacks, *SecurityFocus*, June 4, 2004, http://www.securityfocus.com/news/8835.

[19] B. Sullivan, Study: ID theft usually an inside job, *MSNBC,* May 21, 2004, http://msnbc.msn.com/id/5015565.

[20] ConsumerSentinel, Consumer Sentinel: The Cybertool for FraudBusters, April 17, 2003, http://www.consumer.gov/sentinel/about.htm.

[21] PhoneBusters Website, June 10, 2004, http://www.phonebusters.com/english/aboutus.html.

[22] M. Hume, Identity Theft Cited as Threat After Equifax Security Breach, March 17, 2004, http://www.theglobeandmail.com.

[23] S. Tuck, Mob role suggested in theft of SINs, other data, *Globe and Mail*, May 27, 2003, p. A4.

[24] J. E. Matejkovic, K. E. Lahey, Identity theft: no help for consumers, *Financial Services Review*, Elservier Science Inc., 10 (2001), pp. 221-235.

[25] Federal Trade Commission, Fraudulent Email Seeks to Capture Consumer Information, June 24, 2003.

[26] Hulme and Claburn, Tiny, Evil Things, *Information Week*, April 26, 2004.

[27] S. Gardiner (IC: Industry Canada), Confidential: Not For Release or Distribution, ORNEC Workshop, February 11, 2004, Ottawa, Canada.

[28] The US Census Bureau, Retail 2Q, 2004 E-commerce Report, August 20, 2004, http://www.census.gov/mrts/www/current.html.

[29] The Ottawa Citizen, Canadians warm to online shopping, January 14, 2003, p. D1.

[30] D. McClellan, Desktop counterfeiting, Technology Review, Cambridge, February 1995, Vol. 98, Issue 2, p. 32.

[31] Center for Immigration Studies, America's Identity Crisis Panel Discussion Transcript, Cannon House Office Building, Washington, DC, May 14, 2002, http://www.cis.org/articles/2002/idpanel.html.

[32] Digimarc Corporation, Combating Identity Document Counterfeiting: A Digital Watermarking Capabilities Paper, 2003, http://www.digimarc.com/docs/Combating%20Identity%20Document%20Counterfeiting.pdf .

[33] M. A. Gips, The Spurious and the Injurious, *Security Management*, December 2003, Vol.47, Issue 12, p. 66.

[34] Royal Canadian Mounted Police, Counterfeiting and Credit Card Fraud, June 23, 2004, http://www.rcmp.ca/scams/ccandpc_e.htm.

[35] National Crime Prevention Program, Identity Theft Prevention Kit, Government of Australia, 2003, http://www.ema.gov.au/www/rwpattach.nsf/viewasattachmentPersonal/682ECB6BB9B6B0C7CA256E3C001F8180/$file/ID%20Theft%20Kit.pdf.

[36] A. Cavoukian, Consumer Biometric Applications: A Discussion Paper, Information and Privacy Commissioner (IPC), Ontario, 1999.

[37] D. Coderre, Minister of Citizenship and Immigration, at the forum: Biometrics: Implications and Applications, Ottawa, October 8, 2003.

[38] G. Roethenbaugh, Biometrics Explained, Section 1- An Introduction to Biometrics and General History, December 29, 1998, http://www.icsa.net/services/consortia/cbdc/sec1.shtml.

[39] C. Prins, Biometric Technology Law: Making our body identify for us: Legal implications of biometric technology, *Computer Law & Security Report*, Vol. 14, No. 3, 1998, p. 160.

[40] G. Radwanski, Privacy Commissioner of Canada, to the Standing Committee on Citizenship and Immigration, March 18, 2003, http://www.privcom.gc.ca/speech/2003/02_05_a_030318_e.asp.

[41] U.S. Department of State, Safety & Security of U.S. Borders (Biometrics), August 18, 2004, http://travel.state.gov/visa/biometrics.html.

[42] MapleLeafWeb, National Identity Cards – The Next Step: Canada Looks to Biometrics to Fight Terrorism, April 11, 2003, http://www.mapleleafweb.com/features/privacy/id_cards/cards.html.

[43] CBC, The National – CBC Television, Threats lead US to take unprecedented security measures, Toronto, November 13, 2002.

[44] D.C.G. Brown, G. Kourakos, Public Policy Forum (PPF) Roundtable on Identity Theft and Identity Fraud, June 26, 2003, Ottawa.

[45] K. Krebsbach, Making Cyberspace A Safer Place to Roam ; Do IT executives have enough on their plate?, *Bank Technology News*, New York: June 1, 2004. Vol. 17, Issue 6, p. 22.

[46] SmartCardAlliance, Smart Cards Are a Strong Link in the Chain of Trust for ID Systems, March 9, 2004, http://www.smartcardalliance.org/industry_news.

[47] W. Kou, S. Poon, E. M. Knorr, *Smart Card and Application, In Payment Technologies for E-Commerce*, Weidong Kou (eds.), Springer, 2003, p. 95.

[48] R. G. Smith, Identity-related Economic Crime: Risks and Countermeasures, In Trends and Issues in Crime and Criminal Justice series, Adam Graycar (eds.), Australian Institute of Criminology, September 1999, http://www.aic.gov.au.

[49] Canadian Passport Office, Features of the Canadian passport, August 4, 2004, http://www.ppt.gc.ca/passports/book_e.asp.

[50] Industrial & Commercial Bank of China, How to secure your online transaction, May 27, 2004, http://www.icbc.com.cn/guanggao/040601/zyts.htm.

[51] Federal Trade Commission, National and State Trends in Identity Theft, January - December 2000, January 22, 2001, p. 4, http://www.consumer.gov/sentinel/pubs/Top10Fraud_2000.pdf.

[52] Office of the Corporate Chief Information Officer, Government of Ontario, Discussion Paper on Identity Authentication and Authorization in Electronic Service Delivery, May 5, 2003, http://www.gov.on.ca/MBS/english/fip/pub/index.html.

[53] Personal Information Protection and Electronic Documents Act (PIPEDA), PIPEDA Overview – What, July 1, 2004, http://privacyforbusiness.ic.gc.ca/epic/internet/inpfb-cee.nsf/en/hc00005e.html.

[54] D. Christensen, Major Information Brokers face class action for invasion of privacy, *Miami Daily Business Review,* June 24, 2003.

[55] A. R. Bowden et al., *Triple Bottom Line Risk Management*, John Wiley & Sons, Inc, Canada, 2001, p.15.

[56] K. Bandyopadhyay et al, A Framework for Integrated Risk Management in Information Technology, *Management Decision*, London, 1999, Vol. 37, Issue 5, p. 437.

[57] Electronic Privacy Information Center, US-VISIT: United States Visitor and Immigrant Status Indicator Technology, July 29, 2004, http://www.epic.org/privacy/us-visit/.

[58] M. Harty, A Look at the Goals and Challenges of the US-VISIT Program, March 4, 2004, http://travel.state.gov/visa/testimony12.html.

[59] M. Head and Y. Yuan, Privacy protection in electronic commerce --- a theoretical framework, *Human System Management*, 20(2001), pp.149-160.

[60] S. Prabhakar, Biometric Recognition: Security and Privacy Concerns, *IEEE Security & Privacy*, March/April, 2003, pp. 33-42.


McMaster
University
LIBRARIES

McMaster eBusiness Research Centre (MeRC)
DeGroote School of Business
McMaster University
1280 Main St. W. MGD A201
Hamilton, ON
L8S 4M4

Tel: 905-525-9140 ext. 27027
Fax: 905-528-0556
Email: ebusiness@mcmaster.ca
Web: http://merc.mcmaster.ca