The Dynamics of Identity Theft:

A Comparison of Symptomatic and Systemic Solutions

Mary Lou Garber Bourne

A thesis submitted to the Graduate Faculty of

JAMES MADISON UNIVERSITY

In

Partial Fulfillment of the Requirements

for the degree of

Master of Science

Department of Integrated Science and Technology

December 2004

Table of Contents

List of Figures

Dedication

This research is dedicated to the victims of identity theft, past and future. May this research augment existing works on the underlying causes driving identity theft in today’s society and help broaden our thinking as we consider effective solutions to the identity theft problem.

Acknowledgments

I deeply appreciate the dedication of my advisor, Dr. Mike Deaton. His guidance, feedback, and encouragement were invaluable to the model building and writing process. I am grateful for his time and talent in stretching me beyond where I knew I could go.

I want to thank the faculty members who have inspired me with ideas to embark on this research; Dr. Ron Kander's direction on selecting a thesis topic and Dr. George Baker's innovative course on critical infrastructure and complex system failures. I am grateful to Mr. Ken Newbold of JMU's Institute for Infrastructure and Information Assurance and Mr. Bob Cofod, President of BankDetect, LLC for discussions in the early stages of my research. Mr. Cofod's wealth of work experience in intelligence and bank fraud detection provided an insightful connection to the real world. I would like to thank Dean Dr. Jerry Benson, program coordinator Dr. Barbara Gabriel, and ISAT faculty members for making the Integrated Science and Technology master's program possible and Ms. Mary Lou Cash for making the program run smoothly.

Without the support of my husband, Jeff, and my sons, Jason and Kyle, I would not have been able to dedicate the time and effort to this research. I thank them for their understanding, love, and support.

Abstract

Current policies for addressing identity theft are aimed at treating the symptoms of the crime epidemic by arresting thieves while largely ignoring the underlying dynamics driving exponential growth in the crime. The research described herein shows that strategy to address the identity theft epidemic that primarily focuses on prosecuting thieves without effectively mitigating the underlying forces is doomed to failure. The research employs the methodology of system dynamics to elucidate the dominant factors and dynamic relationships that contribute to this complex problem. A conceptual systems model is developed to explore why current policies are ineffective in addressing identity theft. The model suggests that the dominant forces behind the identity theft epidemic are found in an exploding credit economy, coupled with a business culture that plays fast and loose with consumer information, while experiencing almost no negative financial consequences. This culture creates a rapid-feedback, self-reinforcing dynamic that generates ample opportunities for would-be thieves. The systems model and analysis provide a theoretical system framework for characterizing the problem, thus a more rigorous justification for policy options.

Introduction

Identity theft, using another's personal identifying information in the fraudulent acquisition of goods or services, is broadly recognized to have reached epidemic proportions in the United States (Department of Justice, 2002, p. 2.42). It is one of the fastest growing crimes, victimizing an estimated ten million people in 2003 (Synovate, 2003, p. 7). Since 2001, identity theft has been the top consumer fraud complaint reported to the Federal Trade Commission (FTC), constituting more than 40 percent of total complaints (FTC Consumer Sentinel, 2004, p. 4). Cumulatively, there were an estimated 27 million victims in the U.S. in the five-year period 1998-2003 (Synovate, 2003, p. 12), and over 33 million since 1990 making approximately one in six adults in the U.S. a victim of identity theft (Givens, 2003, p. 3).

The effects of identity theft on the victim can be devastating, both psychologically and financially. As a result of identity theft, the victim's credit rating can be seriously damaged impacting his/her ability to obtain credit for the next several years. A 42-year-old retired Army captain's good name was ruined when an identity thief acquired goods valued at over $260,000 in the victim's name, including two trucks, a motorcycle and time-share property (Fleck, 2004). Traffic violations and murder have been committed using fraudulent names resulting in arrests and jail time for innocent victims of identity theft (Sullivan, 2004c, p. 43).

On a national scale, losses to businesses due to identity theft in the U.S. were estimated to be nearly 50 billion U.S. dollars in 2003 (Synovate, 2003, p. 7). Beyond the financial costs, identity theft impacts society by perpetrating drug trafficking, money laundering, and terrorism (Willox and Regan, 2002, p. 2). Identity theft played a role in the September 11, 2001 attacks on the United States. Two terrorists boarding the aircraft that fateful day had fraudulently obtained Virginia driver's licenses (Willox and Regan, 2002, p. 4). Additionally, Congressional testimony surrounding those attacks show identity theft as a major means of financing acts of terrorism (Sullivan, 2004c, pp. 77-78).

Identity theft has broad implications that threaten consumer confidence by eroding public trust in business transactions (Department of Justice, 2002, p. 2.42). Upon passing recent legislation, President Bush said, "The crime of identity theft undermines the basic trust on which our economy depends. Identity theft harms not only its direct victims, but also many businesses and customers whose confidence is shaken" (Lemke, 2004).

The United States enacted the Identity Theft and Assumption Deterrence Act in 1998 criminalizing identity theft. In 2004, stiffer penalties were added to the law for all crimes committed that involve identity theft (Sovern, 2003, p. 350; Lemke, 2004). Although federal laws were passed in 1999 (Gramm-Leach-Bliley Act) and 2001 (U.S.A. Patriot Act) intending to safeguard consumer information and verify customer identification, identity theft has continued to grow exponentially over the last five years (Sullivan, 2004c, pp. 169–176). Privacy rights groups in California urge that more needs to be done to prevent identity theft:

> (L)egislation must be enacted to require creditors and credit bureaus to improve their credit-granting and complaint-handling practices. Further, easy access to the bits of information that comprise a consumer's financial identity must be curtailed. Sloppy credit-granting practices by banks, department stores, phone services, and other creditors make the crime all too easy to commit. (Benner, Givens, & Mierzwinski, 2000, section V.)

The research described herein shows that any strategy to address the identity theft epidemic by primarily focusing on prosecuting thieves without effectively mitigating the underlying forces is doomed to failure. Current approaches for addressing identity theft largely ignore the epidemic as a systemic problem. The analysis in this thesis suggests policies and practices necessary to effectively address the growth in identity theft. A system-wide perspective is needed to fully understand the interactions and feedbacks of factors driving identity theft.

The research employs the methodology of system dynamics to elucidate the dominant factors and dynamic relationships that contribute to this complex problem. A conceptual systems model is developed to explore why current policies are ineffective in addressing identity theft. The model suggests that the dominant forces behind the identity theft epidemic are found in an exploding credit economy, coupled with a business culture that plays fast and loose with consumer information, while experiencing almost no negative financial consequences. This culture creates a rapid-feedback, self-reinforcing dynamic that generates ample opportunities for would-be thieves. Moreover, while consumers have the greatest short-term risks from identity theft, they have little ability to counter the problem because of significant feedback delays.

Similar findings can be found elsewhere in the literature (LoPucki, 2002; Solove, 2003; Sovern, 2003; Sullivan, 2004c). Some of these analyses are based on a synthesis of anecdotal evidence from victims and thieves (Benner et al., 2000; Sullivan, 2004c). Others base their findings on legal analyses of human identification methods (LoPucki 2002), data security practices (Solove, 2003), and the misallocation of costs incurred by identity theft (Sovern, 2003). This thesis provides a different perspective by providing a theoretical system framework for characterizing the problem by applying conceptual systems modeling techniques, along with some computer based simulations of certain system elements to provide a more rigorous justification for policy options.

Figure 1 provides a broad framework for exploring the identify theft problem. The diagram outlines the major elements of the problem, as identified in the literature. These elements (indicated by the square boxes in the figure) also correspond to the major system components (or ***sectors***) developed in the system model described in this thesis.

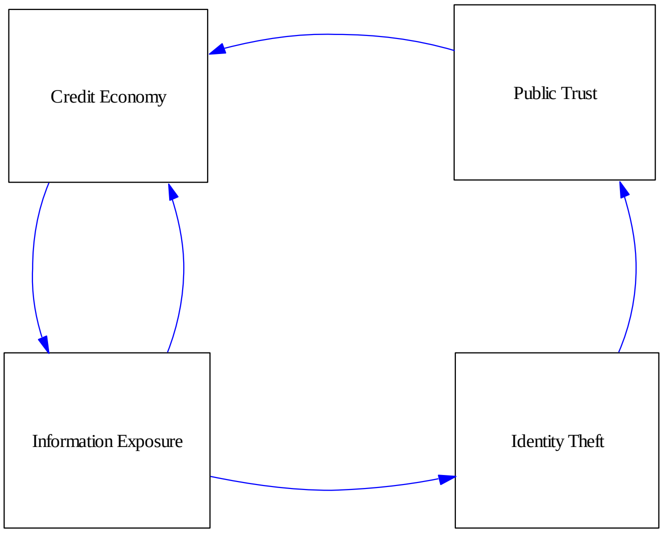


Figure 1: Overview of identity theft sector relationships

The ***Identity Theft*** sector represents the system elements of identity thieves and their victims. This sector also describes the dynamics created when aggressive prosecution of thieves is used in an attempt to curb the identity theft epidemic. The ***Information Exposure*** sector represents the dynamics leading to the increasing exposure of personal consumer information, much of which is then accessible both to businesses (who use the information to drive the credit economy) and to thieves (who use the information for identify theft and fraud). The arrow pointing from ***Information***

Exposure to ***Identify Theft*** indicates that the growth in information exposure provides opportunities for increased incidences of identify theft.

The ***Credit Economy*** represents credit-based transactions between consumers and businesses, and the processes by which those transactions are managed and validated. Within this sector consumers apply for credit in order to make purchases. As credit applicants provide their personal information on the credit application, the businesses or financial institutions then check the credit applicants' credit worthiness and either allow or deny the new credit accounts. Businesses, credit lending industry practices, and government policy allow new credit applicants fast and easy access to credit for quick sales, which keeps the ***Credit Economy*** rolling. A key player in this process is the credit reporting agency, which maintains credit lending and repayment transactions passed from businesses. These compiled transactions create an individual consumer's credit report. If the credit report generally shows no defaults in repayment history on other lines of credit, the applicant is deemed to be credit-worthy and granted an extension of credit to buy goods on account. Businesses enjoy higher revenues from increased credit sales in the growth of the ***Credit Economy*** sector as consumers are able to buy more goods instantly with a promise of future repayment.

Notice the two arrows between the ***Credit Economy*** and the ***Information Exposure*** sectors. These represent a feedback relationship: growth in the credit economy leads to increased personal information exposure, which in turn fuels further growth of the credit economy. This relationship exists because consumers divulge personal information in order to buy goods on credit, as represented by the arrow from the ***Credit Economy*** sector to the ***Information Exposure*** sector. The arrow pointing from the

Information Exposure sector to the ***Credit Economy*** sector represents businesses (defined as all financial institutions, merchants, and credit reporting agencies) exploiting consumer personal information by selling, buying, or sharing it in pursuit of new credit customers.

The rest of this thesis will use a system model to describe how these three sectors, ***Identify Theft***, ***Information Exposure***, and ***Credit Economy*** dynamically interact to create the identify theft epidemic. The model is then used to evaluate the potential impact of policies that primarily focus on catching identity thieves after the crime has been committed.

Figure 1 also includes a ***Public Trust*** sector, which describes the dynamics affecting consumer confidence in our nation's businesses and economy. The arrow pointing from ***Identity Theft*** to the ***Public Trust*** sector signifies shaken consumer confidence and concern for consumers' own financial well-being due to the growing number of identity theft victims. The arrow from ***Public Trust*** to ***Credit Economy*** signifies the dependence of the ***Credit Economy*** on the goodwill and trust of the public. That is, consumers make credit purchases from a business at least partly because they trust that their personal information is safe with that business. To the extent that this trust is eroded, the ***Credit Economy*** cannot continue to grow and flourish.

The dynamics underlying the ***Public Trust*** sector are explored only minimally in this thesis, and are used as a barometer of public tolerance for identity theft. In a worst case scenario, the erosion of public trust could lead to a collapse of the credit economy as consumers withdraw from participation in order to protect their personal information and financial liability. However, it is more likely that the erosion of public trust could lead to greater pressure on government and businesses to address the exponential growth in identity theft through effective policies and business practices. Many factors affect public trust besides the identity theft phenomenon (i.e. public perceptions about the health of the economy). Therefore, in this thesis, the dynamics in the ***Public Trust*** sector are defined only to the extent that is relevant to the identify theft problem.

The next section gives a general description of the process by which someone's identity is stolen and used for fraudulent transactions. Then the research literature is reviewed to provide a foundation for the dynamics implied in Figure 1. Next, an overview of system dynamics shows how that particular methodology is useful in exploring this problem. Lastly, the system model that comprises the core of this research effort is described. This model elucidates the dynamic relationships within and among the sectors in Figure 1. The model is validated with a comparison of historical data to the results from simulation runs of critical components of the model. In conclusion, simulation techniques and a qualitative examination of the feedback relationships implied by the model are used to evaluate the effect of current policies and to suggest approaches to curb the identity theft epidemic.

How Identity Theft Works

Identity theft involves a thief acquiring a victim's personal information, such as name, address, Social Security number, birth date, mother's maiden name, or credit card number, and using it to obtain goods or services for personal gain. An identity thief can be a stranger half-way across the country, on the other side of the world, or even a personal acquaintance of the victim.

The acquisition of personal information by an identity thief occurs through a growing variety of creative methods. Examples include physically stealing a wallet and making driver's licenses in the victims' name, calling customer service representatives claiming to be someone else in order to acquire personal information, or stealing information on-line.

Recent reports show increases in three methods of stealing personal information and/or funds belonging to others: (1) insiders (employees or employers who steal accessible personal information), (2) on-line banking fraud , and (3) mass-mailing electronic notes luring consumers to fraudulent Web sites that require updating personal information (Sullivan, 2004b; Fisher, 2004).

After obtaining another consumer's personal information, the thief may use it to buy goods or services on existing accounts (called account takeover) or to apply for a loan, open a bank or credit account, or sign up for a utility or cellular phone service in the victim's name (Benner et al., 2000). The thief is often successful in the application for credit because the Social Security number provided with the credit account application is checked with a credit reporting agency to verify the applicant's credit worthiness based on track record of repayment history. The credit checking process happens quickly, usually without matching other key pieces of information such as name, address, prior address, phone number or place of employment to verify the identity of the person presenting the information (Benner et al., 2000).

Once credit is extended to the thief, debts from fraudulent charges mount in the victim's name. The time lag between the fraud and discovery is crucial (Synovate, 2003, p.8). The longer the fraud goes undetected, the greater the financial losses to businesses and the more a victim's credit rating drops.

Every consumer who has a bank account, a credit card, or a loan has a credit rating that is a numeric score of the consumer's credit worthiness based on debt repayment history. This score is developed and maintained by a credit reporting agency, which provides this information to companies requesting verification of credit worthiness of a potential new customer. There are three major credit reporting agencies in the U.S. The first was established in 1899 to allow lenders a way to assess consumer credit risk before lending money (Sullivan 2004c, p. 115). When a consumer pays all bills listed under his name on time, he maintains a high credit rating with the credit reporting agencies. However, if someone steals the consumer's identity information and then accrues bills in that person's name, the consumer is unaware of the open accounts, and fails to pay. Hence, his credit rating drops (sometimes precipitously).

Therefore, the most devastating consequences of identity theft fall on the consumer who has no ability to prevent the crime and lacks control in clearing his/her name. Consumers as would-be victims have the most to gain by changes in business practices to prevent identity theft from happening. Businesses feel relatively little financial pain since losses are spread across all businesses accepting fraudulent charges (Sovern, 2003, p. 354). Unfortunately, businesses and credit reporting agencies lack incentives to make changes in the current instant credit extension practices (Sovern, 2003, p. 362).

Analysis of the Identity Theft Problem: State of Current Research

Although the media has helped increase public awareness of identity theft, there are relatively few scholarly works in this area. However, there is a sizeable body of research that lends insight to those factors that drive the identity theft problem. In order to synthesize findings from the literature, this section reviews that work within the context of the four sectors in Figure 1.

*The **Identity Theft** Sector: Findings from the Literature*

Survey statistics show that identify theft is growing exponentially. Catching those committing identity thefts is tough to do. It takes many hours of law enforcement effort to interview victims and others affected by the crime to build a case in order to prosecute thieves. Hence, identity theft is easy to commit and easy to get away with since there is little evidence linking the crime to a thief (Sullivan, 2004c). Legislation since 1998 has stiffened penalties for committing identity theft and bolstered law enforcement efforts to catch thieves. In spite of these efforts, the crime continues to grow exponentially. While this is a necessary part of fighting crime, efforts focused on catching and removing thieves from society are inadequate for reducing the exponential growth in identity theft – a fact that will be illustrated later via the system dynamics model for this sector.

Various surveys and personal victimization accounts substantiate the increasing incidence of identity theft. Of the total consumer fraud complaints formally filed with the FTC in 2003, 42 percent were identity theft incidents, up from 40 percent in 2002 (FTC Consumer Sentinel, 2004, p. 3). In a random telephone survey of over 4,000 adults, sponsored by the Federal Trade Commission in April 2003, 4.6 percent said they had been victims of identity theft in the prior year (Synovate, 2003, p. 4). This percentage applied across the entire U.S. adult population suggests that 9.9 million Americans were victims for the twelve-month period ending April, 2003 (Synovate, 2003, p. 7). The results parallel a separate study by Gartner Research surveying over 2,400 adults in May 2003 that estimated seven million victims nationwide (Litan, 2003a). The findings from both studies indicate that significantly more consumers are victims of identify theft than is suggested by the 214, 905 complaints formally filed with the FTC in the calendar year 2003 (FTC Consumer Sentinel, 2004, p. 4). The disparity between complaints filed and survey results suggest that many victims do not file a formal complaint with the FTC, leaving the crime largely unreported.

A survey conducted three years earlier by the California Public Interest Research Group and the Privacy Rights Clearinghouse compiled case studies from victims seeking support to recover from identity theft and found:

> …the failure of law enforcement, government, and the credit industry to address the root causes of identity theft. By not changing their procedures, these stakeholders have both helped perpetuate identity theft and have made it difficult for victims to resolve their cases expeditiously (Benner et al., 2000).

Based on Congressional testimony to the U.S. Senate Judiciary Subcommittee on Technology, Terrorism, and Government Information on the impact of identity theft, Givens (2000) argues for improved law enforcement efforts, changes in the credit industry business practices, protection of consumer rights, and help for victims to recover from identity theft.

Solove (2003) surmises that "…it is only recently that policymakers have turned their attention to identity theft, and the overwhelming approach in dealing with it has been to enact criminal penalties" (p. 19). The Identity Theft and Assumption Deterrence

Act, Pub. L. No. 105-318 (1998) recognizes identity theft as a federal crime. Before 1998, three states had passed identity theft legislation. By 2002, 44 states had statutes in place. Continuing this legislative trend, stiffer penalties for committing identity theft were enacted in July 2004 that makes helping terrorists acquire false identification a felony (Lemke, 2004).

In 2000, the last year reporting this statistic, there were only 5,807 identity thieves arrested by the Federal Bureau of Investigation (FBI), the Secret Service, and the U.S. Postal Service (Litan, 2003a). Based on roughly four million victims in 2000, it is estimated that thieves have a one in 700 (0.14 percent) chance of being caught by law enforcement (Litan, 2003c). Thieves leave little physical evidence identifying the culprit making identity theft cases difficult to prosecute (Sullivan, 2004c).

In late August 2004, the U.S. Attorney General announced the results of a three-month effort to crack-down on Internet fraud and identity theft. The collaborative law enforcement effort resulted in 103 arrests and 53 convictions that affected 150,000 victims who lost 215 million U.S. dollars (U.S. Department of State). This sting operation reflects the urgency to fight white collar crime as reported in the U.S. Department of Justice Strategic Plan for 2003-2008 (2.46). With this targeted and aggressive law enforcement effort, the prosecution rate was 51 percent, which is below the 58 percent prosecution rate for all federal crimes (U.S. Department of Justice Web site). Furthermore, statistics from this case show the impact that one identity thief can create hundreds or even thousands of victims in a relatively short period of time.

The National White Collar Crime Center, a federally-funded, non-profit organization supports law enforcement efforts of prevention, investigation, and prosecution of identity theft and other high-tech and economic crimes through a nationwide network established to help law enforcement agencies work across jurisdictions to catch thieves (Brown and Kane, 2002).

Law enforcement efforts to catch thieves are an essential part of battling identity theft. The predominant strategy of reducing identity theft through law enforcement efforts is referred to throughout this paper as “conventional wisdom.” Conventional wisdom describes prevailing public policies that concentrate on catching more thieves through law enforcement efforts and removing thieves from the system by sentencing and prosecuting to curb the identity theft epidemic. This approach is necessary, but not sufficient. It defines the problem of identify theft as a harm to individuals by criminals (Solove, 2003). Furthermore, conventional wisdom leads to policies that deal with the symptoms of the problem, not the underlying causes. Similarly, when you are sick, you go to a doctor to find out what is wrong so that you can become healthy again. Your symptoms need to be treated so that you feel better, but ultimately, you want to know what made you sick so you can prevent getting sick in the future. Treating the symptoms alone is not enough when the underlying cause is still present and the sickness could return and spread to others. Conventional wisdom will be described in more detail later as part of the ***Identify Theft*** sector of the system model.

*The **Information Exposure** Sector: Findings from the Literature*

Instances of personal information exposure refer to any activity that takes a consumer’s personal information out of his/her control. The literature shows that businesses play fast and loose with consumers’ personal information through lack of adequate security and buying and selling it for competitive advantage and financial gain.

The “***Information Exposure***” sector includes those system dynamics that lead to an ever increasing level of exposure of personal information as more and more consumer information is collected and used by businesses. As a result, personal information is easily accessible making it vulnerable for exploitation by perpetrators.

Personal information is exposed over time and in many ways so that it should no longer be considered private (i.e. only known by the true owner of the information). Simply knowing the information or possessing documents stating an identity can no longer be relied upon for proving an identity (LoPucki, 2002).

Literature referencing the ***Information Exposure*** sector ranges from discussion of consumers and businesses protecting personal information to those views recognizing that personal information is, and will continue to be, publicly available. In the latter view, Willox and Regan (2002) assert that false identification documents are easy to create and use based on widely available personal information. To counteract the prevalence of using false identifying documents, they propose a knowledge-based authentication system to support identify verification at the time a would-be thief or legitimate consumer seeks credit. According to this approach, a statistically-based model would score the applicant’s answers to questions (i.e. past addresses and phone numbers at a specified point in time) that should only be known by the true owner of the identity. Their research underscores the need for identity theft prevention at the point of application for credit.

LoPucki (2003) argues that personal identifying information such as Social Security numbers and mother’s maiden names of living Americans are already in private hands so that concealing them now will not reduce identity theft (p. 54). He advocates a government controlled, public database of personal information maintained voluntarily by individual consumers to allow them to have a stronger role for consumer awareness and participation in controlling use of personal information. LoPucki (2002) states that the geometric growth in identity theft is a result of the lack of effective defenses in the consumer credit system (p. 3). Based on his research and knowledge in the academic science field of human identification, he contends that solutions to identity theft should focus on the correct identification of credit applicants. He argues that the identity theft problem is not caused by thieves having access to personal information, but rather by creditors and credit reporting agencies having little incentive to properly identify individuals applying for credit (LoPucki, 2002, p. 9).

Sovern (2003) critiques the credit industry and the laws that govern the credit reporting agencies. He upholds that businesses granting credit to consumers and credit reporting agencies have the greatest power to prevent identity theft and the most knowledge about systems for granting credit, yet they lack legal and financial incentive to prevent identity theft (p. 375). He proposes changes necessary in credit industry laws such as requiring businesses to verify the identity of the credit applicant and more careful processing of pre-approved credit applications.

Businesses depend on, collect, process, and store an ever-increasing amount of personal information on employees and customers (Solove, 2003, p. 18). In 2000, there were 550 billion web-connected documents of which 95 percent were publicly available. By 2003, the volume had more than tripled (Lyman and Varian, 2003). The advent of electronic commerce (e-commerce) in 1999 as a means of conducting business transactions and purchasing goods spurred the move to Internet-based applications and a profusion of servers storing Internet-accessible information (Turban, Rainer, and Potter, 2003).

A consumer's Social Security number is the personal identifier used in financial and business transactions with employers, banks, creditors, businesses, and medical records. This federally assigned number has become the main matching mechanism in financial relationships between creditors and consumers. Matching is used as the process to link identifying information on a consumer across organizations (LoPucki, 2002, p.13). In order to match records, the identifying information must exist in system records on both sides of the match. However when Social Security numbers were first issued in 1936 to track employee wages and Social Security benefits, they were not intended to become a national identifier (Solove, 2003, p. 24). As businesses and organizations have grown and become increasingly automated over the last 30 years, Social Security numbers have been used widely and freely as convenient, easy to remember personal identifiers and pass codes to prove identities for all types of business transactions.

Exposure of personal information creates a wealth of data available to identity thieves via the Internet, a bank teller, a telephone customer service representative, or a payroll manager's desk (Sullivan, 2004a). When a consumer applies for credit, he/she divulges certain key elements of personal information, such as name, Social Security number, and address in exchange for instant credit and immediate purchase of goods or services. Businesses and credit reporting agencies sell personal information to other businesses for target marketing purposes to solicit new credit customers.

With a Social Security number, a name, and an address, a credit check with one of the three major credit reporting agencies (also called credit bureaus) is made quickly to see if the consumer is worthy of repaying the debt based on the consumer's credit rating. When any retailer, landlord, or utility company requests a consumer credit file from a credit reporting agency, current credit reporting industry standards allow the agency to match only two of the following four characteristics on the consumer's file: the consumer's (1) name, (2), Social Security number, (3) birth date, (4) account number with the creditor (LoPucki, 2002, p. 25). The credit check is done instantly so the consumer does not have to wait, therefore having the opportunity to change his/her mind on making the purchase.

Litan, reporting for Gartner Research on information technology issues related to identity theft, states that identity theft prevention efforts should focus on stopping fraud at the source, businesses that extend credit (Litan, 2003d). She asserts that financial businesses in the credit economy should not depend on government actions to solve the problem of consumer information exposure and law enforcement. "By denying credit to identity thieves, financial firms will likely leave them no incentive to commit the crime"(Litan, 2003d, p. 2).

Others address the need for businesses to act responsibly by protecting personal information and accepting accountability for potential security breaches. Security breaches, exposure of personal information in a broad sense, occur by thieves stealing information from a business database (hacking) or by employees abusing access privileges to personal information. Solove (2003) asserts that the identity theft finds its root cause in businesses that fail to protect personal information, which in turn enables thieves to have easy access to data. He proposes control over data security practices and consumer participation in collection and use of personal information.

Congresswoman Feinstein of California proposed federal legislation (S.1350, Notification of Risk to Personal Data Act, 108th Cong., 1st Sess. 2003) requiring businesses to inform consumers when their unencrypted personal information had been compromised in a security breach and exposed to perpetrators. Examples of information exposure are evident in the number of security breaches in the past several years exposing millions of customer and employee records (Clark, Goodyear, & Updegrove, 2003; Jewell, 2004b; Krim, 2003; Kucher, 2004; Laganas, 2002; McIntyre, 2003; Sullivan, 2002; Vijayan, 2004). Although the proposed federal legislation did not pass, California adopted legislation in July 2003 requiring businesses that experience a security breach notify their customers or employees who are California residents that their personal information was exposed and that they may be at risk of identity theft (Bass, 2003; Brandt, 2003; Office of the Attorney General State of California Department of Justice Web site).

In an innovative university outreach program, a department within Michigan State University partners with businesses to perform risk assessments and train business personnel on the importance of securing sensitive information (Henriksen, 2001). Similarly, professors from several Florida universities recognize the liability that businesses have with regard to employee and customer personal information. Their study reveals that while much of the focus on identity theft has been on the individual victim, costs to businesses due to the crime is nearly ten times the amount individuals incur (Gerard, Hillison, & Pacini, 2004, p. 3).

However, the magnitude of the financial cost to businesses is diminished since losses attributable to identity theft are spread across many thousands of businesses that accepted the fraudulent applications and charges (Sovern, 2003). Losses to businesses in terms of uncollected debts resulting from fraudulent purchases are written off (expensed) as a cost of doing business (Sovern, 2003; Sullivan, 2004c). Moreover, Sovern (2003) sees identity theft and the lack of prevention to date as a misalignment in the costs of prevention versus benefits gained. He discusses shifting the burden of loss to the following groups who help create identity theft: (1) businesses who fail to adequately protect personal data, and (2) credit bureaus for their lack of accountability in reporting data accurately.

ID Analytics, a fraud detection software company, analyzed identity fraud from consumer credit applications and known fraudulent transactions across industries to better understand the crime for finding preventive solutions. Their results, published in September 2003 in the National Report on Identity Fraud with the Center for Information Policy Leadership, show that 97 percent of applications have a valid Social Security number (ID Analytics). Conclusions show that fraud must be stopped by the businesses extending credit (ID Analytics Web site).

Sullivan (2004c) explores factors driving the identity theft epidemic through extensive research and discussions with victims and criminals to expose how identity theft works, and in so doing, conveys a system-wide perspective of the identity theft problem. He delves into the beginning of the credit economy growth, grounding the current crisis in historical context. His research reveals creative and abundant ways that thieves access personal information and how easily they acquire credit in the victims' names. Moreover, he reveals the underpinnings of the identity theft crisis as the credit industry's need for speed in processing instant credit applications for the sake of business profits.

*The **Credit Economy** Sector: Findings from the Literature*

The literature describes a credit economy that is booming with more consumers using credit now than ever before. Through aggressive marketing and sales strategies, businesses make it convenient for consumers to use credit as a means of encouraging more sales. Moreover, this sector creates a fertile environment for increased exposure of personal information, and hence, increased potential for identity theft.

Consumer debt for installment loans (for example, extensions of credit for a set period of time from banks or car dealerships) and revolving accounts (credit cards) reached an all-time high in 2003 of 1.98 trillion U.S. dollars. Consumer debt has climbed at an average rate of seven percent per year since 1988, spiking to fifteen percent in 1994 and 1995 and over eleven percent in 2000. Credit card debt doubled in 10 years, constituting more than 730 billion U.S. dollars in 2003 (Federal Reserve Bank of Philadelphia Web site).

The Visa brand card corporation reports 429 million Visa credit and debit cards issued in the U.S. in 2003 (Visa card Web site). Visa represents about 50 percent of the credit card market share with 14,000 financial institution members. Visa processed 1.1 trillion U.S. dollars in transactions last year. Worldwide, Visa processed 2.5 trillion U.S. dollars through 21,000 member institutions with 1 billion Visa cards issued in 2003.

The growth of electronic commerce (e-commerce) since 1999 has, in turn, spurred growth in the credit economy. Credit cards are the predominant payment mechanism for Internet purchases. Visa reports on-line sales grew from two percent of total transaction volume in 2000 to six percent in 2003 (Visa Web site). With the success of Internet shopping, e-commerce represented 1.9 percent of total revenues in 2003, up from 0.7 percent in 1999 (E-marketer Web Site; U.S. Department of Commerce Web site). While these percentages seem low compared to total revenue volume in consumer purchases, the growth rate is significant, averaging more than twenty percent per year.

Financial institutions and credit issuers compete for business by mass mailing pre-approved credit card applications. These "credit offers" require that name, address, and Social Security number be returned for processing a credit check to determine credit worthiness. Customers with certain credit ratings or purchase preferences are targeted through data mining techniques to receive pre-approved offers of credit. In 1996, 2.5 billion pre-approved credit card offers were mailed by financial institutions to lure new customers, whereby the average household received 24 solicitations per year (Killian, 1997). In 1998, approximately 3.4 billion pre-approved credit card offers were mailed (Givens, 2000), rising to 5 billion in 2003 (Wolk, 2004).

The Public Trust Sector: Findings from the Literature

As identity theft creates more and more victims, public trust in our nation's businesses and government erodes. Victims are angry at businesses that allow identity theft to occur (Sullivan, 2004c; Sovern, 2003; Benner et al., 2000). When public trust and consumer confidence decline, consumers are less likely to buy goods on credit, which in turn negatively impacts business revenues.

President Bush refers to identity theft as undermining public trust and shaking consumer confidence (Lemke, 2004, p.1). The U.S. Department of Justice's 2003 – 2008 Strategic Plan recognizes that identity theft as a white collar economic crime erodes the trust of the public (2002, p. 2.42). Furthermore, research shows that identity theft is now known to be an organized funding mechanism for terrorist operations and drug-trafficking schemes (Willox & Regan, 2002).

Since consumer spending accounts for two-thirds of our nation's economy, consumer confidence is an important economic indicator that reflects the U.S. economic growth rate (Dean, 2004). The Federal Reserve Board monitors consumer debt levels as confident consumers are more likely to spend more (Federal Reserve Bank of Philadelphia Web site). Economic publications report changes in consumer credit card debt levels as a means of keeping a pulse on U.S. consumer confidence (Associated Press, 2004; Aversa, 2004).

Using System Dynamics Modeling to Explore the Identify Theft Problem

The rest of this thesis uses system dynamics modeling techniques to describe the dynamics behind the exploding identity theft problem. The resulting model provides a conceptual framework for synthesizing the findings from the literature, and takes a further step by formally identifying the feedback mechanisms and relationships behind the epidemic for a more rigorous analysis. In order to understand the approach taken, it is necessary to provide a brief introduction to the methodology of system dynamics.

The Value of System Dynamics

Sterman (2000) points out that policy makers often define policies for addressing problems using an "event-oriented" view. That is, if there is a problem, we can simply take actions to address the problem and thereby get the results we desire. While such an approach is, in principle, very reasonable, it often fails to account for the fact that our actions will in fact cause the entire system to adjust, sometimes leading to results that are the opposite of what was intended. A simple example cited by Sterman (2000) is the case in which policymakers decide to address the problem of traffic congestion by building more capacity into the highway system. Results over a period of decades indicates that such actions actually lead to worse traffic congestion, as the excellent roadway network encourages urban sprawl, growth, and more traffic (Sterman, 2000, pp. 177-190).

At least one reason for such surprising results is because policy makers fail to understand the original problem from a system-wide perspective and consider the long time span over which a system can respond to changes. System dynamics is a formalized discipline for analyzing complex problems in terms of dynamic relationships between variables – relationships that can exhibit complicated feedback mechanisms and delays over extended periods of time. A system dynamics model helps document and identify and analyze these feedbacks and delays. A working simulation model can then be built and tested against reality to gain insight on possible system responses to various types of policy interventions (Sterman, 2000, p. 7). System dynamics has been applied to complex problems in a wide variety of disciplines, including studies of the U.S. cocaine epidemic (Sterman, 2000, pp. 250-262), global climate change (Sterman, 2000, pp. 241-249), project management (Sterman, 2000, pp. 55-66), and the growth and limitations of e-commerce (Oliva, Sterman, & Giese, 2003; Bianchi & Bivona, 2002).

Benefits of this methodology are identified by Sterman (pp. 32-39) as follows:

- examine issues from multiple perspectives
- expand the scope for considering the factors affecting the problem

- document, simulate, and validate competing mental models that attempt to explain the dynamics behind the problem
- gain insight into dynamically complex issues and policy resistance
- consider long-term consequences and side effects of actions.

Applying the system dynamics methodology to the problem of identity theft complements recent research by taking what researchers have learned about this problem and synthesizing those findings into a conceptual system model that explicitly identifies the underlying feedbacks and delays that are the real driving forces behind the epidemic. By so doing, the dynamics of the problem are more fully understood, and policy options can be evaluated in light of those dynamics. This thesis describes such a conceptual model (called a ***causal loop diagram***), and uses that model to explore the merits of policy that focuses predominantly on catching identity thieves. The resulting analysis suggests how and why policy centered on conventional wisdom is doomed to failure and provides insights for creating policies that can more effectively address the identify theft problem.

A Five-Step Modeling Process

The use of system dynamics to analyze a problem follows a clearly-defined methodology (Sterman, 2000). In particular, the modeling process proceeds through five steps, listed below. The process is not strictly sequential,rather, several steps may be addressed concurrently. Neither is the process linear. It is often the case that the system modeler will revisit earlier steps as the model and analysis leads to new insights that in turn necessitate changes in earlier steps. The five steps are listed below, along with a brief description of the nature and purpose of each step. We then proceed with separate sections to document each step within the context of the identify theft problem.

1) Problem articulation: Define the problem and key variables; graph the behavior of key variables over time in a reference mode; formulate a question (or questions) that the modeling effort will attempt to address.
2) Dynamic hypothesis: Create a working hypothesis that attempts to answer the questions raised in the Problem Articulation. This explanation should be expressed in terms of dynamic relationships and feedback between system variables.
3) System dynamics model: Develop a system model that describes to an adequate level of detail the relationships and feedback mechanisms identified in the Dynamic Hypothesis. When developing a working simulation model, the modeler must also use mathematical expressions to describe the dynamic relationships between the variables in the model. In some cases the modeler stops short of developing a running computer model and develops a conceptual model that identifies the system structure and feedback relationships (all described in a causal loop diagram).
4) Validation and analysis: Evaluate the model against real life. This can be done by running the model (if a working simulation model is built) and comparing simulated results to actual system behavior. If only a causal loop diagram is developed, the system structure and behavior implied by the model can be compared with known system characteristics and behavior to validate the model.
5) Conclusion: Use the model to answer the questions posed in the Problem Articulation.

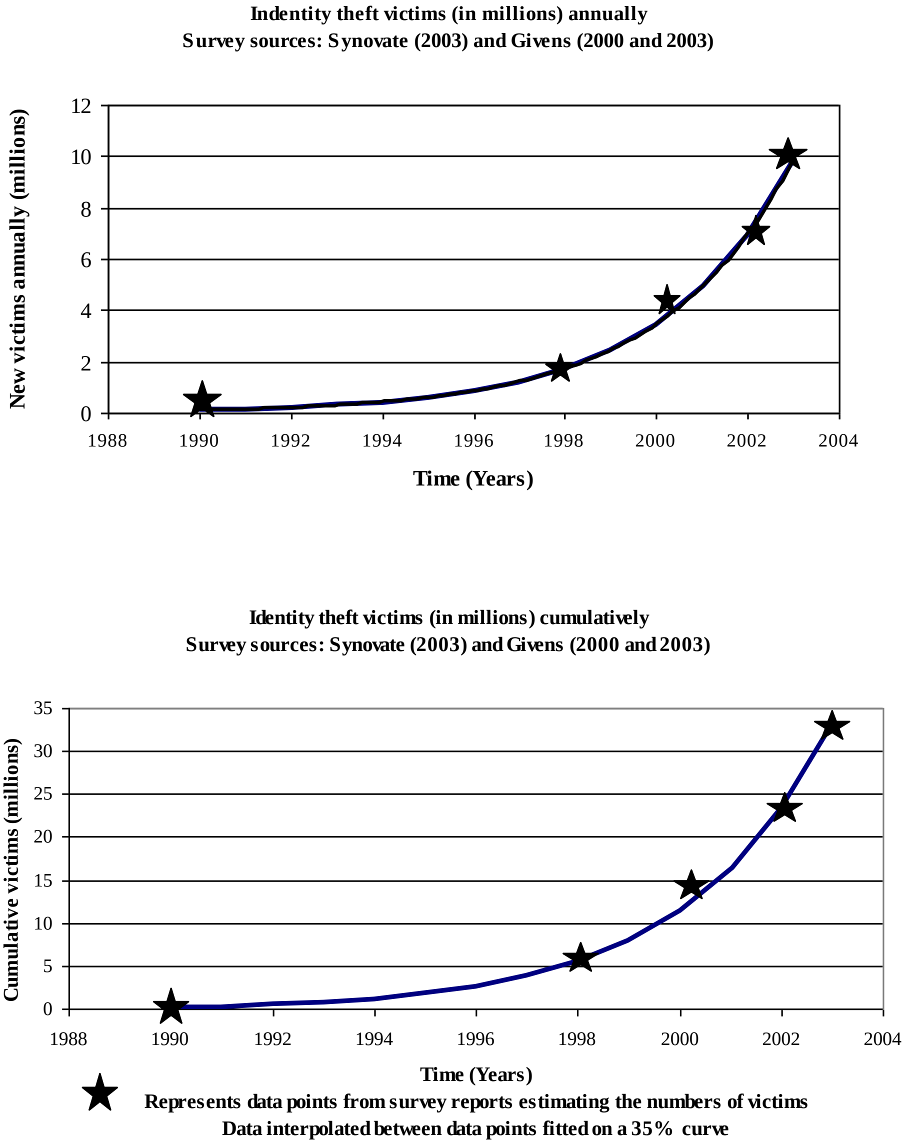
Problem Articulation for the Identity Theft Problem

The model developed herein is intended to address these questions:

- What are the factors driving the exponential growth in identity theft?
- Is the pursuit and prosecution of thieves an adequate strategy for curbing the epidemic?
- What policies would be effective?

Key variables to consider in the model include identity theft victims and identity thieves. Because this problem has entered the public consciousness in only the last few years, data on the problem come mostly from surveys and theft cases reported since 1990. However, the roots of the problem begin in the 1950s as supported by literature, particularly Sullivan (2004c). Appendix A presents an historical overview of the identity theft problem in context with technology, legislation, and impact on society. While many supporting details could be added to the timeline, it serves as a thumbnail sketch to present in context important events from the literature review.

The graphs in Figure 2 show the numbers of identity theft victims since 1990, based on the Synovate study and data collected from cases reported to the FTC and victim support networks (Givens, 2000; Givens, 2003; Synovate, 2003). The data points estimated in the survey reports are represented on the graphs below with a star symbol. Based on these data points, an increase in the estimated number of identity theft victims over time approximates a 35 percent annual growth rate added as the trend line.



★ Represents data points from survey reports estimating the numbers of victims

Data interpolated between data points fitted on a 35% curve

Figure 2: Identity theft victims 1990-2003

The goal of this research is to build a model to explain the underlying dynamics driving this exponential growth curve of identity theft. By examining the systemic factors driving identity theft growth, the model will show that the conventional wisdom approach focused predominantly on catching more thieves is inadequate because it fails to account for the system-wide dynamics leading to the identity theft epidemic.

Dynamic Hypothesis for the Causes of the Identity Theft Epidemic

The dynamic hypothesis is a working theory that seeks to answer the question of what drives identity theft. In the current context, a dynamic hypothesis is provided to answer the first question posed in the Problem Articulation, namely: *What are the factors driving the exponential growth in identity theft.* The resulting hypothesis (and system model) will then provide a basis for answering the last two questions (1) Is the pursuit of identity thieves an adequate strategy, and (2) What policies are needed?

In accordance with Figure 1 and the forgoing discussion, the dynamic hypothesis can be stated as follows. The dominant forces behind the identity theft epidemic are found in an exploding credit economy, coupled with a business culture that plays fast and loose with consumer information, while experiencing almost no negative financial consequences. This culture creates a rapid-feedback, self-reinforcing dynamic that generates ample opportunities for would-be thieves.

This hypothesis stands in contrast to the hypothesis underlying the conventional wisdom approach. Namely, that identity theft arises primarily because of a growth in the number of identity thieves. Hence, if we eliminate the thieves, the problem is solved. Referring to Figure 1, this is equivalent to isolating the ***Identity Theft*** sector as the primary source of the problem. However, Figure 1 (and the literature) suggests that this growth arises from dynamics outside that sector.

The exponential growth of identity theft incidents (which will later be modeled in the ***Identity Theft*** sector) indicates that thieves have a growing number of opportunities for conducting identity theft. Opportunities for identity theft stem from information about other consumers as would-be victims (i.e. ***Information Exposure***) and opportunities to use that information to obtain goods or services in the victims' name (i.e. ***Credit Economy***). Without both of these factors working in tandem, the identity theft problem would not have the "fuel" to grow as it has. Interactions of these three sectors in Figure 1 do not happen without fall-out. The sector that is affected in the long-term is ***Public Trust*** representing consumer confidence tied directly to the ***Credit Economy*** sector. Figure 1, as the foundation for stating the dynamic hypothesis represents a tightly-coupled, interdependent system that has been building over a period of 50 years.

System Dynamics Model of the Identity Theft Problem

A systems model is built to explain the dynamic hypothesis by exploring the underlying dynamics driving exponential growth in identity theft. First, a brief overview of the fundamental concepts will describe how system dynamics works.

System dynamics concepts – stocks, flows, and causal links.

Following the methodology outlined in Sterman (2000), a system dynamics model can be constructed to represent the dynamic relationships and processes underlying the identity theft problem. This methodology uses a simple "stock and flow" structure, where stocks represent "sinks" or "reservoirs" in a system. These can be thought of as elements in the system where things accumulate, are stored, and can eventually dissipate or move to other sinks. The flows (double-line "pipe" arrow) represent the processes by which things flow into or out of the stocks. The cloud connected to a flow denotes a source or sink from a stock outside the model boundary (Sterman, 2000, p. 192).

For example, Figure 3 shows two different stocks represented by rectangular boxes. The stock named ***Active identity thieves*** represents the collection of all individuals committing identity theft at a given point in time. The second stock represents the number of ***Identity theft victims***.

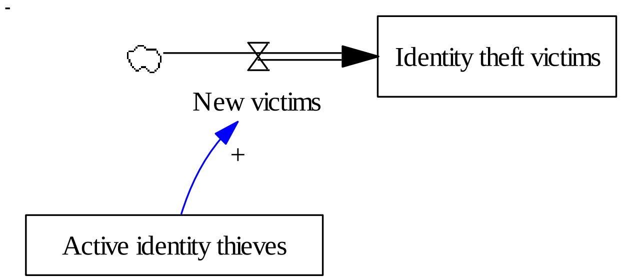


Figure 3: Identity theft victims stock

The single-lined arrow running from the ***Active identity thieves*** stock to the ***New victims*** flow is called a causal link. This link indicates that the number of identify thieves at any given time has a causal influence on the number of new victims. That is, the number of ***Active identity thieves*** has a causal effect on the number of ***New victims***, thereby affecting the stock of ***Identity theft victims***. The "+" sign on the causal link arrow is called the polarity of the causal link. A "+" means that changes in the cause (i.e. the number of ***Active identify thieves***) will lead to corresponding changes in the effect (i.e. the number of ***New victims***) in the same direction as the cause (all other elements being held equal). Hence, if the number of identity thieves goes up, so will the number of new victims (all else held equal). A minus ("-") polarity means that changes in the cause will lead to corresponding changes in the effect, but those changes will be in the opposite direction as the cause (all else held equal).

The double-lined arrow labeled as ***New victims*** and pointing into the stock of ***Identity theft victims*** represents a flow of new identity theft victims. The polarity of the double-lined arrow flow into a stock is understood to be positive and no symbol is necessary. Likewise, the flow out of a stock has a causal influence on the stock and the causal influence has a negative polarity. In Figure 4, the number of ***Active identity thieves*** is reduced by the outflow ***Thieves caught***.

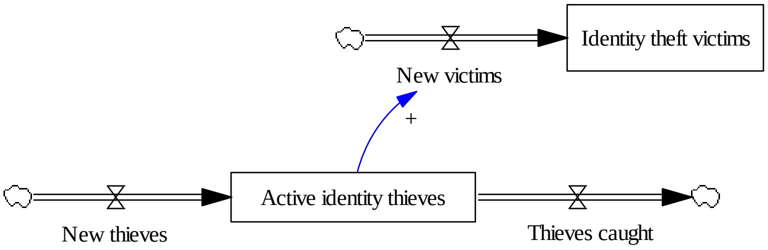


Figure 4: Active identity thieves stock

The mental model and its impact on policy.

Policy makers formulate policy based (at least in part, if not wholly) on an underlying ***mental model***. A mental model refers to the conventional and presumed understandings about how the system actually works, and about what dynamic relationships drive system behavior. The mental model is in fact a dynamic hypothesis about how the system works and hence leads to policy interventions designed to impact system performance in desired directions. Hence, mental models are very important and are implicit in every policy decision. If those models fail to account for significant factors affecting the overall problem, they will inevitably lead to flawed policies for addressing the problem.

Unfortunately, these mental models are seldom explicitly defined, and are therefore not subject to review and criticism. The discipline of system dynamics affords a methodology for defining mental models by requiring the policy maker to clearly state her dynamic hypothesis about the underlying system causes of the problem and then to represent that hypothesis with a ***causal loop diagram (CLD)***. The CLD uses the basic conventions illustrated in Figure 4 and provides a basis for policy makers to examine their assumptions (as represented in the CLD and dynamic hypothesis) and to evaluate their mental model in light of what is known about the problem. In this way, progress toward more effective policies is possible.

*The **Identity Theft** sector: A mental model and its policy implications.*

We begin by defining the system elements and relationships in the ***Identify Theft*** sector in Figure 1. This model will serve as one component of the overall systems model developed in this thesis. Moreover, we will show how this model represents the mental model behind policies that attempt to address identity theft primarily through pursuit and prosecution of identity thieves.

Figure 5 shows the same elements as Figure 4, but with more detail added to indicate feedback and dynamic relationships in causal loop diagrams within the ***Identify Theft*** sector. The CLD captures the feedback, or learning that occurs between variables, which creates a feedback loop. A feedback loop is any closed chain of cause-effect relationships in a system whereby changes at one point in the loop work through the chain to eventually “come back” to either amplify or mitigate the original change. Positive feedback occurs when the cause-effect chain works to amplify the original change. A positive feedback loop reinforces or amplifies the behavior of the system and drives it in one direction. Negative feedback occurs when the chain works to mitigate or “undo” the original change. A negative feedback loop balances the behaviors to maintain equilibrium through self-correcting or goal-seeking behavior that prevents the behavior from being driven in one direction.

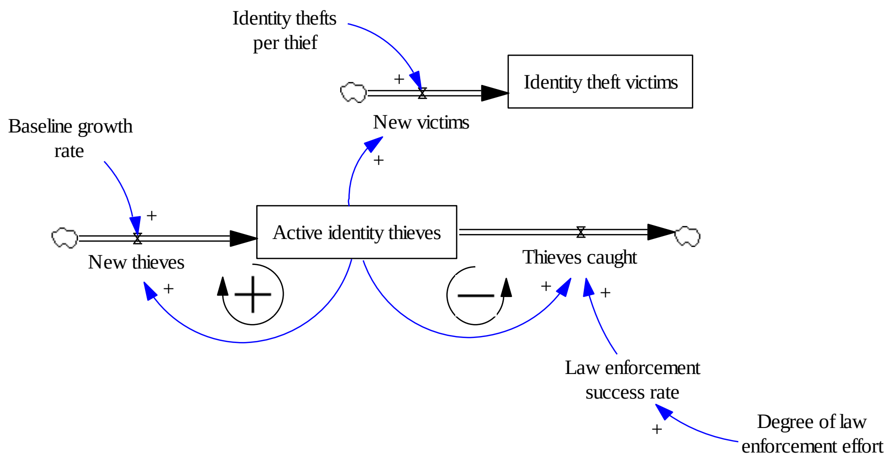


Figure 5: Law enforcement effort drives thieves caught

For example, the single-lined arrow from ***Active identity thieves*** to ***Thieves caught*** shows that the population of ***Active identity thieves*** and the ***Law enforcement success rate*** together determine the number of ***Thieves caught***. Moreover, as thieves are caught, the number of ***Active identity thieves*** goes down (remember that the outflow from the stock has a negative polarity thus decreasing the stock). Hence, there is an unbroken circle of cause-effect relationships running from ***Active identity thieves*** to ***Thieves caught***, and back to ***Active identity thieves***. Notice that as the number of active identity thieves increases, so does the number of thieves caught, which in turn reduces the number of active identity thieves. Hence, this is an example of negative feedback: changes at one point in the loop work their way through the chain of cause and effect to “undo” or mitigate the original change.

Similarly, the single-lined arrow from ***Active identity thieves*** to ***New thieves*** indicates that ***Active identity thieves,*** combined with the ***Baseline growth rate*** variable determines the number of ***New thieves***. The ***New thieves*** flow feeds the stock of ***Active identity thieves,*** thereby increasing the size of the stock. This chain of relationships

(Active identity thieves > New thieves > Active identity thieves) forms a positive feedback loop (also called a reinforcing feedback loop) because increases in the Active identity thieves stock work through the chain of cause and effect in the loop to reinforce (amplify) the original change. Notice that the positive loop is denoted by the plus sign and a directional flow arrow inside the loop. The negative loop is denoted with a similar and complimentary notation.

Another new causal link in Figure 5, the ***Degree of law enforcement effort,*** represents the level of effort that law enforcement agencies place on catching identity thieves. The greater the effort, the greater the ***Law enforcement success rate*** (i.e. the percent of active thieves who are caught).

Figure 6 shows the positive causal link relationship between ***New victims*** and the ***Degree of public urgency*** that arises from an increasing number of new victims. The ***Public tolerance level*** serves as a threshold of public tolerance for the problem which, when exceeded, affects the ***Degree of public urgency***. The tolerance level can be influenced by awareness through privacy rights groups and media reports. In this model, ***Public tolerance level*** is exogenous meaning that it has no precursor causes in the model (Sterman, 2000, p. 95). For our purposes, this variable can be treated as constant. Further expansion of the model scope is possible by treating this variable as endogenous (i.e. having precursor causes).

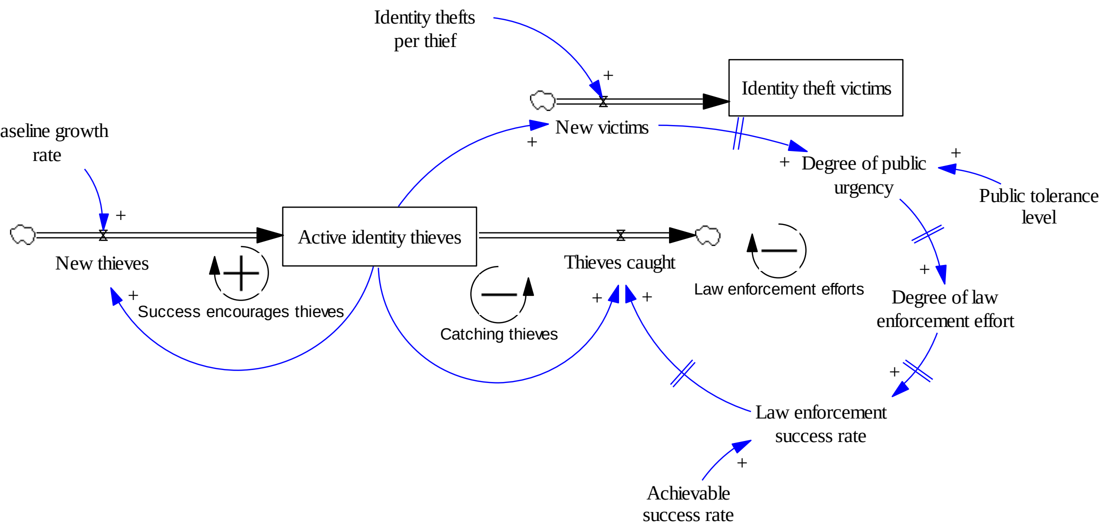


Figure 6: Conventional wisdom mental model

A growing number of ***New victims*** raises the ***Degree of public urgency*** which in turn increases the ***Degree of law enforcement efforts***. This creates a balancing feedback loop and is shown with a minus sign as “Law enforcement efforts.” This feedback loop is characterized by long delays (indicated by a dash across the causal links). This delay notation reflects the real-life inherent delays and time lag between a growing number of new theft victims and public urgency of the crime. Lags also occur between ***Public urgency*** and ***Degree of law enforcement effort***. Delays exist between the ***Degree of law enforcement effort*** and the ***Law enforcement success rate*** signifying the difficulties in being able to identify and catch the thief. The only flow without a delay in this balancing loop is between the ***Active identity thieves*** stock and ***New victims***.

One powerful factor reinforcing identity theft is that the crime is easy to commit and get away with, making it a highly lucrative, low-risk, white collar crime (Brown and Kane, 2002). The low risk of an identity thief being caught is widely reported in the media, which is likely to entice more thieves. This positive feedback loop first described in Figure 5 with the flow between ***Active identity thieves*** and ***New thieves*** is named in Figure 6 as “Success encourages thieves.” This reinforcing feedback loop represents the immediate financial rewards achieved through identity theft as incentives to encourage ***New thieves*** to commit the crime.

The negative feedback loop first identified in Figure 5 is named in Figure 6 as “Catching thieves” and represents the conventional wisdom approach of focusing on arresting and prosecuting identity thieves to address the problem. ***Achievable success rate*** is an exogenous variable that influences ***Law enforcement success rate***. This variable is an indicator of the percentage of arrests and prosecutions that can be expected from this type of crime. ***Baseline growth rate*** is an exogenous variable representing the growth rate of new thieves. When the ***Achievable success rate*** is equal to or higher than the ***Baseline growth rate***, there is no increase in identity theft. ***Identity thefts per thief*** is an indicator to approximate an average of how many victims result from one thief.

The stock of ***Active identity thieves*** is a typical population birth-death model where ***New thieves*** are added to the population of thieves and thieves are eliminated from the population as they are caught. In a balanced situation, the number of ***New thieves*** would approximate the number of ***Thieves caught***. If the rate at which thieves are caught exceeds the baseline growth rate at which new thieves are added, the number of thieves will decline, and the identity theft epidemic will come to an end as ***New victims*** and ***Active identity thieves*** level off with a slower growth rate.

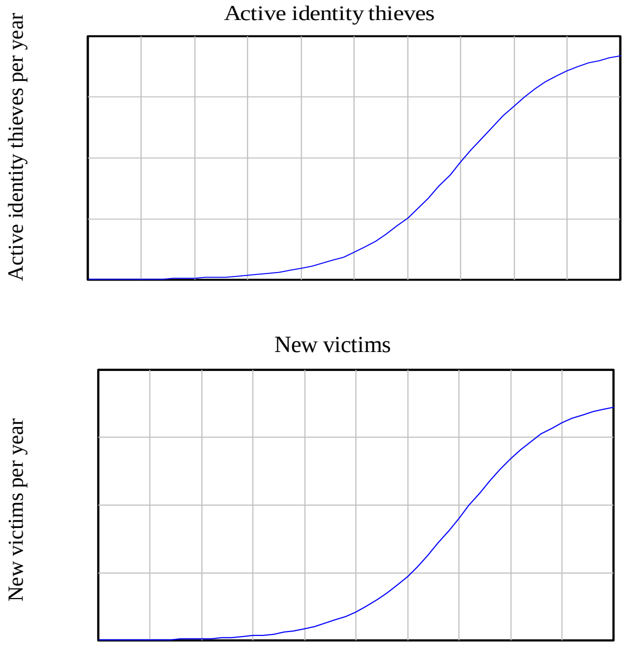
How does the system in Figure 6 actually behave? Figure 7 gives an example of a simulation run for this model. The scales on the axes are not important at this point; only the shape of the curve is relevant to understanding the dynamic behavior of this system.

The curve shows how the number of ***Active identity thieves*** behaves over time. Notice that in the early stages, the curve exhibits exponential growth. This corresponds to the time before public awareness has reached a crisis and law enforcement efforts are minimal. As the number of victims increases, the ***Public tolerance level*** is exceeded, and pressure mounts for greater ***Law enforcement efforts*** to catch and prosecute thieves. If "Law enforcement efforts" are successful, more and more thieves are caught, thereby curbing the growth of the ***Active identity thieves*** stock. One would expect (or hope) that the curve in Figure 7 would eventually decline toward zero, but it does not. This is because the ***Public tolerance level*** is a constant. This formulation of the system dynamics implies that" Law enforcement efforts" will stabilize at a point that keeps the epidemic at a level just below the ***Public tolerance level***. If the ***Public tolerance level*** were to change, the curve in Figure 7 would move accordingly.

Figure 7 gives some important insights into the role that feedback loops play in the behavior of a complex system. Recall that positive feedback loops tend to create exponential growth. Negative feedback loops try to move the system to some steady state level. Hence, when the curve in Figure 7 exhibits exponential growth in the early stages, this represents a time when the "Success encourages thieves" positive feedback loop dominates the system dynamics. That is, as long as the public isnot too upset, "Law enforcement efforts" will be minimal, and thieves will see identity theft as a lucrative, low risk business. Hence, the number of thieves grows exponentially.

The time span in Figure 7 when the curve levels off corresponds to the goal-seeking behavior indicative of negative feedback. In particular, when the epidemic is serious enough to warrant public pressure, the "Law enforcement efforts" and "Catching thieves" loops begin to dominate the dynamics, and the system seeks a steady state. In this case, the steady state corresponds to the number of thieves that can be "tolerated" by the ***Public tolerance level***.

In theory, effective law enforcement efforts should mitigate the number of new theft incidents. In 2002, the federal conviction and sentencing rate for all crimes was 58 percent based on 124, 335 cases opened (U.S. Department of Justice Web site). Simulating a lower rate to compensate for the difficulty in finding the thief, a ***Law enforcement success rate*** of 30 percent produces results that show law enforcement efforts working fairly effectively in Figure 7. The first graph of simulation results shows ***Active identity thieves*** climbing and then leveling off over a 50-year period of time as public urgency to fight the crime increases law enforcement efforts. This simulation indicates desirable results of conventional wisdom and that catching thieves works.



Simulation results of ***Achievable success rate*** 30 percent; ***Baseline growth rate*** 20 percent

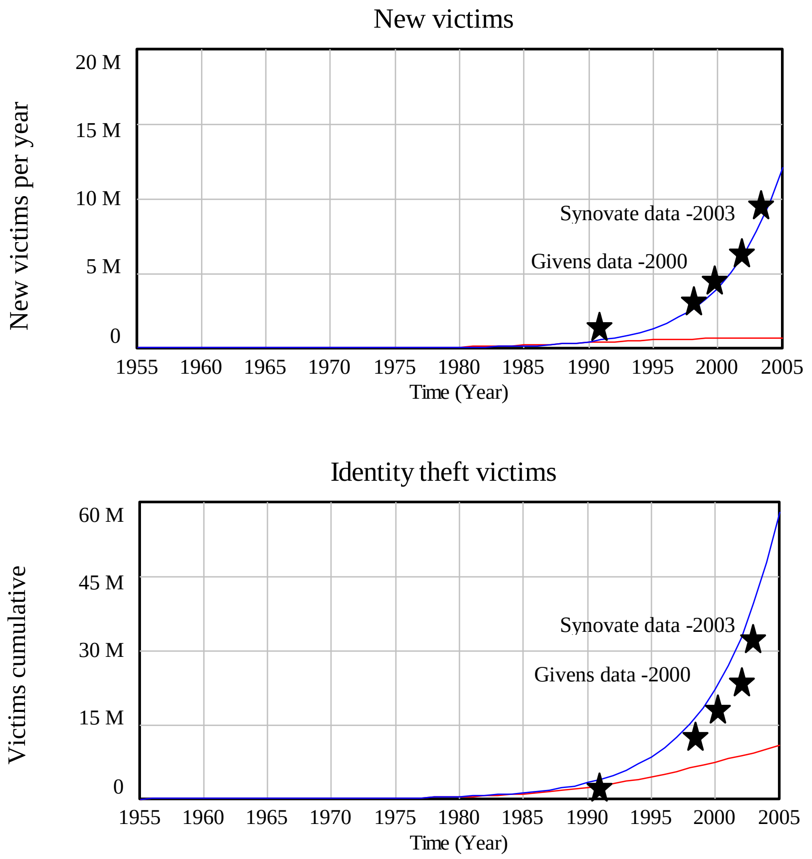
Figure 7: Conventional wisdom simulation results

The second graph shows a similar curve shape for ***New victims***, indicating that catching thieves reduces the number of new identity theft victims. However, by comparing these simulated results with the survey data in Figure 2, we see a different curve shape (trend line) for the number of victims annually. The curve in Figure 7 levels off when the ***Public tolerance level*** increases ***Law enforcement efforts*** whereas the curve in Figure 2 shows exponential growth continuing with no indication of leveling off.

This simulation result shows the basic premise of the conventional wisdom mental model using a 30 percent ***Achievable success rate***, half of the success rate achieved for all crimes. A ***Baseline growth rate*** was set at 20 percent. What we have learned is that to achieve diminished growth in identity theft under the conventional wisdom outlook, ***Achievable success rate*** needs to be fairly high (one out of three thieves arrested) and ***Baseline growth rate*** needs to be below ***Achievable success rate*** to curb the identity theft growth curve. We next examine whether these rates are realistic.

In 2000, the last year reporting this statistic, it was estimated that identity thieves have a one in 700 (0.14 percent) chance of being caught by law enforcement (Litan, 2003c). Due to resource constraints and the time and effort identity theft cases require, law enforcement generally limits its investigation to those cases involving more than $100,000 (Sullivan, 2004c). Most identity theft cases do not reach this amount and therefore do not receive attention from law enforcement (Sullivan, 2004c). Therefore, ***Achievable success rate*** is set to 5 percent in the model simulation to more closely reflect reality yet giving leeway to more success in law enforcement efforts through focused sting operations. Additionally, the ***Baseline growth rate*** is set to 25 percent. Both rates are chosen to be conservative (i.e. higher law enforcement success and lower theft growth) while representing a realistic look at the potential impact of increased law enforcement efforts.

New simulation results in Figure 8 are based on these revised rates. The graphs show the previous simulation results under the conventional wisdom (the lower trend line) compared to simulation results using revised rates. The revised rates produce exponential growth in new victims similar to the curve shape and scale to the Synovate (2003) survey and Givens (2000) survey data shown in Figure 2.



Upper trend line simulation results of ***Achievable success rate*** 5%; ***Baseline growth rate*** 25% (see Fig. 2)

Lower trend line simulation results of ***Achievable success rate*** 30%; ***Baseline growth rate*** 20% (see Fig. 7)

Figure 8: Simulation results comparing conventional wisdom to survey data

These simulation results suggest that policies focused primarily on aggressive pursuit and prosecution of thieves will likely be ineffective in curbing identity theft. In fact, such policies cannot succeed unless we can assume that policy makers underwrite a Herculean and expensive law enforcement effort in law enforcement, and that those efforts lead to unprecedented success rates in catching thieves. From a systems standpoint, the failure of the current approach to mitigate identity theft by arresting and prosecuting thieves indicates that there are other factors driving identity theft, which are not accounted for in the ***Identify Theft*** sector. The following sections will attempt to provide a fuller explanation of the identify theft epidemic that draws on the aforementioned dynamic hypothesis and elaborates on the relationships in Figure 1.

Information exposure: Growing access to personal information.

The conventional wisdom mental model described above does not tell the whole story. It does not account for the factors driving ***Baseline growth rate***. It presumes that the main reason that identity theft is on the rise is because the number of thieves is on the rise. Hence, if we reduce the number of thieves, the problem will go away. However, this mental outlook ignores the fact that the growth in identity thieves is driven by other factors that must be addressed to understand the systemic problem and potential solutions.

One factor creating opportunities for thieves is the growth in consumer personal information exposure. The overview in Figure 9 expands the discussion from the Identity theft sector where conventional wisdom focuses on law enforcement efforts to the ***Information Exposure*** sector, exploring more completely the basic definition of identity theft: thieves use personal information belonging to other consumers in order to acquire goods or services in another’s name.

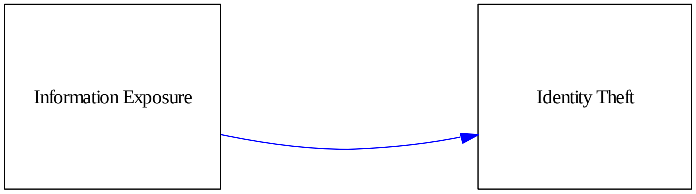


Figure 9: Overview of *Information Exposure* and *Identity Theft* sectors

Each time personal information is shared, it is exposed to those who process it and store it. As information is shared by people, across organizations, and matched between information databases, new instances of exposure occur in the reinforcing “Information economy” feedback loop created by the single-lined arrow from ***Instances of information exposure*** to ***New instances*** in Figure 10. The single-lined arrow from the exogenous variable ***Internet growth rate*** to ***New instances*** represents the exponential growth of data available on the Internet in the last ten years. The Internet presents a host of opportunities for exposing information, such as fraud scams enticing consumers to link to fraudulent Web sites and divulge personal information (Fisher, 2004). The exogenous variable ***Internet growth rate*** could be expanded in future research and treated as an endogenous variable by including it in feedback loops. For model simplicity, ***Internet growth rate*** is treated as an exogenous variable helping to create ***New instances*** of information exposure. As the stock of ***Instance of information exposure*** grows, more opportunities are created for identity thieves. (**Note**: the square box in Figure 10 represents the ***Identity Theft*** sector and is shown as a link to simplify the diagram and to emphasize the section of the model under discussion. The entire model will be presented later in the model section.)

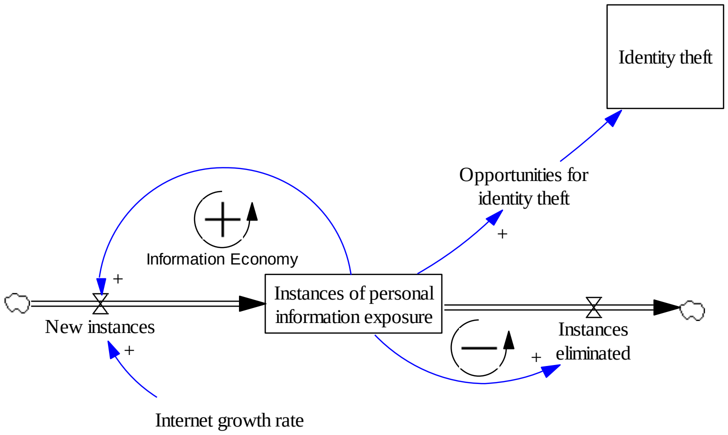


Figure 10: Information exposure

The single-lined arrow going from ***Instances of personal information exposure*** to ***Instances eliminated*** is the flow of information that is no longer exposed. With the outflow from the stock ***Instances of information exposure***, a negative feedback loop is created. On the premise that once information is exposed, therefore vulnerability to copying and preserving for future use, this balancing loop is weak compared to the positive reinforcing growth loop of the "Information economy."

Businesses and credit reporting agencies storing personal information sell it to other businesses that target their marketing efforts to solicit new credit customers. A fraction of those target marketing solicitations result in new customer credit applications. Thus, in Figure 11, ***New instances*** of personal information exposure create a stock of ***Instances of personal information exposure***. The ***Sale of personal information for target marketing*** helps businesses produce ***New credit customer solicitations*** which leads to ***Consumer credit applications***. Consumers applying for credit divulge personal information that is then used in ***Instant credit checks with credit reporting agencies*** to determine credit worthiness of the applicant. Divulging personal information in the application process leads to ***New instances*** of information exposure.

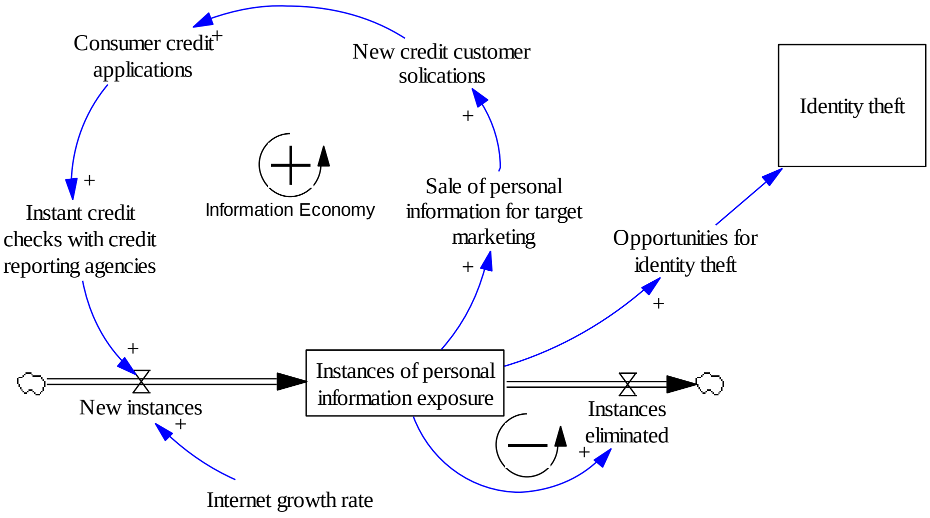

Consumer credit applications
+
New credit customer solications
+
Identity theft
+
Instant credit checks with credit reporting agencies
Information Economy
Sale of personal information for target marketing
+
Opportunities for identity theft
+
+
Instances of personal information exposure
New instances
+
Instances eliminated
+
Internet growth rate

Figure 11: Information economy loop

Findings in the literature support the growth in the “Information economy” loop, which produces exponential growth in the ***Information Exposure*** sector. This growth feeds ***Opportunities for identity theft***, which in turn drives the ***Identity Theft*** sector.

Dynamics of the growing credit economy.

From the “Information economy” loop in Figure 11, we see that causal links can be added representing the effects of ***Consumer credit applications*** leading to new credit customers. New credit customers mean more revenue for businesses. Figure 12 is an overview of the relationship between the ***Information Exposure*** and ***Credit Economy*** sectors.

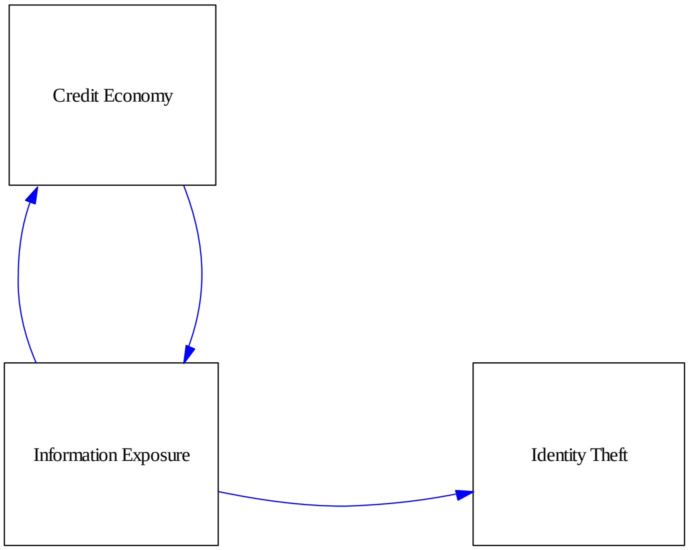


Figure 12: Overview of *Information Exposure* and *Credit Economy* relationships

The ***Credit Economy*** sector is an important element in the system dynamics driving identity theft and cannot be ignored. Consumer credit debt has grown since the 1950s and exponentially since the late 1980s. Credit spending is an important U.S. indicator signaling strength of the economy and consumer confidence (Dean, 2004).

Figure 13 shows the consumer debt level in 2003 at an all-time high of 1.98 trillion U.S. dollars. Consumer debt is composed of revolving (credit card) and installment debt, which are extensions of credit to individuals for personal expenditures (Federal Reserve Bank of Philadelphia Web site). Consumer debt has increased on average seven percent annually from 1990 to 2003, spiking to almost 15 percent in 1995 and 17 percent in 2000.

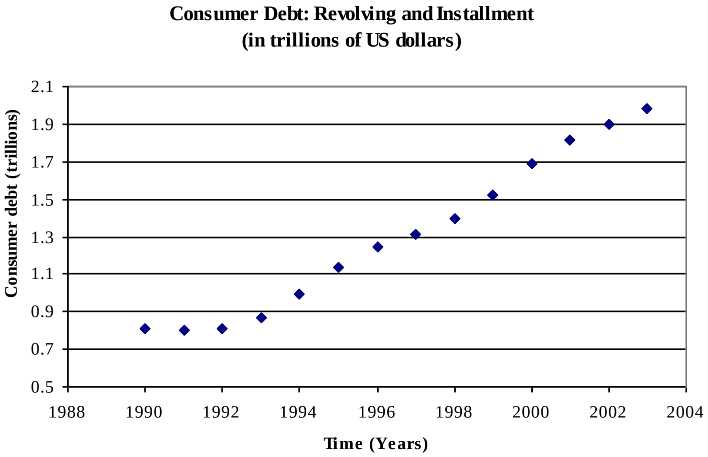


Figure 13: Consumer debt level, 1990 - 2003

This level of consumer debt growth is sustained by retailers and financial institutions doling out instant credit with cursory credit application verification to encourage customers to purchase goods (Litan, 2003c; Solove, 2003, p. 32). Figure 14 represents the trend of annual consumer debt level compared to the annual number of identity theft victims since 1990. The trend shows exponential growth similar in shape to each set of data plotted over years as shown in Figure 2 and Figure 13. The correlation of these two sets of data, consumer debt and identity theft victims, signifies a common driving force - fast and easy access to new consumer credit accounts.

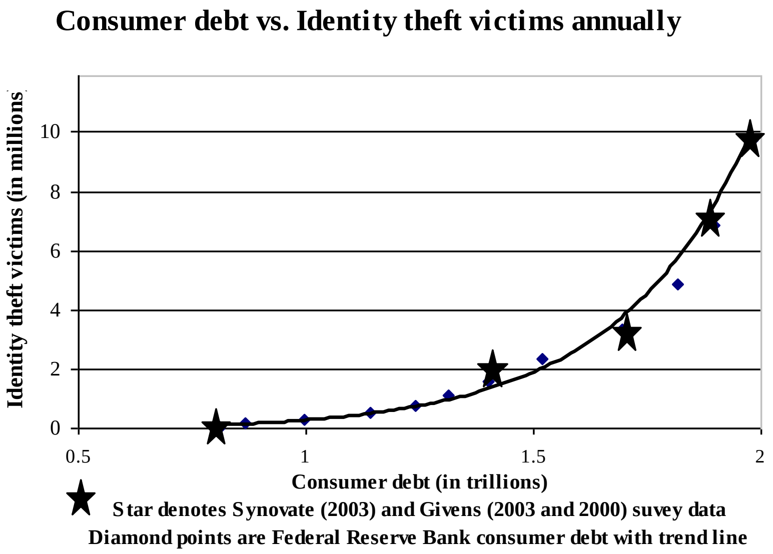


Figure 14: Comparison of consumer debt to identity theft victims, 1990 - 2003

To explore what is happening, we begin building a model for the ***Credit Economy*** sector in Figure 15. The new stock element is ***Active consumer credit accounts***. Like the other basic stock models described earlier, it is a birth-death model. The outflow arrow goes to ***Inactive accounts*** and creates a negative feedback loop as inactive accounts reduce the total number of active credit accounts. ***Inactive rate*** is an exogenous variable that interacts with the ***Active consumer credit accounts*** stock to produce ***Inactive accounts*** to show the rate at which active accounts become inactive. ***New accounts*** feed ***Active consumer credit accounts*** by the double-lined inflow arrow. The ***Application acceptance rate*** is the percentage of ***Consumer credit applications*** that become ***New accounts***. For modeling purposes the ***Application acceptance rate*** is set high (99 percent) and the ***Inactive rate*** is low (0.1 percent). The basic model shows that as more new consumer credit accounts are opened and active, business revenues go up as consumers buy on credit.

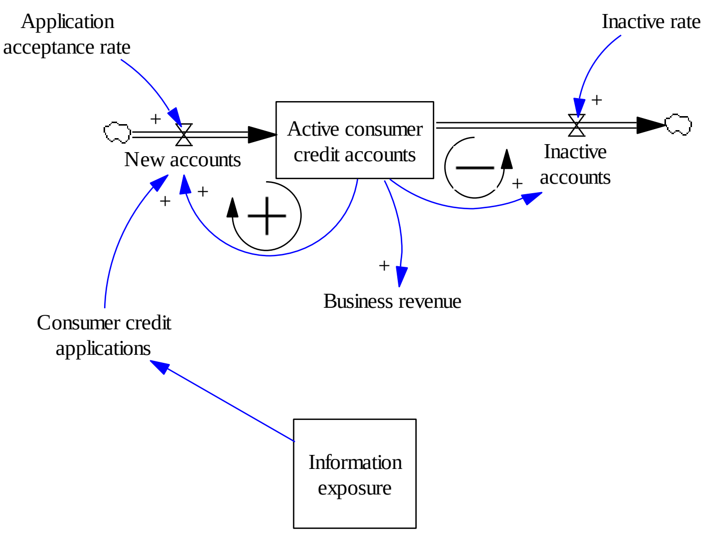

Application acceptance rate
Inactive rate
+
+
Active consumer credit accounts
New accounts
Inactive accounts
+
+
+
+
Business revenue
Consumer credit applications
Information exposure

Figure 15: Consumer credit accounts stock

*Interplay: **Credit Economy**, **Information Exposure**, & **Identity Theft** sectors.*

Figure 16 expands this basic model. ***Consumer credit applications*** prompt lenders to extend credit to new consumers by making instant credit checks with credit reporting agencies. As new credit customers are approved, ***New accounts*** are opened, and ***Business revenues*** increase by more credit sales. ***Annual revenue per account*** is an exogenous variable that converts ***Active consumer credit accounts*** to ***Business revenue***. Lenders encourage consumer credit spending through mailed solicitations, incentives, rebates, and zero-percent financing options. ***Target marketing effort*** is an exogenous variable that is a percentage of ***Business revenue*** spent on marketing efforts for ***New credit customer solicitations.*** A percentage of these solicitations (***Response rate***) result in ***consumer credit applications***. This forms the "Credit economy" reinforcing loop. It has a short feedback cycle whereby businesses see the effects of new credit accounts through financial statement revenue reported on a monthly, quarterly, and yearly basis.

When the "Credit economy" loop is anchored in the overview of all sectors (Figure 16), we begin to see that two exogenous variables (***Target marketing effort*** and

Instant credit checks with credit reporting agencies) become indigenous, or part of a dynamic feedback loop.

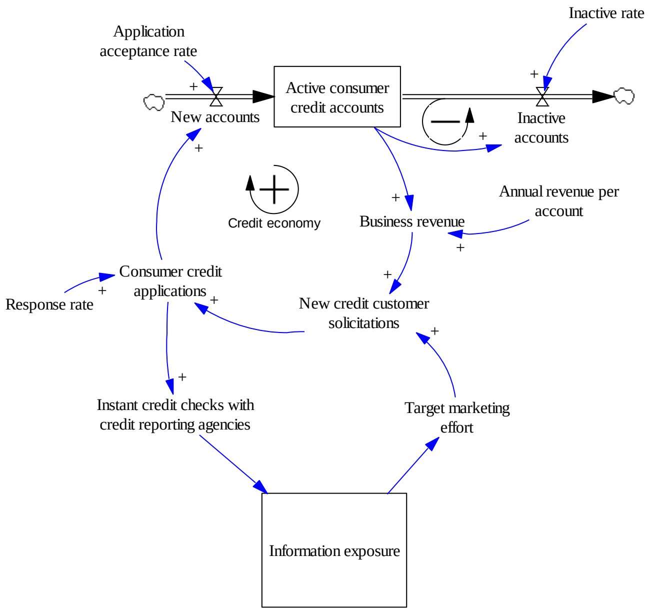

Application acceptance rate
Inactive rate
Active consumer credit accounts
New accounts
Inactive accounts
Credit economy
Business revenue
Annual revenue per account
Consumer credit applications
Response rate
New credit customer solicitations
Instant credit checks with credit reporting agencies
Target marketing effort
Information exposure
+
−

Figure 16: Credit economy loop

We can now combine the two feedback loops to produce Figure 17. In putting the two feedback loops together, we see how the ***Information Exposure*** sector drives the ***Credit Economy*** sector and vice versa. This is a tightly-coupled system where the two feedback loops depend on one another. A quick run through of both loops working together show that information exposure drives target marketing efforts to solicit customers who then apply for credit accounts. Through the ***Consumer credit application*** process, personal information is divulged which creates more ***Instances of information exposure***.

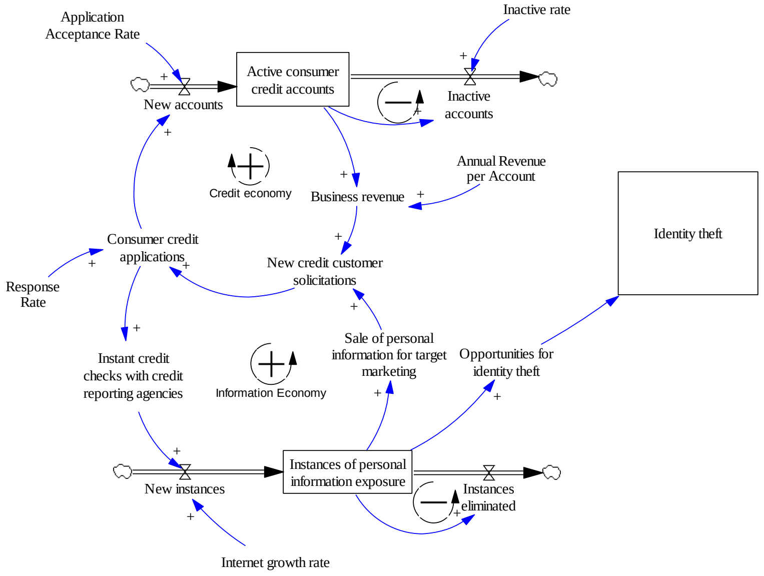

Application Acceptance Rate
Inactive rate
Active consumer credit accounts
New accounts
Inactive accounts
Credit economy
Business revenue
Annual Revenue per Account
Identity theft
Consumer credit applications
New credit customer solicitations
Response Rate
Instant credit checks with credit reporting agencies
Information Economy
Sale of personal information for target marketing
Opportunities for identity theft
New instances
Instances of personal information exposure
Instances eliminated
Internet growth rate
+
−

Figure 17: Credit economy and information economy loops

This model reflects that once personal information is divulged, it is exposed indefinitely. The two loops together feed the exponential growth of identity theft. There are no strong negative feedback loops that would tend to balance the exponential growth rate and cause the growth to level off in reaching an equilibrium state. Instead, the effect is exponential growth in opportunities for identity theft. All feedback loops discussed to this point are combined in Figure 18. The positive loops associated with the ***Credit Economy*** and the ***Information Exposure*** sectors drive the opportunities for identity theft while balancing the loops in the ***Identity Theft*** sector.

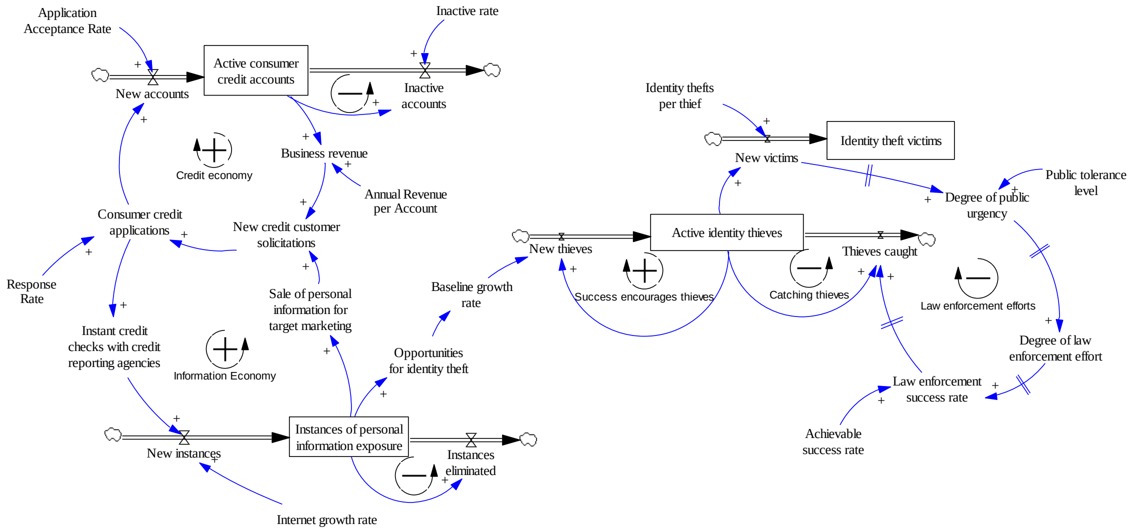

Application Acceptance Rate
Inactive rate
Active consumer credit accounts
New accounts
Inactive accounts
Credit economy
Business revenue
Annual Revenue per Account
Consumer credit applications
New credit customer solicitations
Response Rate
Sale of personal information for target marketing
Instant credit checks with credit reporting agencies
Information Economy
Opportunities for identity theft
Baseline growth rate
Instances of personal information exposure
New instances
Instances eliminated
Internet growth rate
Identity thefts per thief
Identity theft victims
New victims
Public tolerance level
Degree of public urgency
Active identity thieves
New thieves
Thieves caught
Success encourages thieves
Catching thieves
Law enforcement efforts
Degree of law enforcement effort
Law enforcement success rate
Achievable success rate

Figure 18: Combined feedback loops of three sectors

We see that ***Opportunities for identity theft*** drive the ***Baseline growth rate*** that was discussed in the ***Identity Theft*** sector. Exponential growth in the ***Credit Economy*** and the ***Information Exposure*** sectors leads to exponential growth in the ***Identity Theft*** sector. This mental model more thoroughly explains the dynamics driving the 35 percent increase in identity theft victims shown in the literature. The model shows the dynamics driving identity theft and how powerful those dynamics are relative to the “Law enforcement efforts” and “Catching thieves” balancing loops. Note that these balancing loops contain delays (cross marks on the causal links), which lessen their ability to respond quickly. The positive feedback loops on the other hand are quick to respond to reinforcing behavior, thus producing exponential growth.

*Role of the **Public Trust** sector.*

The last sector to be explored is ***Public Trust***. Figure 19, first seen in Figure 1, shows a relationship between the ***Identity Theft*** sector and ***Public Trust*** and from ***Public Trust*** to the ***Credit Economy*** sector. The increasing numbers of identity theft victims over the last five years causes consumers to lose trust in business practices and government policy that allow identity theft to occur. One out of six U.S. adults has become a victim of identity theft since 1990 making consumers concerned for their own financial security. The burden of cleaning up the mess left by identity theft falls to individual victims who have little or no control over the crime (Givens, 2003). Identity theft shakes consumer confidence, which over time affects the credit economy.

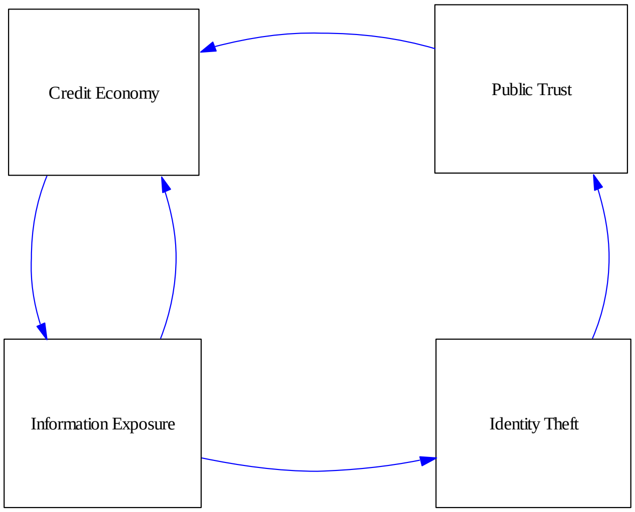


Figure 19: Overview of all sectors

Within this framework, several more causal links will be added to the causal loop diagram model shown in Figure 18. The literature identifies impacts from identity theft on victims, businesses, and society. The impact on businesses will be modeled with regard to the data security issues found in the literature. More could be addressed in this area by future models. Impact to victims is without question, devastating. Collectively, the impact to individuals will be examined as the effect on the ***Public Trust*** sector. The impact on public trust will be discussed relative to the ***Degree of public urgency*** first discussed in the ***Identity Theft*** sector.

When businesses fail to implement appropriate data security policies, procedures, and systems, personal information is exposed making it vulnerable to perpetrators. Generally, businesses do not have the incentive to protect personal information therefore businesses do not put forth the cost and effort to do so (Sovern, 2003, p. 368).

One reason that financial institutions may not feel the urgency of identity theft as individual consumers do is that losses from credit card fraud are not concentrated on the banks issuing credit cards. Instead, current business practices pass losses from identity theft back to the merchant who accepted the fraudulent charges (Sovern, 2003). Spreading the cost dilutes the potency of the 50 billion U.S. dollar loss to businesses estimated in 2003 so that many merchants share the burden (Synovate, 2003, p. 6). However, when financial losses from identity theft mount, or the threat for future loss exists, businesses are motivated to put forth the effort to protect personal information.

Figure 20 shows ***Active identity thieves*** leading to ***Financial losses for businesses*** at the time that a new victim is created. Losses occur because the identity thief charged goods on a credit account in a victim's name for which the thief has no intention of repaying. If the victim can prove that he/she did not acquire the goods and that a theft has occurred, generally the victim does not have to repay the creditor. The loss of stolen goods is absorbed by the business lending credit to a thief. (**Note**: The legal ramifications are more extensive, but simplified for the purpose of building the model.)

Financial losses for businesses motivate ***Businesses' effort to protect personal information***. Better data protection practices efforts lead to ***Instances eliminated*** thus reducing the stock of ***Instances of information exposure*** and reducing ***Opportunities for identity theft***. Both causal links have positive directional signs. Adding these flows creates the "Businesses protecting data" balancing feedback loop in Figure 20.

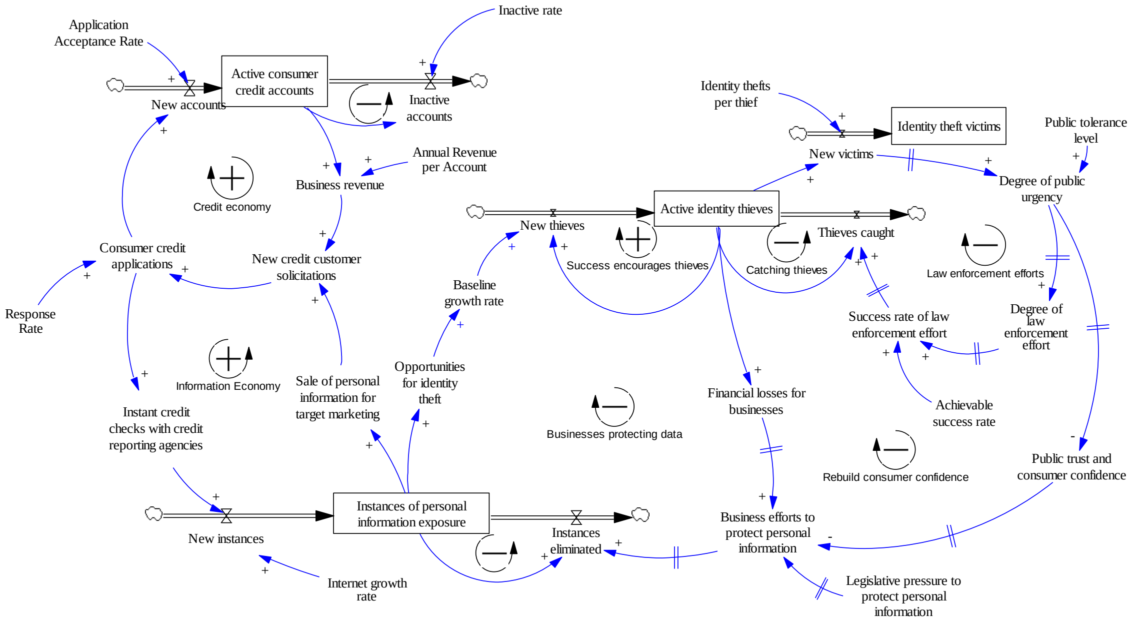

Inactive rate
Application Acceptance Rate
Active consumer credit accounts
New accounts
Inactive accounts
Identity thefts per thief
Identity theft victims
Public tolerance level
Annual Revenue per Account
Credit economy
Business revenue
New victims
Degree of public urgency
Active identity thieves
New thieves
Thieves caught
Success encourages thieves
Catching thieves
Law enforcement efforts
Consumer credit applications
New credit customer solicitations
Baseline growth rate
Success rate of law enforcement effort
Degree of law enforcement effort
Response Rate
Information Economy
Opportunities for identity theft
Sale of personal information for target marketing
Instant credit checks with credit reporting agencies
Businesses protecting data
Financial losses for businesses
Achievable success rate
Rebuild consumer confidence
Public trust and consumer confidence
Instances of personal information exposure
New instances
Instances eliminated
Business efforts to protect personal information
Internet growth rate
Legislative pressure to protect personal information
+
-

Figure 20: Businesses protecting data

Some businesses have recently made efforts to better protect consumer information. When consumer personal information is provided to a business through an application for credit, there are two ways that information can be exposed: (1) electronically in an unencrypted database exposing it to potential theft from anyone with access to the data, and (2) physically through the paperwork of business transactions making it at risk to insiders, employees and employers (Michigan State University Web site). Data security business policies and practices determine the businesses' level of effort to protect personal information.

Legislation holding businesses liable for not adequately protecting data is a threat for a financial loss. This ***Legislative pressure to protect personal information*** is an exogenous variable in Figure 20 that also drives ***Businesses' effort to protect personal information***. The state of California passed notification of security breach legislation in July 2003 requiring California resident notification when their unencrypted personal data was compromised (i.e. exposed) as a result of a security breach (Office of the Attorney General State of California Web site; Bass, 2003; Brandt, 2003). This is one example of legal action encouraging corporate accountability, or risk being held liable in a lawsuit for not protecting consumer personal information. A similar bill was presented by the Senate, but failed to be included in federal legislation last year (S.1350, Notification of Risk to Personal Data Act, 108th Cong., 1st Sess., 2003).

From the consumer viewpoint, as the ***Degree of public urgency*** increases, ***Public trust*** *and* ***consumer confidence*** decreases. Erosion of ***Public trust and consumer confidence*** happens over a long period of time and is indicated by a delay marking on the causal link. As ***Public trust and consumer confidence*** decreases, businesses may fear losing customers, which increases ***Business efforts to protect personal information***. This causal link has an opposite effect and is indicated by a minus sign. This link creates the balancing feedback loop "Rebuild consumer confidence."

Current business practices and U.S. laws feed the systemic problem of identity theft. Businesses have legal recourse by pursuing victims when debts are incurred fraudulently in victims' names (Solove, 2003; LoPucki, 2002). When that avenue is exhausted, accounting practices allow businesses to expense uncollectible debts as a cost of doing business. Businesses are willing to accept the risk of extending bad credit because the financial loss is a small fraction of business revenue. The relatively small percentage of transaction volume due to theft does not give financial institutions incentive to change their business practices (Litan, 2003a, p. 2).

The last causal links to be added to the model stem from ***Public trust and consumer confidence*** as shown in Figure 21. When ***Public trust and consumer confidence*** decrease, consumers may react by withdrawing from the ***Credit economy*** sector in two ways: closing active consumer accounts and not applying for new credit. As ***Public trust and consumer confidence*** decrease, the ***Inactive rate*** for credit accounts will have the opposite effect shown by a minus on the causal link. This link creates the balancing feedback loop "Loss of faith" where consumers close existing credit accounts.

Another balancing feedback loop is formed by a causal link from ***Public trust and consumer confidence*** to ***Response rate*** for new credit applications. As ***Public trust and consumer confidence*** decreases, ***Response rate*** also decreases, thus a plus sign is used on the causal link indicating the corresponding effect. This completes a balancing feedback loop "No credit for me."

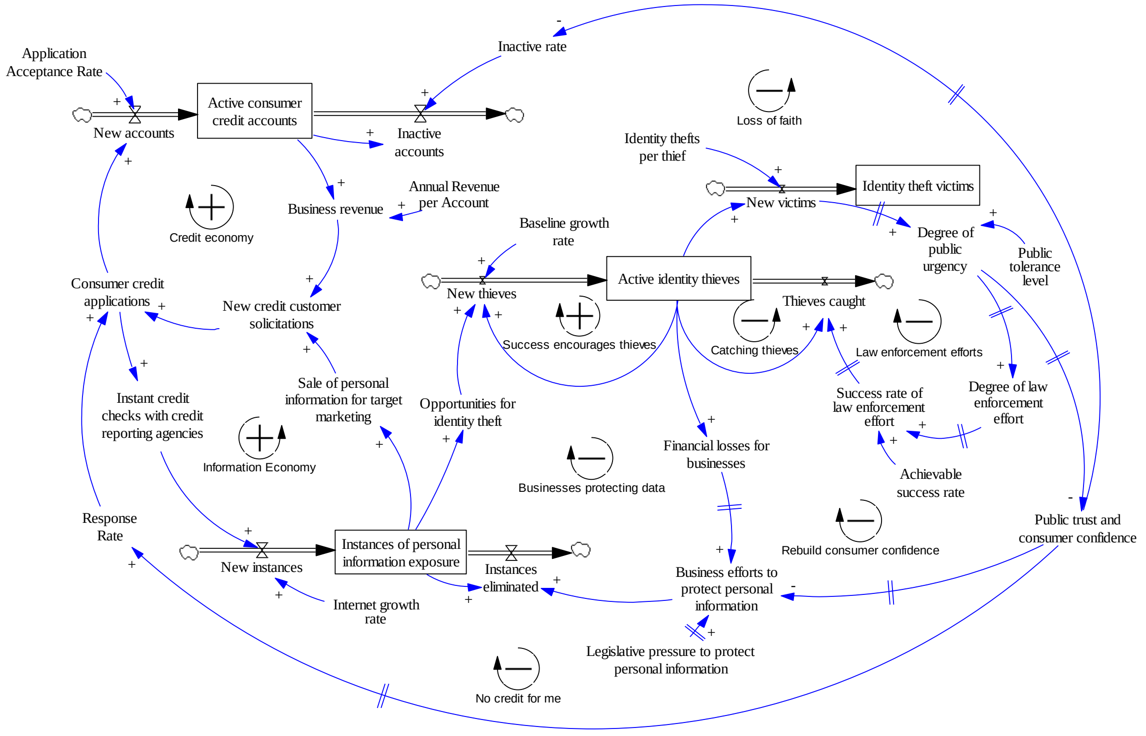

Application Acceptance Rate
New accounts
Active consumer credit accounts
Inactive rate
Inactive accounts
Loss of faith
Identity thefts per thief
New victims
Identity theft victims
Credit economy
Business revenue
Annual Revenue per Account
Baseline growth rate
Degree of public urgency
Public tolerance level
Consumer credit applications
New credit customer solicitations
New thieves
Active identity thieves
Thieves caught
Success encourages thieves
Catching thieves
Law enforcement efforts
Instant credit checks with credit reporting agencies
Sale of personal information for target marketing
Opportunities for identity theft
Success rate of law enforcement effort
Degree of law enforcement effort
Information Economy
Financial losses for businesses
Businesses protecting data
Achievable success rate
Response Rate
Instances of personal information exposure
New instances
Instances eliminated
Rebuild consumer confidence
Public trust and consumer confidence
Business efforts to protect personal information
Internet growth rate
Legislative pressure to protect personal information
No credit for me

Figure 21: System dynamics model of the identity theft problem

Both of these balancing feedback loops show delay marks indicating long-term effects of identity theft on public trust and consumer confidence. The overall economic impact of the cycle shows a decrease in active consumer credit accounts and a long-term negative impact on the credit economy through the erosion of public trust and consumer confidence.

Validation and Analysis

The system dynamics model in Figure 21 provides a detailed system theoretic explanation of the dynamic hypothesis described in this thesis. Moreover, this model represents the author's mental model of the underlying dynamics behind the identity theft epidemic. If correct, this model suggests that exponential growth in the ***Credit Economy*** and the ***Information Exposure*** sectors drives exponential growth in the ***Identity Theft*** sector and also suggests that efforts to curb the epidemic will fail if they ignore these other sectors and concentrate primarily on catching thieves (in the ***Identity Theft*** sector of Figure 1). The question is whether or not this mental model in Figure 19 squares with reality.

The literature supports the dynamic hypothesis and model in Figure 21. For example, all of the following are increasing at an exponential or higher rate: credit accounts (Visa Web site), consumer debt (Federal Reserve Bank of Philadelphia Web site), credit offer solicitations (Killian, 1997; Givens, 2000; Wolk, 2004) information exposure (Sullivan, 2004c), and identity theft victims (Synovate, 2003).

Most of the literature on identity theft is comprised of anecdotal evidence from reported identity theft cases, legal reviews of credit practices and legislation, and surveys of consumers to ascertain the magnitude of the problem. The model in Figure 21 is substantiated by the literature to be a more complete explanation of factors driving identity theft. To validate the model further, a sampling of credit offer solicitations were evaluated to gauge the causal link between the ***Credit Economy*** and the ***Information Exposure*** sectors as a lynchpin that feeds the ***Identity Theft*** sector.

One important feature in Figures 1 and 21 is the "Information economy***"*** positive feedback loop between the ***Credit Economy*** and the ***Information Exposure*** sectors. This loop drives exponential (or faster) growth in both of these sectors, thereby leading to higher and higher levels of information exposure. As this happens, the opportunities for identity theft dramatically increase, thereby leading to more and more thieves, identify theft incidents, and identify theft victims. The model implies that the resulting rate of growth of the population of active identity thieves outstrips any realistic or affordable law enforcement efforts. Hence, the validity of the model and the findings implied in the earlier sections depend on the validity of this positive feedback loop between the ***Credit Economy*** and ***Information Exposure*** sectors.

Does the literature support the existence of this feedback relationship? Note that this feedback loop describes a growth in the exposure of personal information because of aggressive marketing tactics by business and financial houses as they pursue new credit customers. These tactics lead to new credit applications by potential customers, which are then checked for authenticity through credit reporting agencies. The literature shows that credit offer solicitations mailed to consumers are all-too easily stolen and used by identity thieves to acquire a credit card in someone else's name. These mailed solicitations are easily stolen from mailboxes and retrieved from trash bins. The thief then uses the personal information of another to apply for a credit card in the victim's name. Verification of consumer identity is generally performed hastily by banks making perfunctory credit checks. A credit card is then mailed to the thief in the victim's name. Credit offer solicitations mailed to households and returned via mail to banks are vulnerable to identity theft (Sullivan, 2004c). Just how prevalent the problem is in terms of the number of credit offer solicitations mailed leading to fraudulent applications is an area where some data exists. However, more information is needed to understand the connection and the impact where credit offer solicitations constitute the ***Information Exposure*** sector and credit applications leading to new credit accounts constitute the ***Credit Economy*** sector. When the two sectors collide by a fraudster's abuse of these sectors, the ***Identity Theft*** sector is set in motion.

The large amount of revenue that financial institutions and retailers gain through consumer credit spending overshadows the potential loss that could result from issuing bad credit. Visa estimates that fraud losses are between 0.05 and 0.07 percent of transactions or seven cents per 100 U.S. dollars in transactions (Visa Web site). Banks estimate that one percent of credit card, banking, and loan applications are fraudulent largely due to identity theft (Litan, 2003e). These low percentages mask the magnitude of identity theft incidents given the high volume of credit applications and corporate revenues. Thus, businesses continue to supply instant credit as long as revenues well-exceed losses stemming from identity theft.

Financial lenders are extremely competitive and aggressive in pursuing new credit customers. Unfortunately, data useful to understanding the volume of solicitations are not available. Data on credit offer solicitation were sketchy and estimated since many financial institutions participate in target marketing and data would have to be gathered from each institution. Furthermore, a bank's marketing efforts are not likely to be shared with consumers and competitors.

Financial institutions and credit issuers compete for business by mass mailing pre-approved credit card applications requiring name, address, and Social Security number be returned for credit checking processing. Customers with certain credit ratings or purchase preferences are targeted through data analysis to receive pre-approved offers of credit. In 1996, 2.5 billion pre-approved credit card offers were mailed by financial institutions to lure new customers, whereby the average household received 24 solicitations per year (Killian, 1997). In 1998, approximately 3.4 billion pre-approved credit card offers were mailed (Givens, 2000), rising to 5 billion in 2003 (Wolk, 2004).

The two graphs in Figure 22 show simulation results of running the credit economy loop with parameters set to reflect currently available numbers (credit accounts may be understated). The active consumer credit accounts represent an estimate of all consumer debt accounts, revolving and installment.

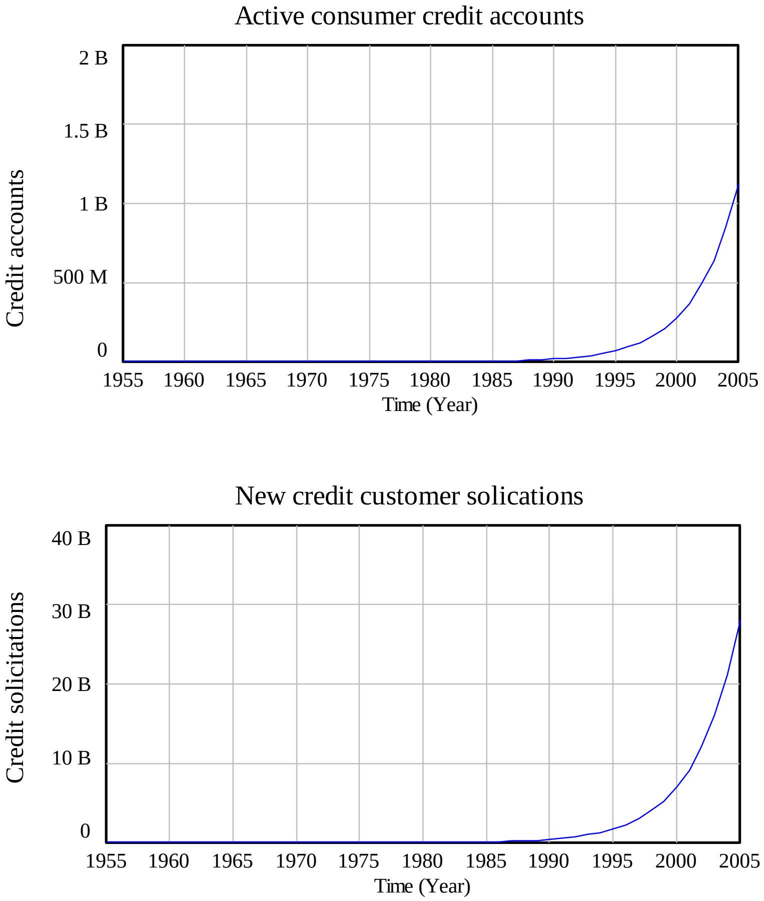


Figure 22: Simulation results of credit economy loop

While new customer solicitations appear to reflect the 1996 and 1998 reported numbers (2.5 and 3.4 billion, respectively), the simulation shows that solicitations may be higher than that reported for 2003 (5 billion). The significance and concern of the upward trend in credit card solicitation mailings is the opportunity they present for a perpetrator to commit identity theft by applying for credit in the victim's name.

To illustrate the large number of credit card solicitations implied in the model and described in the literature, data were collected on the number of credit card pre-approved offers by financial institutions received at one address during a five-month sampling period of June 1, 2004 through October 31, 2004 (SNL Financial).

Annualized sample	**Totals for sample period**	**Visa**		**Mastercard**		**Other**	
		BankOne	35	Capital One	23	AT&T	10
		Providian	2	MBNA	16	Discover	8
				CitiBank	9	Amer. Express	1
				Chase	2		
				Household	2		
259 offers	**108**		**37**		**52**		**19**

Table 23: Credit card solicitation sampling, June 1 through October 31, 2004

This sampling is anecdotal data that illustrates the reports on the billions of credit offers mailed to consumers. In this sample, 108 credit offers were received at one household address during the five-month sample period. This sample extrapolated over a twelve-month period equates to 259 offers per household or 130 offers per person per year, ten times greater than estimates seven years ago. Assuming 100 million U.S. adults (fewer than half of the U.S. adults over age 18) receive similar mailings as the sample household, 13 billion solicitations per year are calculated. The data suggests that the number of credit card offers mailed in 2004 is higher than five billion reported for 2003. The sample follows more closely simulation results from the model and supports the trend that the number of credit offer solicitations continues to increase.

Furthermore, businesses analyze consumer purchase preferences to increase sales by targeting specific customer profiles (Turban, Ranier & Potter, 2003, p. 153; Sovern, 2003, p. 366). Customer data is mined for competitive advantage, and sold between organizations both legally and illegally (Mayer and Witte, 2004). In the sample of solicitations, 19 of the 108 credit offers (18 percent) promoted organizations associated with the consumers, such as the American Kennel Club, Rotary Club, airline frequent flyer membership, and a university from which the household members graduated. These examples of solicitation using the consumers' affiliations demonstrate the business practice of exposing personal information through sharing or selling it to businesses. Such practices place the potential for higher revenues ahead of corporate responsibility for customer data.

To validate the ***Identity Theft*** sector, model simulation results of victims are compared to estimated victims reported in the literature (see Figure 24). The star symbol represents data points of the cumulative number of victims of identity theft estimated by 2003 Synovate survey data of U.S. adults. Simulation results produced data points following a similar curve shape as shown in the upper, smooth line.

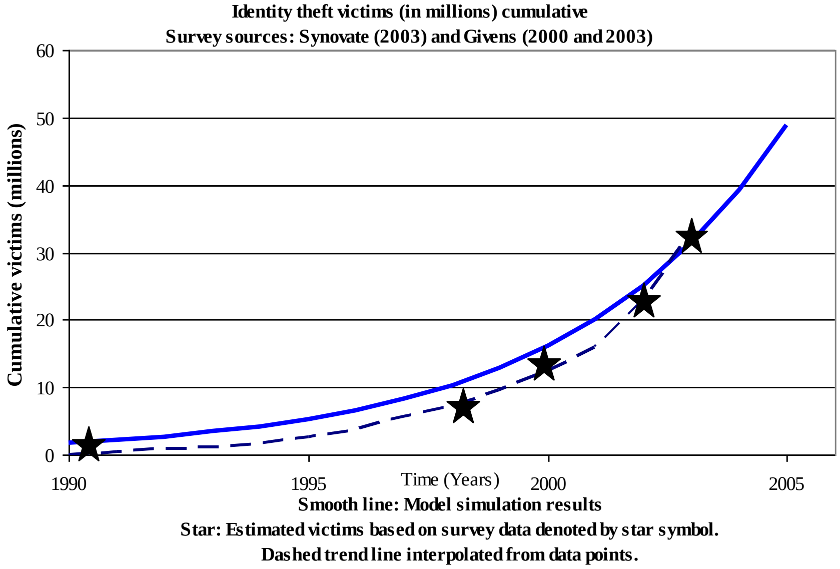


Figure 24: Comparison of simulation results and reported theft victims

Conclusions

The system dynamics model in Figure 21 shows the positive, reinforcing feedback loops associated with factors underlying and driving exponential growth in identity theft. All positive loops have a quick feedback cycle, which reinforces the behavior at a fast pace. The balancing feedback loops, located predominantly in the lower right corner of Figure 21, have delays causing them to be weaker to respond in balancing the positive, growth loops.

The system dynamics model demonstrates that addressing the problem of identity theft solely by the conventional wisdom of catching thieves is not adequate for reducing identity theft incidents due to underlying reinforcing feedback loops driving opportunities for thieves, namely the ***Credit Economy*** sector and the ***Information Exposure*** sector. A conventional wisdom mental model entices policymakers to respond to public pressure arising from increased identity theft incidents by enacting legislation to prosecute identity thieves. Policy decisions based predominantly on conventional wisdom address the <u>symptoms</u> of the identity theft problem without addressing the underlying <u>systemic</u> causes and the long-term impact on the ***Public Trust*** sector.

The conventional wisdom model of catching thieves is analogous to plugging a hole in a dam to prevent a leak from becoming bigger. As the water level rises, the pressure builds behind the dam causing more and bigger holes (***Opportunities for identity theft***). The flaws and weakness of the dam's infrastructure cannot be fixed solely by plugging the holes (***Law enforcement efforts*** and ***Catching thieves***). Similarly, as businesses continue to play fast and loose with consumer personal information, and as more thieves see the financial gains with little risk of getting caught, the loss of consumer confidence weakens the economy over time. Policymakers and businesses afraid that tightening the instant credit flow by more careful verification of customer identities would cause an immediate slow-down in the economy, failing to see the long-tem economic damage of the current system dynamics (Sullivan, 2004c).

In modeling the driving forces behind the identity theft problem, several policy-setting conclusions are drawn by running simulations. First, “Law enforcement efforts” will never be effective in curbing the high growth rate in identity theft by attempting to reduce the number of identity thieves. Second, personal information is not secret, is made more available through target marketing in the ***Information Exposure*** sector, and will continue to be exposed to some degree even with “Businesses protecting data.” Third, the financial rewards for identity thieves are quick and easy which drive “Success encourages thieves.” Lastly, soliciting new credit customer applicants increases ***Business revenues*** in the ***Credit Economy*** sector. Overall, the exponential growth of exposed personal information makes instant credit easy to obtain, identity theft easy to commit, and law enforcement ineffective from a systemic view.

An assumption in the current credit economy, evidenced in the literature, is that financial institutions are unwilling to slow the pace of issuing credit because fast, easy, and recklessly issued credit spurs the U.S. economy (Litan, 2003c; LoPucki, 2002; Solove, 2003; Sovern, 2003; Sullivan, 2004c; Synovate, 2003). This assumption plays a dominant role in creating the conventional wisdom associated with current policy, business practices, and potential solutions to prevent identity theft. Under the principle of corporate governance, business leaders and policymakers should examine if this assumption reflects accountable and responsible actions on behalf of business organizations. What is best for the long-term health of the economy? What are the consequences from policy decisions regarding the ***Credit Economy***, ***Information Exposure, Identity Theft***, and the ***Public Trust*** sectors? Based on the system model, what policies would be effective?

With the system dynamics model in Figure 21 as a new mental model, policies should be considered that will introduce balancing loops to mitigate the growth in identity theft. Just as the model shows the factors driving identity theft, it provides insight to the vulnerabilities where policy and business practice changes can be made to change the behavior over time. Reducing the exponential growth in identity theft is a three-fold effort represented in the three sectors ***Identity Theft***, ***Information Exposure***, and ***Credit Economy***.

We conclude through the modeling process that "Law enforcement efforts" and "Catching thieves" balancing loops in the ***Identity Theft*** sector are necessary but not adequate to control the exponential growth. What can be changed in the ***Information Exposure*** and ***Credit Economy*** sectors to decrease opportunities for identity theft?

Although it is recognized that personal information should not be considered private, it should be protected to prevent further unnecessary exposure and enticement for identity thieves. Policy and business practice changes should, at a minimum, consider the following recommendations for the ***Information Exposure*** sector:

1) Businesses should examine their information systems to see how the consumer's Social Security number is used and where it is printed.
    a. Social Security numbers should not be used or stored unless it is vital to the consumer's financial or employment history

b. If it is deemed necessary to maintain the Social Security number, it should be stored as encrypted data, there should be adequate system security, and business policies and practices should limit personnel with access rights.

2) Consumers should have a more active role in indicating how their personal information is used and an easier way to communicate their desires to businesses. Although privacy notices are mailed from businesses to customers for opting in or out of sharing information with others, and opting out of credit offer solicitations is possible, these processes are cumbersome and not consumer/customer-focused.

3) Stiffer penalties for organizations that expose personal information through information systems security breaches or through poor business practices.

Identity theft <u>prevention</u> needs to occur in the ***Credit Economy*** sector where the following policy and business practice changes should, at a minimum, consider the following recommendations:

1) The credit applicant's identification should be authenticated through some instantaneous means of identity risk assessment <u>before</u> credit is extended.

2) Consumers should be able to protect themselves by controlling whether credit is extended in their name to prevent identity thieves from quickly and easily receiving credit using another person's information.

Further research is needed to consider each of these recommendations in business policy changes and their impact on the system dynamics model. Resistance to policy changes needs to be evaluated in view of current policies, parties affected, and principles of corporate governance and accountability (The Critical Infrastructure Protection Program Report, 2004, p. 1).

By using a model to explore the underlying causes of a problem and its feedback loops, decision-makers have a new mental model substantiating policy options. Complex problems, such as identity theft, can be modeled incorporating multiple viewpoints to produce the best possible representation of the problem. This particular system dynamics model demonstrates that exponential growth in the ***Identity Theft*** sector is driven by exponential growth in the ***Credit Economy*** sector by easily accessible credit using exposed personal information in the ***Information Exposure*** sector. While efforts in law enforcement and businesses protecting personal information are an integral part of the cycle to counteract identity theft, those actions alone will never be enough to reduce the exponential growth in identity theft. Technological solutions, legislation, and business practices should focus preventive efforts at the point of application for consumer credit with more thorough customer identification processes, *before* identity theft occurs.

Bibliography

Associated Press. (2004, June, 8). Credit card use cools in April: Despite slowdown, consumer debt rises to a record. Boston Globe. Retrieved June 10, 2004 from http://www.boston.com/business/articles/2004/06/08/credit_card_use_cools_in_april/

Aversa, J. (2004, June 7). Credit card spending growth slows in April. *USA Today*. Retrieved June 10, 2004 from http://usatoday.com/money/economy/fed/2004-06- 07-credit_x.htm

Barua, A. & Whinston, A. (2001) Internet Economy Indicators http://www.internetindicators.com/

Bass, G. (2003, September 15). Case study: One company's response to the California identity theft law. *SANS Institute*. Retrieved January 26, 2004, from http://www.sans.org/rr/papers/11/1260.pdf

Benner, J., Givens, B., & Mierzwinski, E. (2000, May) Nowhere to turn: Victims speak out on identity theft: A CALPIRG/Privacy Rights Clearinghouse Report. Retrieved June 26, 2004 from http://www.privacyrights.org/ar/idtheft2000.htm

Bettelheim, A. (2000, March 11). Congress urged to do more to combat identity theft and ensure victims' rights. *Congressional Quarterly Weekly*. Vol 58, no. 11, 543.

Bianchi, C. & Bivona, E. (2002) Opportunities and pitfalls related to e-commerce strategies in small-medium firms: a system dynamics approach. *System Dynamics Review*. 18(3), 403-429. Retrieved August 26, 2004 from Wiley InterScience Web site http://www3.interscience.wiley.com/cgi-bin/fulltext/98518314/PDFSTART

Brandt, A. (2003, October). California law protects us all from security breaches. PC World. Vol 21, no. 10. October, 2003. Retrieved February 17, 2004 from Wilson Web database.

Brown, R. & Kane, J. (2002, September). Identity theft. National White Collar Crime Center Web site http://www.nw3c.org/

Bureau of Justice Statistics. (2004). Retrieved June 16, 2004 from http://www.albany.edu/sourcebook/

Clark, R. N., Goodyear, M., & Updegrove, D. (2003, November). Damage control: When your security incident hits the 6 o'clock news. EDUCAUSE conference proceedings video. http://www.educause.edu/conference/annual/2003/resources.asp

Consumer Reports. (October, 2003). Stop thieves from stealing you. Consumer's Union. October, 2003. Vol. 68, Iss. 10 p 12-17. Retrieved February 26, 2004 from http://proquest.umi.com/pqdweb?index=15&did=000000487821271&SrchMode=3&sid=1&Fmt=4&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1077805970&clientId=50078

Consumer's Union (Publisher of Consumer Reports), Consumer Federation of America, & U.S. PIRG. (2004, January 7). 2003 Changes to the Fair Credit Reporting Act: Important steps forward at a high cost. Retrieved March 12, 2004 from http://www.pirg.org/consumer/pdfs/fcrafinalsumm.pdf

Crimes and Criminal Procedures, 18 U.S.C. Sect. 1028 (2000).

Dean, S. (2004, June 10). Consumer confidence is up, but that may not mean your own. *ContraCosta Times, Inc*. Retrieved June 16, 2004 from http://www.contracostatimes.com

Electronic Frontier Foundation. (2003, October 27). Analysis of the provisions of the USA Patriot Act that related to online activities http://www.eff.org/Privacy/Surveillance/Terrorism/20011031_eff_usa_patriot_analysis.php

Electronic Privacy Information Center. The USA Patriot Act (EPIC) September 24, 2001. http://www.epic.org/privacy/terrorism/usapatriot/

Emarketer.com Web site. Retrieved May 24, 2004 from http://www.emarketer.com/

Equal Credit Opportunity Act 15 U.S.C. Sect. 1691 (d) (2000).

Equifax Web site http://www.equifax.com/

Evans, D. (2002, October 3). Secretary of Commerce press release on the case for confidence. Retrieved from Department of Congress Web site September 4, 2004 http://www.commerce.gov/opa/press/2002_Releases/Oct_03_Evans_memo.htm

Fair and Accurate Credit Transaction Act, Pub. L. 108-159, (2003)

Fair Credit Reporting Act (FCRA) 15 U.S.C. Sect. 1681 g (a) (1) (2000).
H.R. 4311, Identity Theft Prevention Act ., 106th Congr., 2d Sess. Sect. 2 Sect. 3 (g) (2000).

Federal Register Vol. 64, No. 207 October 27, 1999. Notices p. 57887-90. http://www.ftc.gov/foia/031103privact1974.pdf

Federal Reserve Bank of Philadelphia Web site. Supervision Regulation, and Credit. Consumer Finances -- Recent Trends in Consumer Finances and a Look at Consumer Debt. Retrieved September 2, 2004 from http://www.phil.frb.org/src/specialstudies/cfarticle3.html

Federal Trade Commission. (2003, December). Information compromise and the risk of identity theft: Guidance for your business. Retrieved February 22, 2004 from www.ftc.gov/bcp/conline/pubs/buspubs/idtbizkit.htm

Federal Trade Commission. (2004). Privacy choices for your personal financial information. Publication FRB1-xxx-0202. Retrieved from FTC website June 19, 2004 www.ftc.gov

Federal Trade Commission Consumer Sentinel. (January 22, 2004). National and State Trends in Fraud & Identity Theft January – December 2003. http://www.consumer.gov/sentinel/pubs/Top10Fraud2003.pdf

Fisher, D. (2004, May 24). Tales of cyber-crime running rampant. Retrieved from eWEEK.com Web site May 30, 2004. http://www.eweek.com/article2/0,1759,1597360,00.asp

Fleck, C. (2004, February). Stealing your life: Identity thieves hit nearly 10 million Americans last year – could you be next? Retrieved February 9, 2004 from AARP Web site http://www.aarp.org/bulletin/yourlife/Articles/a2004-01-28-stealinglife.html

Free Republic.com Web site as reprinted from *Houston Chronicle* (2003, March 5) Hackers access UT database, nab 59,000 names, social security numbers. http://www.freerepublic.com/focus/news/857910/posts

Foley, L. (2002). Fact Sheet 17L: Should I change my Social Security number? Identity Theft Resource Center. http://www.idtheftcenter.com/html/fs115.htm

Gerard, G., Hillison, W., & Pacini, C. (2004, April 19). What your firm should know about identity theft. *Journal of Corporate Accounting and Finance*. 15(4), 3-11. Retrieved August 26, 2004 from Wiley InterScience Web site http://www3.interscience.wiley.com/cgi-bin/abstract/108069281/ABSTRACT

Givens, B. (2000, July 12). Identity theft: How it happens, its impact on victims, and legislative solutions. Testimony for U.S. Senate Judiciary Subcommittee on Technology, Terrorism, and Government Information. Retrieved May 27, 2004 from http://www.privacyrights.org/AR/id_theft.htm

Givens, B. (2003). How many identity theft victims are there? What is the impact on victims? Recent surveys and studies from the Identity Theft Resource Center, Federal Trade Commission, Garner, and Privacy & American Business. Privacy Rights Clearinghouse Web site accessed May 29, 2004 www.privacyrights.org

Harris Interactive (2003, August). Identity theft new survey and trend report. Commissioned by Privacy & American Business. Retrieved June 20, 2004 from http://www.bbbonline.org/idtheft/IDTheftSrvyAug03.pdf

Henriksen, D. (2001, February 22). School of Criminal Justice implements project to combat identity theft. Retrieved August 26, 2004 from Michigan State University Web site http://www.msutoday.msu.edu/research/index.php3?article=77861477322c1f2e43fdfabba0ab2dae

Hicks, M. (2004, August 27) Reactions mixed to federal fraud sweep. http://www.eweek.com/article2/0,1759,1640354,00.asp

Hurley, E. (2003, October 1). Coalition to help enterprises manage identities against theft. YaHoo News. Retrieved October 1, 2003 from http://news.yahoo.com/news

ID Analytics Web site http://www.idanalytics.com

Identity Theft and Assumption Deterrence Act, Pub. L. No. 105-318 (1998).

Identity Theft Prevention and Survival Web site http://www.identitytheft.org/

Identity Theft Protection Web site for state and federal laws related to identity theft. http://www.identity-theft-protection.com/laws.html

Internet World Stats. Web site for usage and population statistics. Accessed October 22, 2004. http://www.internetworldstats.com/stats.htm

Jewell, M. (2004a, July 6). Credit card theft brings fresh attention to growing problem. Retrieved July 7, 2004 from *USAToday.com* http://www.usatoday.com/tech/news/computersecurity/2004-07-06-idtheft_x.htm

Jewell, M. (2004b, August 10). Big trust in databases leads to big ID thefts. Retrieved July 7, 2004 *from The Seattle Times*. http://seattletimes.nwsource.com/html/businesstechnology/2002001059_credittheft10.html

Korzeniowski, P. (2004, June 19). Consumer alert: Identity theft on the rise. TechNewsWorld. Retrieved June 19, 2004. http://www.technewsworld.com/story/34571.html

Killian, M. (1997, June 15). About credit cards – they're just like drugs. Retrieved June 10, 2004 from http://credit.about.com/cs/anticredit/a/061597_p.htm

Krim, J. (2003, February 19). 8 million credit accounts exposed. *Washington Post.* Retrieved September 25, 2003 from Web site http://www.washingtonpost.com

Kucher, K. (2004, March 17). Personal data at risk, thousands are warned. *The San Diego Union-Tribune.* Retrieved March 19, 2004 from Web site http://www.signonsandiego.com/news/computing/20040317-9999-news_7m17hacker.html

Laganas, A. (2002, August 1) State searches for cause of social security mishap. Retrieved January 15, 2004 from http://www.turnto10.com/news/1590184/detail.html

Lemke, T. (2004, July 16). Penalties stiffened for identity theft *The Washington Times*. Retrieved July 20, 2004 from http://washingtontimes.com/ Article ID: 200407161257320045

Litan, A. (2003a, July 7). Underreporting of identity theft rewards the thieves. Gartner research note number M-20-3244. Retrieved from Gartner database May 27, 2004. https://gartner.jmu.edu/research/116000/116066/116066.html

Litan, A. (2003b, July 7). Identity theft fraud prevention solutions start to proliferate. Gartner research note number M-20-4466. Retrieved from Gartner database May 27, 2004. https://gartner.jmu.edu/research/116000/116064/116064.html

Litan, A. (2003c, September 4). Reduce identity theft by rectifying too-easy credit issuance. Gartner research. Retrieved from Gartner Website search March 10, 2004 http://www.gartner.com

Litan, A. (2003d, September 23). Study shows financial firms need to act against identity fraud. Gartner research. Retrieved from Gartner Website search March 10, 2004 http://www.gartner.com

Litan, A. (2003e, November 13). Application fraud and rising identity theft plagues banks. Gartner research note number M-21-3811. Retrieved from Gartner database May 27, 2004. https://gartner.jmu.edu/research/118400/118450/118450.html

Litan, A. (2003f, November 26). Identity theft measures in U.S. FCRA bill are inadequate. Gartner research. Retrieved from Gartner Website search March 10, 2004 http://www.gartner.com

LoPucki, L. M. (2003, April). Did privacy cause identity theft?. *Hastings Law Journal*, 54(4). Retrieved March 16, 2004, from http://ssrn.com/abstract=386881

LoPucki, L. M. (2002) Human identification theory and the identity theft problem. *Texas Law Review*, 80, Forthcoming http://ssrn.com/abstract=263213

Lyman, P. & Varian, H. (2003). “How much information”. Retrieved November 1, 2004 from http://www.sims.berkeley.edu/research/projects/how-much-info-2003/

Market Wire Website. (2003, January 7). Protecting consumers from identity theft. Las Vegas. Retrieved from http://www.marketwire.com/mw/release_html_b1?release_id=49938

Mayer, C. & Witte, G. (2004, July 19). Checking account fraud is increasing. *Washingtonpost.com.*

McIntyre, D. (November 4, 2003). Database security: Finding out when your information has been compromised. Testimony of President and CEO, TriWest Healthcare Alliance to the U.S. Senate Judiciary Committee, Subcommittee on Terrorism, Technology and Homeland Security. Retrieved February 23, 2003 from http://judiciary.senate.gov/testimony.cfm?id=983&wit_id=2791

Michigan State University Web site on Identity theft: Partnerships in prevention. Accessed August 31, 2004 http://www.cj.msu.edu/~outreach/identity/

Milne, G. R. (2003). How well do consumers protect themselves from identity theft? Journal of Consumer Affairs Vol 37, No 2, 388-402. Retrieved February 17, 2004 from Wilson Web database http://vnweb.hwwilsonweb.com/hww/shared/shared_main.jhtml;jsessionid=3EPRGDUZMCBE5QA3DILSFFWADUNBIIV0?_requestid=62669

MyFICO Web site: A Division of Fair Isaac. Accessed October 12, 2004. http://www.myfico.com/myfico/CreditCentral.asp?fire=1

Office of the Attorney General State of California Department of Justice Web site. http://caag.state.ca.us/idtheft/

Oliva, R., Sterman, J., & Giese, M. (2003). Limits to growth in the new economy: exploring the 'get big fast' strategy in e-commerce. System Dynamics Review, Vo. 19, Issue 2. p. 83-117. Retrieved August 26, 2004 from Wiley InterScience Web site http://www3.interscience.wiley.com/cgi-bin/fulltext/104537714/PDFSTART

Organization for Economic Co-operation and Development. http://www.oecd.org/home/

PRNewswire. (2004, June 17). Trailblazing identity theft forum on banking, credit card and retail issues from a corporate perspective. Retrieved from Web site June 19, 2004 http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=109&STORY=/www/story/06-17-2004/0002195084&EDATE

Pacifici. S. (2003, February 17) Identity theft: A bibliography of federal, state, consumer and news resources. Retrieved January 14, 2004 from Law library resource exchange Web site http://www.llrx.com/features/idtheft.htm

Privacy Act, Pub. L. No. 93-579, (1974).

Public Interest Research Group. (2003, September 9). Credit reporting bill is a Trojan horse: Please oppose HR 2622 unless amendments protecting stronger state privacy laws are included. Retrieved February 26, 2004 from Web site http://www.pirg.org/consumer/pdfs/hr2622floor.pdf

Ritter, T. (January 12, 2003). Financial institutions required to do their part to fight crime. Retrieved January 26, 2004 from Sans Institute Web site http://www.sans.org/rr/papers/31/900.pdf

Roberts, P. (2004, August, 24). Merchant group helps DOJ in fraud stings. Retrieved August 30, 2004 from InfoWorld Web site http://www.infoworld.com/article/04/08/26/HNmerchantfraud_1.html

S.1350, Notification of Risk to Personal Data Act, 108th Cong., 1st Sess. (2003)

SNL Financial. (2004, September 28). Top 50 banks in the United States ranked by asset size. Retrieved October 25, 2004 from http://www.snl.com/bank/vitals/top_50_banks.asp

Solomon, M. (2003, March). Is California asking for too much information? *USBanker*, 113 (3), 20. Retrieved February 18, 2004 from http://proquest.umi.com/pqdweb?index=13&did=000000299706831&SrchMode=3&sid=1&Fmt=3&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1077044718&clientId=50078

Solove, D. (2003, April). Identity theft, privacy, and the architecture of vulnerability. Hastings Law Journal, Vol. 54, p. 1227, 2003. http://ssrn.com/abstract=416740.

Sovern, J. (2003). The jewel of their souls: Preventing identity theft through loss allocation rules. University of Pittsburgh Law Review. Vol 64, no. 2. Winter, 2003. Retrieved February 17, 2004 from Wilson Web database http://vnweb.hwwilsonweb.com/hww/shared/shared_main.jhtml;jsessionid=3EPRGDUZMCBE5QA3DILSFFWADUNBIIV0?_requestid=61850

Sterman, J.D. (2000). Business Dynamics: Systems Thinking and Modeling for a Complex World. Boston: McGraw-Hill.

Strategic Research Institute. (2004, June). ID theft in financial services: Cause. Effect. Remedies. Conference agenda June 30- July 1, 2004, New York City. Retrieved June 13, 2004 from Web site http://www.srinstitute.com/ApplicationFiles/web/WebFrame.cfm?web_id=264

Sullivan, B. (2002, June) The moral dilemma of data leaks. MSNBC. Retrieved March 4, 2004 from http://www.cardcops.com/msnbc/msnbc6.htm

Sullivan, B. (2004a, May 21). Study: ID theft usually an inside job: Up to 70 percent of cases start with employee heist. MSNBC. Retrieved June 10, 2004 from http:///www.msnbc.com

Sullivan, B. (2004b, June 14). Survey: 2 million bank accounts robbed: Criminals taking advantage of online banking, Gartner says. MSNBC. Retrieved June 16, 2004 from http://www.msnbc.msn.com/id/5184077

Sullivan, B. (2004c). *Your evil twin: Behind the identity theft epidemic*. Hoboken, NJ: Wiley.

Synovate. (2003, September). Federal Trade Commission: Identity theft survey report. http://www.ftc.gov/os/2003/09/synovatereport.pdf

Tan, K. (2004, March 6). AmBank targets 150% credit card growth in FY05. The Edge Asia. Retrieved June 10, 2004 from http://www.theedgeasia.com

The Critical Infrastructure Protection Program Report. (2004, September). 3(3). Published by Zeichner Risk Analyitics, LLC.

The New York Job Source. (2004, January 21). The 20 largest banks in the U.S. Retreived October 25, 2004 from http://nyjobsource.com/banks.html

The USA Patriot Act, Pub. L. No. 107-56, Section 326 (2001).

Turban, E., Rainer, R. & Potter, R. (2003). Introduction to Information Technology, 2nd ed. Hoboken, New Jersey: John Wiley & Sons.

U.S. Department of Commerce. Retrieved September 6, 2004 from http://www.economicindicators.gov/

U.S. Department of Justice. (2002). Strategic Plan 2003-2008 Section 2.3 http://www.usdoj.gov/jmd/mps/strategic2003-2008/chapter2.pdf

U.S. Department of Justice Web site. Federal justice statistics accessed October 15, 2004 from http://www.ojp.usdoj.gov/bjs/fed.htm#Prosecution

U.S. Department of State Web site (2004, August 26) Justice Department Targets Online Fraud, Attorney General Says. Retrieved from Web site August 30, 2004. http://tokyo.usembassy.gov/e/p/tp-20040827-17.html

Vijayan, J. (2004, January 5). Data security breaches reveal encryption need. Computerworld. Retrieved February 26, 2004 from Web site http://www.computerworld.com/industrytopics/financial/story/0,10801,88663,00.html

Visa Web site. Accessed September 7, 2004. http://usa.visa.com/personal/newsroom/visa_security.html?it=il/personal/newsroom/visa_faq.html

Willox, N. Jr., & Regan, T. (2002, March). Identity Fraud: Providing a Solution. Retrieved May 27, 2004 from LexisNexis database. http://www.lexisnexis.com/about/whitepaper/IdentityFraud.pdf

Wolk, M. (2004, Jan. 18). The pitfalls of plastic: Credit-dependent Americans pushed to the edge. MSNBC News. Retrieved June 16, 2004 http://msnbc.msn.com/id/3981954/

Appendix A: Timeline of Important Developments

Year	Business Practice	Technology	Legislation	Impact
1950s	Credit industry mails unsolicited active credit cards to consumers	Paper processing		Fraud incidents increase
1960s	Expansion of consumer lending			Consumer credit debt growth
1970s		Wait time on transaction authorization reduced to 1 minute	Privacy Act of 1974	
		Merchants transmit authorized transactions electronically		
1980s	Global ATM network providing 24-hour cash access to cardholders	Electronic data capture point-of-sale terminals		Credit card fraud rises
		Identify suspicious card activity at merchant locations		Visa sales volume doubles.
	Customer card need not be present at point of sale	Magnetic stripe on credit cards		Visa expands to China and Russia
1990s	Selling customer data; target marketing for customer solicitation	Internet; data mining		
	Mail order catalog industry grows	Neural networks to detect spending anomalies as alerts		
	Credit industry mails unsolicited convenience checks	Hackers stealing data from unsecured databases	1998 – Identity Theft Assumption Deterrence Act	Fraud reported to FTC increases to 42% per year
2000	Customer initiated electronic payments	On-line banking	Equal Credit Opportunity Act	
	Zero liability policy on fraud transactions			
	Financial industry largest backers of presidential campaign, both parties			
2001		Hand-held device payment via infrared technology		Terrorist activities funded largely by credit card fraud
			USA Patriot Act	Customer identification program
2002		Bank fraud detection software nightly processing of new account anomalies		
2003		Phishing – e-mail solicitation of personal information	Fair Credit Reporting Act amended	Consumers entitled to one free credit report per year
2004	Truncating card number on transaction receipts		Mandatory additional time if crime involves identity theft	