# Identity Theft:

## An Exploratory Study with Implications for Marketers

Eric M. Eisenstein

*Forthcoming: Journal of Business Research*



Eric M. Eisenstein is an Assistant Professor at the Johnson Graduate School of Management, Cornell University. I thank Charles Nicholson, Peter Otto, George Richardson, and the participants of the System Dynamics and Marketing Strategy workshop held at Cornell University in May of 2007 for their insightful comments, suggestions, and aid in model development. This research was funded by Cornell University.

Correspondence concerning this article should be addressed to
Eric M. Eisenstein
The Johnson Graduate School of Business, Cornell University
321 Sage Hall, Ithaca, New York 14853
Phone: 607-255-8627
Fax: 607-254-4590
Email: eme23@cornell.edu

**Abstract**

Identity theft is the fastest growing crime in America, and millions of people become victims each year. Furthermore, identity theft costs corporations over $20 billion per year, and consumers are forced to spend over $2 billion and 100 million hours of time to deal with the aftermath. This paper uses a system dynamics model to explore policy options dealing with identity theft and to provide implications for marketers. The results indicate that the current approach to combating identity theft will not work. However, inexpensive security freezes could be effective, because they result in a nonlinear reduction in identity theft that is similar to the "herd immunity" seen in epidemiology. Thus, identity theft can be addressed by protecting just a fraction of the total population.

# Identity Theft: An Exploratory Study with Implications for Marketers

"It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently." – Warren Buffet

The quote above is particularly true in our networked electronic age, in which information about any one of us can be transmitted around the world in a matter of seconds. Identity theft is a crime that compromises one's reputation in a few minutes, often without awareness of the victim, and with long term and possibly devastating consequences to the victim's financial position. In the last several years, consumers have been almost continuously exposed to heartrending stories of identity theft and recovery of the victims. Identity theft has been called *the* crime of the 21st century, both due to its rapid growth since 2000 and because it relies on the extensive computer networking and architectures that enable the U.S. economy to exist in its current form. Secretary of the Treasury John Snow has called identity theft "the greatest threat to consumers today…" because identity theft "…destroys the trust in both people and financial institutions that is necessary to run an open, modern economy" (Snow 2003). Because of the publicity surrounding identity theft, it also ranks as one of the most important worries among consumers (Consumers Reports WebWatch 2005; Federal Trade Commission 2007).

## What is identity theft?

At the most general level, identity theft is "…the misuse of another individual's personal information to commit fraud" (Gonzales and Majoras 2007). Most reporting agencies recognize two major subcategories of identity theft: existing account fraud, in which a thief takes over or appropriates an existing account or credit relationship, and new account fraud, in which a thief uses personal information to open new accounts and credit relationships in the victim's name.

Existing account fraud is more prevalent and typically less costly than new account fraud (Anderson 2006; Gonzales and Majoras 2007; Javelin Strategy and Research 2007b). Although existing account fraud may result in thousands of dollars of charges to a credit card, laws and corporate policy limit consumer liability for such fraudulent charges, and existing account fraud rarely affects an individual's credit rating. By contrast, new account fraud costs approximately $850 dollars and 80 hours of time per victim to correct when it is first discovered (Javelin Strategy and Research 2007b). Moreover, whereas existing account theft is generally over at the time of detection (when the fraudulent account is closed), new account fraud is a symptom of a larger problem – that a thief has stolen one's identity. As a result, new account fraud can continue occurring for years before the thief is caught (as the thief continues to open new additional accounts), and the fraud can have a disastrous effect on the victim's credit rating (even if each occurrence is temporary). Because of the severity of the new account identity theft problem, the analysis focuses only on it.

*How does new account theft occur?*

The first step in becoming a victim of identity theft is that a criminal must obtain the victim's identity information, either through low-tech methods such as "dumpster diving" (i.e., rooting through garbage for personal information) or stealing mail, or by using higher-tech methods such as hacking into a corporate computer system, stealing a laptop containing identity information, "phishing" (i.e., fooling a customer into revealing information through a fake website or email), or using malicious computer code to obtain the information (Gonzales and Majoras 2007). Once identity information is obtained, the criminal either uses it directly (if it is account information in the case of existing account fraud), or applies for credit by posing as the victim (in the case of new account fraud). After the application for credit, almost all potential lenders check applicants' credit scores with one of the three major credit bureaus (i.e., Experian, Equifax, and TransUnion). The bureau reports back a credit score, and, based on that score, the

lender chooses whether to extend credit. If the fraud is successful, the lender and the bureau are deceived as to the true identity of the applicant, and the thief obtains credit in the name of the victim. At some point in the future, either the victim or a lender notices the theft, and the resolution process begins by closing the fraudulent account.

*Combating Identity Theft*

Based on how identity thieves exploit the system, there are two overarching approaches to controlling identity theft, which I term *control of information* and *control of use*. Control of information refers to efforts to reduce criminal access to social security numbers and other identifying information about individuals. Control of use refers to tightening procedures surrounding validation of submitted identity information, once an application for credit has taken place, in order to control the usefulness of personal identifying information. Using control of information to combat identity theft is important, but is unlikely to significantly reduce the rate of identity theft. The reasons are that (a) identity information is very widely distributed (particularly social security numbers), which means that there are many potential sites of attack; (b) would-be thieves are diligent and resourceful in stealing or obtaining needed information; (c) previous laws that increased penalties for theft have had little or no impact on identity theft rates. A more realistic approach would be to assume that identity information will fall into malicious hands and to reduce the usefulness of such information (i.e., a control of use strategy). One way of reducing the usefulness of information is to use electronic monitoring services to inform consumers of changes to their credit files (Javelin Strategy and Research 2004; Javelin Strategy and Research 2007a). Monitoring services are fundamentally reactive, as they inform the account owner of a change only after it has occurred. Furthermore, monitoring systems rely on the account owner's continual vigilance, which is a shaky foundation, because people go on vacation, "spam" filters block email, servers crash, and other things interfere with notification. What monitoring does best is to substantially reduce the time from theft to detection, but

monitoring does not prevent a significant amount of identity theft. A second means to reduce the usefulness of information is to create or exploit information bottlenecks in the system, breaking the credit-granting chain of events. There is a natural bottleneck when a credit score is requested from one of the three credit bureaus, because it is almost impossible to open a new credit line without checking with one of the three major bureaus. Thus, the bureaus serve as a natural focal point for preventative measures. One possibility would be to restrict access to credit bureau information about individuals, and a so-called "security freeze" is the legal implementation of this concept. When someone "freezes" their credit bureau file, it means that that the file cannot be shared with potential creditors, which essentially shuts down the possibility of opening a new account. In order for a consumer to open new legitimate lines of credit, she must "thaw" the file, either for a specified period of time, or for a given lender. There is currently no uniform national right to a security freeze; all legislation is at the state level.

**Identity theft and marketing**

Identity theft results in between $17 and $35 billion in losses to retailers and lenders each year, which makes it a major source of loss for companies that market to consumers (Gartner Inc. 2007; Javelin Strategy and Research 2007b). However, the implications of identity theft for marketing are more serious than the direct monetary cost. Identity theft costs corporations substantial amounts of money in the form of preventative services that must used to insulate the business against fraud. More importantly, it is not an exaggeration to say that identity thieves have been enabled by our current marketing practices, and continued concern over identity fraud risks a consumer and legislative backlash against critical marketing activities. It is insightful to compare Europe and America to see how much things could change for American marketers. Identity theft rates are so low in Europe that there are few surveys or statistics to report. In the highest incidence country (Britain) the total identity theft rate is over twenty times less than in America, with the incidence estimated to be 0.17% of the population in Britain vs. 3.9% per year

in America (Weston 2005). The reasons for this disparity are telling: Europe has almost no access to instant credit, companies are largely forbidden from sharing or selling personal data, credit bureaus are tightly regulated as far as who may communicate with them and for what purpose, and debit outranks credit as the preferred means of payment (Weston 2005).[1] If identity theft continues to grow in America, it is easy to imagine regulations that will deprive marketers of our most valuable tools: CRM databases (which are hacked to obtain stored information; e.g., the TJMaxx theft, see Nakashima and Mui 2007); access to instant credit, which is almost necessary for the marketing of some products; the ability to share consumer data with business partners; and tight restrictions on the opening of new accounts. Restricting any of these tools would have a massive negative impact on marketing across almost all industries. Moreover, fear of identity theft is reducing consumer use of Internet shopping (Javelin Strategy and Research 2007b). As a result, controlling identity theft should be a concern for marketers.

The article proceeds as follows: I briefly review the existing literature on identity theft, I describe the creation of a system dynamics model of new account identity theft which can be used to perform policy experiments, and I discuss the conclusions and limitations of the model.

## Literature Review

Identity theft is a new phenomenon. As a result, the literature is not mature, and numerous authors have indicated that additional research is needed (e.g., Anderson 2006; Cheney 2003; Newman and McNally 2005). Most recently, Anderson (2006) explored the effect of demographics on identity theft, finding that being female, having children in the household, and region of the country were significant predictors of new account identity theft, but that income, race, and age were not significant. Newman and McNally (2005) provide a general review of the literature regarding law enforcement, criminal motivations, and a limited number

[1] There are other important non-marketing differences as well. Most European countries use a national identity card, and this number is not as widely distributed as American social security numbers are. Also, many European credit cards use a swipe-with-PIN architecture, which substantially reduces existing account fraud.

of options for prevention. Several papers address problems associated with the use of social security numbers as passwords or identification (e.g., LoPucki 2001; Menton Jr. 2002; Solove 2003). Solove and Hoofnagle (Hoofnagle 2005; Solove 2003) suggest comprehensive changes to the architecture of privacy to combat identity theft from a legal perspective. Among other recommendations to strengthen consumer control over the use of their identifying data, these authors suggest near ubiquitous use of security freezes. Sovern (2003; 2004) examined how the allocation of liability for the costs of identity theft among consumers, credit reporting agencies, and creditors could affect the incidence of identity theft. Kahn and Roberds (2005) develop a purely theoretic model in which identity theft will exist in equilibrium because the costs of increased conclusiveness in identification outweigh the benefits. Numerous (usually nonacademic) surveys have examined the incidence of identity theft (e.g., CyberSource Corporation 2007; Gartner Inc. 2007; Javelin Strategy and Research 2007b); other surveys have investigated consumer attitudes toward electronic monitoring (Javelin Strategy and Research 2004; Javelin Strategy and Research 2007a), and willingness to pay for security freezes (Sauer 2006). Several authors have examined how well consumers have adopted practices that have been suggested to reduce the risk of identity theft (Mayer 2006; Milne 2003; Milne et al. 2004). Consistent with the predictions of economic theory, Bolton, Cohen, and Bloom (2006) show that providing consumers with insurance to cover their out-of-pocket expenses resulting from identity theft makes them more likely to engage in behaviors that risk compromising their identity. There are also several papers that examine the effect of identity theft on the health of victims (Foley and Foley 2004; Sharp et al. 2004). Thus far, however, no one has attempted to model the dynamics of identity theft in such a way that policymakers can see the effects of potential policy changes.

## Combating Identity Theft

There are numerous suggestions for what can be done to combat identity theft. Almost

everyone seems to agree that reducing reliance on the use of social security numbers as identification numbers is desirable (e.g., Gonzales and Majoras 2007; LoPucki 2001; Newman and McNally 2005). These same authors agree that increasing the protection of governmental and corporate computer systems against hacking and intrusion is desirable, although there appears to be no cost-benefit analysis supporting this recommendation. Nonetheless, there are good reasons to believe that such policies will not address the problem. First, concerns have long been voiced about the use of Social Security numbers for identification purposes, but economic pressure toward having a unique national identifier has continuously pushed for their use. Second, numerous laws already restrict the use of social security numbers, but they have had little impact on identity theft, because opportunities for compromise of the information are simply too numerous. Criminals obtain social security numbers with great frequency. For example, the Privacy Rights Clearinghouse estimates that, from 2005 until the middle of 2007, known data breaches resulted in the compromise of over 155 million records containing personal information (Privacy Rights Clearinghouse 2007), and many news outlets have written about the brazen marketing identity information on websites, facilitated by various anonymous electronic payment schemes (e.g., Symantic Corporation 2007; Zeller 2005).

Other suggestions for combating identity theft include consumer education on the importance of shredding documents containing personal information, using firewalls, virus scanners, and spyware detection, controlling access to sensitive information, etc. (Milne 2003; Milne et al. 2004). However, rapid continued progress in this area is unlikely because most consumers believe that they are already "doing their part," to prevent identity theft by shredding sensitive documents, using anti-virus software, and other similar preventative activities (Javelin Strategy and Research 2007b p. 27, Figure 16; Mayer 2006).

Other options that can be used to fight identity theft include increasing the use of electronic monitoring services and security freezes. Both of these options are now readily

available to most consumers. These options both control the usefulness of information that falls into the hands of thieves, which makes them complimentary to the various initiatives addressing control of the information itself. I will focus attention on monitoring and security freezes because monitoring is the most aggressively marketed complement to the control of information, and because security freezes are one of the most common legislative initiatives being considered to fight this crime. I hypothesize that:

1. Prevention will dominate reaction; security freezes will prove much more potent than monitoring at reducing identity theft.
2. There will be a nonlinear effect of protection on theft: the more protected people, the less incentive thieves have to steal (cf., Newman and McNally 2005), and this will produce a nonlinear "herd-immunity"-like effect of freezes on theft.

Furthermore, the model should explain certain observations about the market, including why credit bureaus are opposed to security freeze legislation.

3. Credit bureaus are opposed to security freeze legislation because freezes adversely affect their profits.

## A System Dynamics Model of Identity Theft

To test these hypotheses, I developed a system dynamics model of identity theft. Richardson (1996) defines modern system dynamics as "a computer-aided approach to policy analysis and design." In order to permit policy analysis and design, the model must account for both corporate and human behavior. Identity theft is a result of a complex web of interacting agents, and it is important to model the motivations and actions of these agents at an appropriate level of detail. This model covers only the adult population of the United States, and it examines the effects of consumer and governmental policies only on new account identity theft. It is clear that lenders (and probably consumers) want instant credit approvals, because such approvals allow people to mentally convert a major expenditure into something similar to an impulse

purchase. This behavior needs no specific modeling behind it, because it is how the credit-granting system works today. I assume that identity thieves want to steal as much money as they can, and the credit bureaus (and other purveyors of monitoring services) are profit maximizing. I model individuals as if identity theft affects them as a person, rather than modeling at the account level because this is the level of aggregation at which data is collected. Figure 1 shows a simplified view of the model that displays the major stocks, flows, and critical variables. The actual simulation model is considerably more detailed, containing over one hundred causal links; a detailed discussion of the model would exceed the scope of this article. Those interested in the complete model can download a free version (Vensim PLE) of the simulation software used to conceptualize the model (www.vensim.com) and contact the author for a copy of the model.

---

Insert Figure 1 About Here

---

*Consumer Behavior*

Based on the current options that are under consideration for combating identity theft, consumers must choose among three mutually exclusive *states of protection*, which include electronic monitoring of credit reports (Monitored), using a security freeze to freeze the report (Frozen), and those with neither monitoring nor security freezes (Unprotected; see Figure 1).[2] The upper set of stocks and flows in Figure 1 represents individuals choosing among states of protection. The lower set of stocks and flows represent individuals who have become victims. As Figure 1 shows, individuals are subject to different risks of identity theft that depend on their state of protection (Figure 1, "Probability of Fraud Success" variables). Once a person becomes a victim, they temporarily move into the "Active Fraud" stock associated with their state of protection. During the time that the person is in the active state, identity thieves make money on

[2] It is possible that consumers could have both electronic monitoring and security freezes. However, given the very small number of people who have frozen accounts under existing laws and the fact that freezes protect so well against fraud, the overlap set was not incorporated into the model.

the account through theft (and people do not change protection status during the time that they are being victimized). The time required to detect the theft also varies by consumer state ("Time to Detection").

Anderson (2006, table 5) has shown that identity thieves have little ability to target consumers for new account theft based on wealth or other predictors of how much money they will eventually be able to steal (cf., Javelin Strategy and Research 2007b). As a result, the rate of identity theft varies by consumers' protection state but not by demographics. Various studies report the fraction of people in each of these categories who were victimized (e.g., Anderson 2006; CyberSource Corporation 2007; Javelin Strategy and Research 2005; Javelin Strategy and Research 2007a). Differences in probability of fraud and time to detection across states of protection are shown in Table 1.

---

Insert Table 1 About Here

---

*Behavior of Identity Thieves*

Being an identity thief is a risky proposition: there have been hundreds of identity theft-related arrests, there are thousands of pending cases, and there are myriad law enforcement agents working to bring perpetrators to justice. Prior research has shown that criminals require compensation for the risks that they incur (e.g., Becker 1968; Burdett et al. 2003; Viscusi 1986), and it is reasonable to assume that identity thieves behave in a similar manner to other criminals in this regard. For example, they could be doing something else with their time – either an honest activity, or some other illegal activity. I have modeled the decision making of thieves in a labor-economic framework by assuming that each criminal has a private "reservation wage" below which he will no longer engage in new account identity theft (see Freeman 1996 for a review of evidence that labor market incentives affect crime rates, with extensive use of

reservation wages in a criminal context).[3] Reservation wage refers to the minimum expected value of an attempted theft that is required to induce someone to engage in new account identity theft rather than some other activity. Although each criminal has his own reservation wage, I have assumed that the distribution of these wages is roughly bell-shaped, specifically, reservation wages follow a logistic distribution. Each criminal will cease to engage in new account identity theft if the expected value of theft falls below his reservation wage. Unfortunately, the number of attempted thefts is unobserved, and without knowing the number of attempts, a true expected value of each attempt cannot be calculated. However, under the assumption that the annual number of attempted thefts per criminal has been relatively constant over time, the observed probability of identity theft success can be used to construct a number that is proportional to the true expected value. The distribution of reservation wages used in the model is very broad, meaning that there is substantial heterogeneity in the "wage" demanded from crime (with a minimum reservation "wage" near zero dollars per attempt, reflecting a certain fraction of people who will be willing to engage in crime no matter what). Expected value is calculated from the fraction of consumers in each state of protection, and the attendant probabilities of successful theft and the average amount of money stolen from individuals in each state.

Before computing an expected value, criminals must be aware of new account identity theft as an option. Like any new product, in the early days of identity theft not all potential criminals were aware of it as an option. Under the assumption that, in 2007, the number of criminals who are aware of identity theft is near 100%, I model criminal awareness of identity theft as a logistic diffusion process with a maximum proportional growth rate of 2 (corresponding to 1% awareness in 1998, 50% around 2000, and 100% in 2004).

*Firm Behavior*

[3] Criminals may decide that engaging in other criminal activity, including existing account fraud, remains lucrative enough not to abandon a life of crime. However, existing account fraud is much less intrusive from a consumer perspective, because the responsibility for detection falls largely on businesses and because consumer liability is limited by law. As a result, even a direct substitution of new account for existing account fraud would be preferable from a consumer's perspective.

Credit bureaus and other firms who sell credit monitoring products are assumed to be profit maximizing. Electronic monitoring services provide email (and sometimes text message) support to notify consumers of certain changes to their credit files. These notifications are automatically produced by a computer program that is set up to "watch" a monitored consumer's credit file. In addition, some monitoring services are bundled with "identity theft insurance," which compensates victims for their out of pocket expenses associated with rectifying identity theft. Firms make substantial profits from selling electronic monitoring services to consumers. As of 2005, the average annual price for electronic credit monitoring was approximately $85 (Javelin Strategy and Research 2005). The variable costs associated with sending notification emails, text messages, and of running the monitoring program itself are negligible, and firms incur only a small cost for billing and customer service. Thus, monitoring is essentially 100% profit (contribution, to be precise). If insurance is offered, then there is an additional payout if fraud occurs, which is equal to the probability of victimization * (out of pocket expenses if victimized – deductible) * fraction of claims paid, where fraction of claims paid addresses the common consumer complaint that insurance companies disallow certain losses (e.g., those incurred prior to obtaining the policy). In the worst case scenario (no deductible and 100% of claims paid), insurance will cost firms approximately $10; in reality, the costs will substantially lower due to deductibles and less than 100% fraction of each claim paid. Thus, even in the worst case scenario, credit monitoring is extremely profitable, with margins of $75/$85 ≈ 88%.

Given these enormous margins, two things follow: 1) the more consumers that sign up for monitoring, the greater the profits for the credit bureaus, and 2) the companies are motivated to have enough ongoing identity theft to provide continued motivation for consumers to buy their monitoring services. It is likely that companies who sell credit monitoring also have some degree of control over the rate of identity theft. This seems plausible because firms face an economic decision governed by signal detection theory, in which they must determine how

stringent a threshold they will set for new account applicants to "prove" their identity. As in all SDT applications, if the threshold is set too high, the firm makes more type II errors, rejecting legitimate applicants, and if the threshold is set lower, the firm will make more type I errors, allowing more identity theft (see Swets 2000 for a review of SDT). I have assumed that collectively, firms can increase the rate of identity theft by 30% over the 2006 rates, and that firms will linearly increase the theft rate as the annual growth rate of their profits falls below 5%, which is a common expectation for growth on Wall Street. Thus, if profits are slipping, firms make procedural changes that result in increased amounts of identity theft. I should be clear that this is not necessarily their immediate goal, nor is it necessary to attribute malign motivations to firms. For example, imagine that firms discover that their profits are falling. One thing that they might do is to try to acquire additional customers, and one way to do this is to relax the approval threshold or to encourage the credit bureaus to relax their threshold, resulting in an increase in both fraudulent and legitimate approvals.

---

Insert Figure 2 About Here

---

*Model Dynamics*

In the model (as in the real world), the incidence of identity theft is fundamentally driven by the fraction of people in each state of protection. For the purpose of explaining the model dynamics, it is helpful to divide consumers into just two stocks, "protected" and "unprotected." Figure 2 depicts these two conceptual stocks along with the major feedback loops in the model. As shown in Figure 2, moving people from an unprotected into a protected state reduces identity theft in two ways. First, it directly reduces identity theft by prevention, decreasing total new account fraud (see Table 1). Furthermore, the number people in the protected stock exerts an indirect effect on fraud, because the number of protected people also exerts a negative effect on

the expected value of committing new account identity theft, and decreases in the expected value of fraud decrease the number of thieves who are willing to engage in theft by dropping the expected value below their reservation wage (the "Expected Value" loop). In addition, the number of people in the protected state drives credit industry profits. When the growth rate of profit falls below a target level, firms act in ways that result in an increase in identity theft, resulting in the positive feedback loop labeled "credit industry profit management." Note that all consumers exist in either an unprotected or a protected state at any given time (number unprotected = total population – number protected). Thus, these loops could just as easily have been drawn from the unprotected stock to total fraud level and to EV of fraud; however, it does not make sense to display both sets of loops simultaneously, as this would be "double counting" the effects of a shift from unprotected to protected. As fraud decreases, so does the flow from unprotected to protected, allowing more people to return to the unprotected state through natural "churn."

In Figure 2, I have simplified the model to include only two stocks. In reality, there are three stocks, with "protected" breaking down into frozen and monitored. This further division affects the stocks and flows in the following way: first, freezes are much more effective than monitoring both at directly reducing identity theft (the probability of theft is lower for people whose accounts are frozen than for monitored) and therefore at reducing the expected value of fraud (a stronger negative effect on Expected Value, and its loop). However, freezes are also much less profitable to the credit bureaus, which means that increasing the fraction of frozen vs. monitored people will reduce credit industry profits and profit growth, strengthening the credit industry profit management loop. As in many models, in this case what is important is the relative strength of these various effects, which will be discussed in greater detail below.

*Model Detail*

The critical underpinning of the model are flows among the consumer states. Initially, all

consumers begin in the unprotected state. For simplicity, population is held constant at the 2007 level. No qualitative model behaviors are changed by this assumption. Variables that affect the flow of consumers among states of protection were estimated from data, where possible.

Table 1 shows the incidence and time to detection differences among states of protection. I estimated the rate of new account identity theft by combining data from the 2003-2007 Javelin reports (Javelin Strategy and Research 2007b) and from the FTC data used by Anderson (2006), following the recommendation of Armstrong (2001) for combining forecasts by averaging. Combined, these studies produce an estimate of the incidence of new account identity theft of 1.30% of the adult population of the U.S. There are no published data on the rate of theft for individuals with security freezes, and I set this rate to be 0.01%. Because monitoring is primarily reactive and is not designed to prevent (but rather to provide quick notification of) identity theft, the rate for monitored individuals was set to be 10% lower than the rate for unprotected, and the sum was constrained so that the correct weighted average rate of theft was maintained. Time to detection for unprotected and monitored consumers are derived from the Javelin (2007a) data, and time to detection for frozen consumers was set to 20% longer than the unprotected time because people who are protected are likely to be less vigilant (Bolton et al. 2006).

There are two primary ways that consumers move from unprotected to "protected" (i.e., monitored or frozen) states. First, consumers see articles, hear news reports, and are otherwise exposed to information about identity theft, which can motivate them to sign up for some type of protection proactively. Second, consumers who discover that they are victims of identity theft are more likely to obtain protection after their discovery.

Some people will proactively obtain monitoring services. When the number of identity thefts in a given period of time has been published, news articles appear that warn people about identity theft, and the articles report on protection options that can are available to consumers. I

used newspaper articles as a proxy for total news coverage of identity theft. Specifically, I used Lexis/Nexis to determine the number of newspaper articles whose headline contained the words "identity theft" that were published in Northeast regional sources prior to June 2007. Northeast regional sources were used (rather than all outlets) because most articles are nationally syndicated, and counting only one region ameliorates any problems with double counting. I then regressed the lagged number of articles onto the rate of identity theft. Results revealed an excellent linear fit ($R^2 = .77$), with an intercept = 17.6 articles and a slope of 21.8 articles per million detected identity theft cases. The number of articles affects the fraction of unprotected consumers through a logistic response function that similar to that used in the case of reservation wages of thieves.[4] In summary, proactive adoption of monitoring is driven by reporting of the incidence of identity theft in the previous period, and news reports published in newspapers are used as a proxy for all information sources. People are assumed to maintain their monitored status for 10 years on average.

Proactive adoption of security freezes is driven by the availability of freezes, the awareness that they exist, and their cost. There is currently no national law governing security freezes, and therefore states have passed laws that govern access to freezes. Beginning with California in 2003, various states have passed laws allowing consumers to freeze their credit. Existing laws as of mid-2007 reveal that 75% of the population of the U.S. will have access to security freezes by mid-2008, and that most states passed laws for which the effective date lies between 2006 and 2008 (Consumers Union 2007). Since consumers cannot obtain a freeze without an enabling security freeze law, the fraction of the population for whom freezes are available is a model parameter, which is set to closely reproduce the actual fraction of the country covered by security freeze laws through 2008 (Consumers Union 2007). Because so few people in the country have been covered by security freeze laws, there is little data available on

[4] In this case, a logistic function with a mean = 75, asymptote = .05, and sensitivity parameter = .06 was used, with the parameters set to produce a good fit between observed uptake of monitoring service and actual uptake.

how security freezes will be received by consumers. However, in 2006, the marketing research was conducted with a representative sample of 1,200 respondents in three states (Sauer 2006) that asked consumers for their likelihood of adopting a security freeze as a function of the cost to freeze and the cost to thaw (recall that the cost to freeze is the amount consumers pay to initiate the freeze, and the cost to thaw is the amount paid to temporarily or permanently lift the freeze so that credit can be obtained). I estimated "pseudo-demand curves" from the research data by fitting an exponential distribution to the percentage of customers who checked the "top box" (i.e., extremely likely to adopt), a common heuristic for determining who will actually adopt in applied marketing contexts (Green 2002, personal communication). In both cases, the fit was excellent. For placing freezes, the estimated relationship had an $R^2 = .99$, with p("extremely likely") = 0.5346 exp (-0.1721 * cost to place freeze), and for thaws, the relationship had an $R^2 = .89$, with p("extremely likely") = 0.3145 exp(-0.1607 * cost to thaw). These curves are not true demand curves, because the AARP questions treated the cost to freeze and thaw as independent predictors of adoption, rather than modeling them jointly. Hence, in the model, I used the cost to freeze curve as the demand curve for adoption of security freezes and the cost to thaw to influence the rate at which people abandon freezes in favor of being unprotected. This seems reasonable, as the salient cost when adopting is the cost to place the freeze, while the cost to thaw is most salient during ongoing use of the freeze. Finally, in order to proactively adopt a security freeze, people must be aware that security freezes exist. There are no published data on the number of people who are aware of security freezes, though anecdotal and survey evidence suggest that the numbers are extremely low. I have assumed that awareness grew from 0% in 1998 to 0.5% of the population in 2007. Proactive adoption of freezes is driven by the product of the demand curve probability of adoption as a function of price and awareness. I allowed the thaw demand curve to influence the churn rate for thaws. The churn rate for freezes is set to 5 years when the thaw price is at its maximum, $12, and this rate is reduced by the cost to thaw

equation mentioned previously. Thus, as the cost to thaw drops, the churn rate goes down (i.e., the length of time that people will continue their freezes goes up).

A second path by which unprotected individuals obtain protection is in the aftermath of becoming a victim. When unprotected consumers detect that they are victims, 25% go on to obtain some form of protection (Javelin Strategy and Research 2007b, p. 29). The type of protection obtained is split between security freezes and monitoring. Clearly, the availability of a freeze restricts the number of people who can obtain this form of protection, and I further assume that the relative cost of placing a freeze determines the fraction of people who will freeze vs. adopting monitoring. Specifically, I assume that people are 50% less price sensitive to freezing after becoming a victim than they would have been if they had not been a victim. Because credit bureaus are required to inform consumers in most states of their right to freeze when they report that they have become victims of identity theft (if indeed they have such a right), I have assumed 100% awareness of freezes for consumers who detect identity theft. Those consumers who detect identity theft, obtain protection, and do not obtain a freeze will instead choose monitoring.

*Model Summary*

The model dynamics depicted in Figures 1 and 2 are driven by the fraction of consumers in each state of protection. For consumers in a given state of protection, Table 1 summarizes their probability of becoming a victim and the average time required to detect the compromise of identity information. The longer the account is compromised without detection, the greater the profits to identity thieves. Credit industry profits from identity theft depend on the relative fees charged for security freezes and for monitoring, and when the growth rate of profits falls below 5%, firms can increase the rate of theft by up to 30% for non-frozen accounts using a linear adjustment with a maximum at 0% growth. At any given time, some people are victimized, and once victimized, they remain in their state of protection until they detect the theft. After

detection, people are more likely to adopt some form of protection. Similarly, some people are motivated to adopt protection proactively based on fear of identity theft resulting from hearing about the amount of theft occurring. People do not remain protected forever, but "churn" due primarily to the cost of maintaining protection. People also discontinue protection when fewer thefts take place, as they judge the risk to be lower. The dynamics of the model depend on the relative strength of the loops depicted in Figure 2.

## Policy Experiments and Results

### *Model calibration*

For all policy experiments, the model was run from 1998 until 2050. By the end of 2008, approximately 75% of the country will be covered by state-level security freeze laws that have already been passed, there is very low awareness of security freezes (.01%), the population-weighted average cost of a freeze is $8.10 per bureau (given three major bureaus, the total cost is $24.30 to freeze one's credit files), and the population-weighted average cost to thaw is $7.85 (conservatively assumed to be required for one bureau per thaw).[5] Other relevant input parameters, including rates of theft and time to detection based on state of protection are the same as previously discussed. Comparing the model results from 1998 until 2007, the model generates predictions that are consistent with observed data. For example, the model output shows that, in 2006, detections of new account identity theft were 2.91 million individuals. I compared this model estimate to the to the average of new account identity theft estimated from the 2003-2007 Javelin reports (Javelin Strategy and Research 2007b) and the FTC data used by Anderson (2006), following the recommendation of Armstrong (2001) for combining forecasts by averaging. The average theft rate in these studies produces an estimate that 2.92 million new account fraud detections were observed in 2006, and the 2003 to 2006 growth rates also match

[5] The population-weighted average costs to freeze and thaw were derived from the state-level populations and costs to freeze and thaw.

closely.[6] Similarly, as of the end of 2006, 24.8 million individuals were protected by electronic monitoring (Consumers Union 2007), which corresponds to the model output of 24.0 million with monitoring. Finally, the best estimate for the total amount stolen by thieves through new account identity theft in 2006 was around $24 billion, the model predicts $21.5 billion, which is well within the large error margins associated with estimating the profit from illicit activities.

*Scenarios*

I conduct policy experiments for three scenarios, all of which involve manipulation of the availability of freezes, the cost of freezes, the cost of thaws, and the awareness level of security freezes. These policy levers determine the adoption rate of freezes vs. monitoring, they influence the fraction of people who will obtain protection, they permit explorations of the dynamic hypotheses outlined earlier, and, most importantly, they are under the control of policymakers. First, a status quo scenario maintains the status quo as of 2007, which is to say that the availability and cost of freezes remains the same as described in the model calibration section (*q.v.*). However, in the status quo scenario, I have also assumed that an additional 1% of the population becomes aware of security freezes each year between 2008 and 2033. A second scenario explores what would happen if the credit bureaus and related firms had their way and were able to persuade the federal government to ban security freezes by the end of 2008 ("National Ban").[7] A third scenario represents the opposite possibility: that the federal government will pass a comprehensive national right to security freeze law in 2008 ("National Freezes"). Table 2 displays scenario assumptions.

---

[6] There have been a number of surveys on identity theft over the last 5 years. The FTC ran a survey in 2003 (used by Anderson 2006), and Gartner, Inc., Javelin Strategy and Research, and other firms have all conducted surveys aimed at estimating the incidence of identity theft. It is not surprising that the different survey methodologies that were employed result in variations in the estimates of identity theft. However, all surveys have found identity theft levels that are consistent with the results reported here, and the differences are not generally statistically significant.

[7] [Bureaus have] "…been scrambling for two years to get federal lawmakers to defuse the onrush of state laws empowering consumers to freeze access to their credit histories to prevent identity theft. [They] spent a record $1.4 million on federal lobbying in 2006, nearly double what [they] spent in 2004, according to the Center for Responsive Politics." Acohido, Byron and Jon Swartz (2007), "Credit bureaus fight consumer-ordered freezes," in USA Today. Online ed.

Insert Table 2 and Figures 3 and 4 About Here

---

*Results*

A comparison of the major outcome measures associated with the scenarios reveals that security freezes dominate monitoring in the prevention of identity theft. In particular, theft is greatest when freezes are banned completely, lowest when National Freezes are enacted, and intermediate in the status quo condition where some individuals obtain freezes (Figure 3). This finding supports Hypothesis 1, which predicted that proactive approaches to preventing identity theft would be better than reactive. Similarly, the results support Hypothesis 2, and reveal a nonlinear protective effect of security freezes. The dotted line in Figure 4 plots the fraction of individuals with security freezes against the incidence of theft, using (2006) as the index year = 1. The data imply that, for example, when 40% of the population is covered by freezes, we should expect a 68% drop in identity theft, and with 50% covered by freezes, we should expect a 90% decrease in theft. The solid line in Figure 4 plots the same data after breaking the Credit Industry Profit Management loop, and no qualitative differences result from eliminating this loop. There are two explanations for the nonlinearity of the response to freezes. First, freezes reduce theft by preventing an account from being opened without authorization, and they are far better prophylaxis than monitoring. Second, the fact that people with freezes will be considerably more difficult to steal from reduces the expected value of engaging in theft from the thieves' point of view. As the expected value of theft falls, the distribution of thieves' reservation wages implies that there will be a "tipping point" at which a large fraction will no longer find new account identity theft to be worthwhile (see Figure 2, Expected Value loop). Finally, the model supports Hypothesis 3, revealing that credit bureaus make the most profit if freezes are banned, next most under the status quo, and least under a national freeze plan, which is an inverse relationship to the number of people with freezes. Although credit bureaus make

some money when people freeze their accounts, they make less than they do from monitoring because the freeze fees are lower and are paid less frequently. From a marketing perspective, freezes cannibalize the monitoring business.

---

Insert Table 2 and Figure 5 About Here

---

*Robustness*

It is possible to explore each hypothesis in greater depth. For example, one could ask whether any amount of monitoring can achieve the same effect as having 40% of the population covered by a security freeze. I changed the model assumptions so that freezes were banned, 90% of the population adopted monitoring, and the time to detection with a monitored account was reduced to a mere 10 days. Although the rate of identity theft goes down relative to the Status Quo scenario, no nonlinear effect of monitoring is observed and theft levels remain greater than 1% of the population in steady state. Monitoring cannot compensate for lack of freezes.

It is also important to investigate the behavioral assumptions governing the economic actors. There is no qualitative change in any results if the credit bureaus do not, in fact, have any control over the rate of identity theft (equivalent to breaking the Credit Industry Profit Management loop in Figure 2, see Figure 4). Similarly, no qualitative change in model behavior results from changing the distribution of reservation wages demanded by thieves, either by inducing a shift in the mean or by changing the spread of the distribution. Making the distribution tighter does not affect the qualitative results, because if a reasonable fraction of the population obtains security freezes, the expected value drops below the mean in any case, so the large herd immunity-like effect becomes sharper, but does not go away. A change in the mean compensation demanded by thieves to any reasonable level also has no effect on model behavior, because with 33–50% of the population obtaining freezes, the expected value of theft drops to a

point where a substantial fraction of thieves would have to be willing to work for a pittance to justify continuing attempts to open new accounts.

To further investigate the robustness of the model dynamics, I conducted a sensitivity analysis on all critical input parameters. Specifically, I assumed that each critical variable would take on a value drawn from a random uniform distribution spanning a range of reasonable values. This procedure is quite conservative, because in reality, values are likely to be more sharply constrained. For example, I allowed the length of time that people continue to pay for monitoring once they sign up to be uniformly distributed between .75 years and 7 years, and I chose similarly broad confidence intervals for other input parameters.[8] After assigning the ranges of the random uniform distributions, I produced 5,000 runs through the model with a random draw from each variable's distribution used for each run, so that on each run, a vector of inputs was produced by taking a random draw from the uniform distribution associated with each input, this vector was used in the model run, the results were recorded. The qualitative behavior patterns among scenarios do not change based on maximally stressful variations in the most critical input parameters. Furthermore, I ran a parallel set of 5,000 draws after breaking the "credit bureau profit management loop," and similarly found no change in qualitative behavior. No qualitative behaviors are changed in the other scenarios either. In conclusion, the model results are robust to maximally stressful variations in the input parameters, and the hypotheses hold under these stressed conditions.

## General Discussion

The model predicts that society could substantially reduce, and possibly almost eliminate, new account identity theft by having only a fraction of the population freeze their credit bureau

[8] Other variables that were analyzed included: the length of time people keep security freezes once signed up, the fraction of unprotected individuals who adopt some form of protection after detection, the mean value and spread of the distribution of thieves' reservation wages, the decrease in price sensitivity associated with freezing after discovering identity theft, the rates of fraud for individuals with monitoring and freezes, the time to detection with monitoring, and the maximum number of people who would be willing to sign up for a security freeze if it were free. Details are available from the author.

accounts. The reduction occurs for two reasons. First, security freezes are substantially better than monitoring at preventing fraud. Monitoring prevents little fraud; it primarily shortens the time to detection. Reduced time to detection is of limited use, however, because thieves anticipate detection and have become resourceful enough to steal large amounts soon after obtaining the fraudulent credit line. Second, the fact that it is very difficult to obtain credit from a frozen bureau account means that the expected value of fraud drops quickly with increasing numbers of frozen bureau files. This, in turn, creates a nonlinear effect on thieves' incentives to participate in new account identity theft. In practice, it is likely that an even smaller fraction of all individuals require freezes in order to obtain reductions in identity theft that are similar to those shown in the model (i.e., 75-90% reductions in identity theft). In the model, all unprotected consumers are viewed as homogeneous and interchangeable. In reality, people have different risks of identity theft (based on their behavior patterns and to a certain extent, demographics) and markedly different values as targets of identity theft (based on their credit score and wealth level). Even though thieves do not appear to be able to target based on these characteristics (Anderson 2006), if the highest expected value targets are also more likely to obtain security freezes, which is quite likely, the effect would be to drive down the expected value of theft much faster than the model predicts, and thus to reduce identity theft faster with a smaller fraction of the population "frozen."

In spite of the attractiveness of security freezes as a preventative measure, adoption of security freezes has been extremely low (under 70,000 nationwide, Kim 2007). The model provides a possible reason, which is that there is a serious conflict of interest between credit bureaus' profit maximizing behavior and good public policy. Bureaus want to minimize freezes and maximize monitoring; the public interest is best served by having many people freeze and none monitor. The bureaus are in an analogous position to a burglar alarm company in the midst of a crime wave – no one will admit that the crime is a good thing, and yet, it is in the company's

interests for the crime to continue. This fact explains the credit bureaus' staunch opposition to freeze laws in the legislative arena at both the state and federal levels (e.g., Acohido and Swartz 2007; see footnote 7). If the model is correct and security freezes will exist (bureaus have failed to prevent freezes through lobbying), it follows that the credit bureaus have a financial incentive to make freezing and thawing one's credit report as expensive and onerous as possible, and to maintain low awareness that freezes exist. Each of these tactics has been pursued by the bureaus.

First, the bureaus have lobbied to increase the fee schedule for freezes and thaws in every state that has passed freeze-enabling laws (cf., Acohido and Swartz 2007). Second, the bureaus have engaged in a variety of techniques to make the process of freezing and thawing more onerous, for example time delays in thawing (up to three days), requirements for all requests to be made by certified or overnight mail, and overzealous identification requirements (e.g., an arbitrary PIN for each bureau, which, if lost or entered incorrectly, triggers an identification process that can take weeks). Furthermore, as predicted by this analysis, bureaus make it difficult to find information about security freezes on their websites, maintaining low awareness of freezes. I searched the websites of Experian and Equifax (TransUnion has no search feature) for the word "freeze" in June of 2007. At Equifax, zero hits were produced, at Experian, only negative information from their "ask Max" column was produced. A follow-up search for "security freeze" produced zero hits at Equifax, and a link to the correct portion of the website at Experian. Similar difficulties are encountered when navigating the sites. The bureaus make it very difficult to find information about security freezes. At TransUnion, finding security freeze information requires finding a small link that is buried four menu-levels deep in only one part of the website, and is not linked to from the section entitled "Guarding Against Identity Theft" on the top-level screen. At Equifax, I was unable to find any link to instructions on how to initiate a security freeze, and general information on freezes was placed two levels down under "Learning Center." At Experian, I was unable to find any link on the website to security freeze

information, including under "site map." Clearly, the bureaus are uninterested in making it easy to obtain information on freezes. The hidden freeze information stands in stark contrast to the bureaus' treatment of monitoring. All three bureaus feature a link comprising one third of the initial screen (at the top-level domains) advertising their monitoring service. Prominent links on all sites tout "Products," all of which involve monitoring. These observations validate the assumptions of the model and support Hypothesis 3. As of November 2007, all three bureaus have announced that they will make freezes available to people in all states. However, consistent with the model's predictions, these "for profit" freezes cost over $100/year if consumers wish to have rapid thaws, making this service as or more profitable than monitoring.

Marketers should be particularly concerned about new account identity theft. There is already substantial evidence that some consumers are not purchasing online due to fears of identity theft (IBM Corporation Survey 2005; Javelin Strategy and Research 2007b). However, there is the danger that if identity theft were to increase substantially, there could be a serious backlash against critical marketing activities, including the maintenance of CRM databases, the ability to provide instant credit, or that government may enact onerous reporting requirements regarding the disposition of consumer information. The interests of marketers are aligned with the public good – we should want to see a federal law passed that enables all consumers to cheaply and easily obtain a security freeze at all three bureaus, cheaply and rapidly thaw their file, the entire process should be streamlined and simple, and marketers, retailers, and the government should engage in a large public relations campaign to raise awareness.

In response to proposed security freeze legislation, the credit bureaus frequently cite extensive costs in implementing the systems. These costs are largely fictional. For placing a freeze, the process should require only slightly more complexity than the existing fraud and active-duty alert system, which is free to consumers (a fraud alert can be placed with a two minute phone call, and only requires a prospective lender to take "reasonable steps" to confirm

identity, it is not a freeze on the bureau file). Furthermore, for fraud and active-duty alerts, the bureaus share notice of the alert among the three companies, substantially reducing firm costs and consumer effort. For thawing the file, companies could enforce more stringent requirements that still provide an adequate balance between verification of identity and convenience, there are numerous suggestions for how this could be accomplished in a cost effective manner.[9]

*New vs. Existing Account Identity Theft*

In this paper, I have focused only on new account identity theft because this type of theft is so much more costly to the victims and to society than the most common types of existing account fraud (e.g., having a credit card stolen). Nonetheless, there are numerous types of existing account fraud that are extraordinarily intrusive for consumers. For example, if an identity thief is able to appropriate an existing bank or brokerage account, the victimization can be just as complete as if a new account had been opened. In addition, criminals sometimes engage in other types of identity theft, for example, obtaining a government ID in someone else's name. These crimes are not considered "new account" identity theft, and therefore other types of solutions are generally discussed. I have proposed that to combat new account identity theft, the credit bureaus need to develop a cheap and easy way for consumers to freeze their bureau accounts when they are not in the market for credit, and for consumers to quickly and cheaply thaw their accounts when they seek credit. The existing system is neither cheap nor easy. However, if the credit bureaus were to develop a cheap and easy system, the suggestions in this paper raise a different possibility: that the credit bureaus could become de facto guardians of identity. This would represent a whole new line of business for the bureaus. Interestingly the validating business could be used to prevent large fractions of existing account fraud as well. For example, when someone attempts to make changes to an existing account, or get new utility service, or even apply for change of address with the government, the entity that was applied to

[9] For example, companies could require callers to phone from their home phone, where caller ID is used to verify the number, and then use a choose *k* of *N* question challenge/response strategy to verify identity.

could check with a credit bureau. If the person's bureau account was frozen, no change would be permitted. After thawing their file with the credit bureau, the applicant would have essentially validated their identity. Of course, corporations and the government would still require alternate procedures for validating those people who have no credit history, or who were not in the credit-history system. But for a large fraction of the at-risk population, the same infrastructure that is required to reduce new account identity theft could be used to combat existing account identity theft, and even some types of impersonation.

*Next Steps and Future Research*

Identity theft is the quintessential crime of the information age. It is extremely expensive to corporations, which lose over $20 billion per year in write-offs, it undermines consumer confidence, and it costs consumers billions of dollars and millions of unpaid hours of time to rectify their financial reputation after victimization. In this paper, I have shown that one reason that we observe as much identity theft as we do is that there is a fundamental conflict between the interests of credit bureaus and the interests of consumers and society, and this is because credit bureaus make more money by selling their most profitable "protection services" (i.e., monitoring), than they would by selling a more efficacious service. Furthermore, the credit bureaus want enough identity theft to exist in the market that people are interested in buying their protective services, which effectively provides them a financial incentive to have more theft.

In future research, it would be interesting to attempt to devise a game theoretic model that captured the incentives of credit bureaus and consumers in greater generality. Future research should also focus on estimating many of the parameters used in this model with greater precision. The importance of this problem and the inchoate nature of the research provide myriad opportunities across a wide variety of fields. Academic researchers should play a role in figuring out how to align the interests of the credit bureaus with those of society, while preserving the marketing tools that firms need to continue conducting their businesses.

## References

Acohido, Byron and Jon Swartz (2007), "Credit bureaus fight consumer-ordered freezes," in USA Today. Online ed.

Anderson, Keith B. (2006), "Who are the victims of identity theft? The effect of demographics," Journal of Public Policy and Marketing, 25 (2), 160-71.

Armstrong, J. Scott (2001), "Combining Forecasts," in Principles of Forecasting - A Handbook for Researchers and Practitioners, J. Scott Armstrong, Ed. Norwell, MA: Kulwer Academic.

Becker, Gary S. (1968), "Crime and Punishment: An Economic Approach," The Journal of Political Economy, 76 (2), 169-217.

Bolton, Lisa E., Joel B. Cohen, and Paul N. Bloom (2006), "Does Marketing Products as Remedies Create "Get Out of Jail Free Cards"?," Journal of Consumer Research, 33 (1), 71-81.

Burdett, Kenneth, Ricardo Lagos, and Randall Wright (2003), "Crime, Inequality, and Unemployment," The American Economic Review, 93 (5), 1764-77.

Cheney, Julia S. (2003), "Identity Theft: A pernicious and costly fraud," in Payment Cards Center Workshop. Federal Reserve Bank of Philadelphia

Consumers Reports WebWatch (2005), "Leap of faith: Using the internet despite the dangers," Consumer Reports WebWatch (Ed.). Yonkers, NY: Princeton Survey Associates.

Consumers Union (2007), "Consumers Union list of state security freeze laws, at http://www.consumersunion.org/campaigns//learn_more/003484indiv.html," Online edition, accessed June 15, 2007.

CyberSource Corporation (2007), "Online Fraud Report – Credit Card Fraud Trends and Merchants' Response"."

Federal Trade Commission (2007), "FTC Issues annual list of top consumer complaints, accessed at http://www.ftc.gov/opa/2007/02/topcomplaints.shtm on 6/10/2007," FTC (Ed.) Vol. February 7.

Foley, Linda and Jay Foley (2004), "Identity theft: The Aftermath 2004," Identity Theft Resource Center.

Freeman, Richard B. (1996), "Why Do So Many Young American Men Commit Crimes and What Might We Do About It?," The Journal of Economic Perspectives, 10 (1), 25-42.

Gartner Inc. (2007), "Gartner says number of identity theft victims has increased more than 50 percent since 2003," in http://www.gartner.com/it/page.jsp?id=501912, accessed on 6/10/2007.

Gonzales, Alberto R. and Deborah Platt Majoras (2007), "Combating Identity Theft: A Strategic Plan," Office of the President (Ed.): U.S. Department of Justice.

Green, Paul (2002), "Using the "top box" to predict adoption," Eric M. Eisenstein (Ed.). Philadelphia.

Hoofnagle, Chris J. (2005), "Putting Identity Theft on Ice: Freezing Credit Reports to Prevent Lending to Impostors," in Security Privacy in the Internet Age, Radin Chander, Gelman, Ed. Palo Alto: Stanford University Press.

IBM Corporation Survey (2005), "Fear of Identity Theft and Credit Card Fraud Worry Consumers During the 2005 Holiday Season, According to IBM Survey, accessed at http://www-03.ibm.com/press/us/en/pressrelease/7973.wss on 6/14/2007," IBM.

Javelin Strategy and Research (2004), "Credit Monitoring and Identity Fraud Insurance: What do consumers need, and how should it be offered?," in, Javelin Strategy and Research, Ed. Hacienda, CA: Javelin Strategy and Research.

---- (2005), "Credit Monitoring and Identity Fraud Insurance: What do consumers need, and how should it be offered?," in, Javelin Strategy and Research, Ed. Hacienda, CA: Javelin Strategy and Research.

---- (2007a), "Credit Monitoring services: Generating revenue, mitigating losses, and inspiring customer loyalty," in, Javelin Strategy and Research, Ed. Hacienda, CA: Javelin Strategy and Research.

---- (2007b), "Identity Fraud Survey Report," in, Javelin Strategy and Research, Ed. Hacienda, CA: Javelin Strategy and Research.

Kahn, Charles M. and William Roberds (2005), "Credit and identity theft," in Working paper: Atlanta Federal Reserve Bank.

Kim, Jane J. (2007), "More People are Freezing Credit Reports," in the Wall Street Journal. October 24th, 2007 ed. New York.

LoPucki, Lynn M. (2001), "Human identificaiton theory and the identity theft problem," Texas Law Review, 80 (November), 89-134.

Mayer, Robert N. (2006), "Defending Your Financial Privacy: The Benefits and Limits of Self-Help," American Association for the Advancement of Retirees (Ed.).

Menton Jr., Francis J. (2002), "Can you protect yourself from identity theft?," New York Law Journal, 227 (April 29).

Milne, George R. (2003), "How Well Do Consumers Protect Themselves from Identity Theft?," The Journal of Consumer Affairs, 37 (2), 388.

Milne, George R., Andrew J. Rohm, and Shalini Bahl (2004), "Consumers' Protection of Online Privacy and Identity," The Journal of Consumer Affairs, 38 (2), 217.

Nakashima, Ellen and Ylan Q. Mui (2007), "Data theft grows to biggest ever," in Washington Post. Online ed. Vol. Friday, March 30, 2007. Washington, DC.

Newman, Graeme R. and Megan M. McNally (2005), "Identity Theft Literature Review," Department of Justice (Ed.).

Privacy Rights Clearinghouse (2007), "Chronology of Data Breaches," Privacy Rights Clearinghouse.

Richardson, George P. (1996), Modelling for Management: Simulation in Support of Systems Thinking. Aldershot, U.K.: Dartmouth Publishing Company.

Sauer, Jennifer H. (2006), "Security Freeze Legislation: Consumer Attitudes On Paying Activation And Lifting Fees," Vol. 2007. Washington, DC: AARP.

Sharp, Tracey, Andrea Shreve-Neiger, William Fremouw, John Kane, and Shawn Hutton (2004), "Exploring the psychological and somatic impact of identity theft," Journal of Forensic Science, 49 (January), 1-6.

Snow, John (2003), "United States Treasury Secretary John W. Snow: Remarks Advocating the Renewal of the Fair Credit Reporting Act," The Treasury Department, Washington, DC, June 30.

Solove, Daniel J. (2003), "Identity theft, privacy, and the architecture of vulnerability," Hastings Law Journal, 54 (April), 1227-76.

Sovern, Jeff (2003), "The jewel of their souls: Preventing identity theft through loss allocation rules," University of Pittsburgh Law Review, 64 (Winter), 343-406.

---- (2004), "Stopping Identity Theft," The Journal of Consumer Affairs, 38 (2), 233.

Swets, John A.; Dawes, Robyn M,; Monahan, John (2000), "Psychological Science Can Improve Diagnostic Decisions," Psychological Science in the Public Interest, 1 (1), 1-26.

Symantic Corporation (2007), "Internet Threat Report," Vol. XI.

Viscusi, W. Kip (1986), "The Risks and Rewards of Criminal Activity: A Comprehensive Test of Criminal Deterrence," Journal of Labor Economics, 4 (3), 317-40.

Weston, Liz Pulliam (2005), "What Europe can teach us about identity theft."

Zeller, Tom Jr. (2005), "Black Market in Stolen Credit Card Data Thrives on Internet," New York Times. New York.

Table 1. Comparison of states of protection.

| Value | State of Protection Monitored | Frozen | Unprotected |
|---|---|---|---|
| p(fraud) | 0.0117 | 0.0001 | 0.0132 |
| Time to Detection | 0.25 years | 0.6 years | 0.53 years |

Table 2. Summary of scenarios

| Parameter | Status Quo | Scenario<br>National Freezes | National Ban |
|---|---|---|---|
| Availability of freezes | 75% of population covered by end of 2008 no increases in coverage | 100% of population covered by end of 2008 | 0% of population covered by end of 2008 |
| Awareness of freezes | 1% of population becomes aware from 2008 to 2033; 25% total awareness in 2033 | 8% of the population becomes aware from 2008 to 2018; 80% total awareness in 2018 | N/A |
| Population-Weighted Cost of Freezes: change from 2003 – 2018 | Declines from $9.40 to $8.10 / bureau | Declines from $9.40 to $3.33/bureau | N/A |
| Population-Weighted Cost of Thaws: change from 2003 – 2018 | Declines from $12 to $4.85/thaw | Declines from $12 to $1.85/thaw | N/A |

Figure 1. Major Stocks and Flows of the System Dynamics Model of Identity Theft

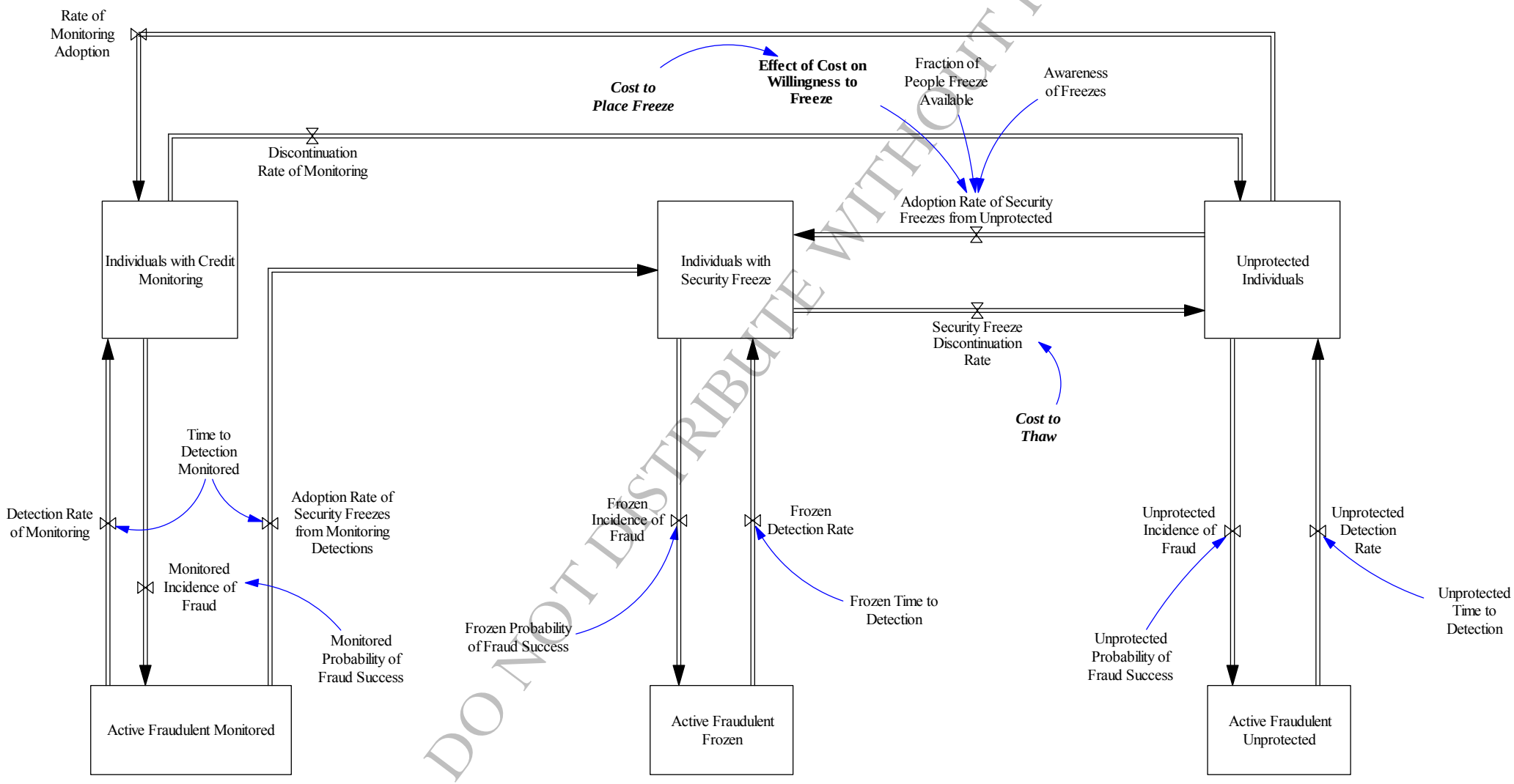

Figure 2. Major feedback loops in the system

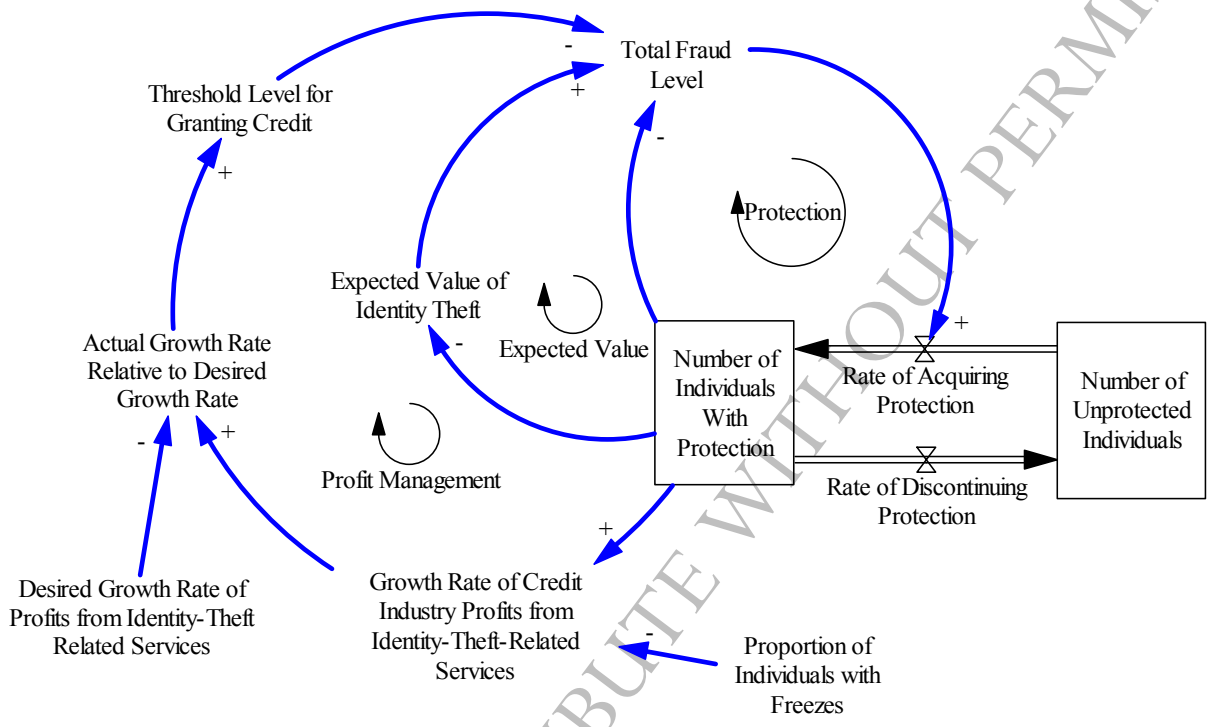

Figure 3. Number of new account identity theft victims.

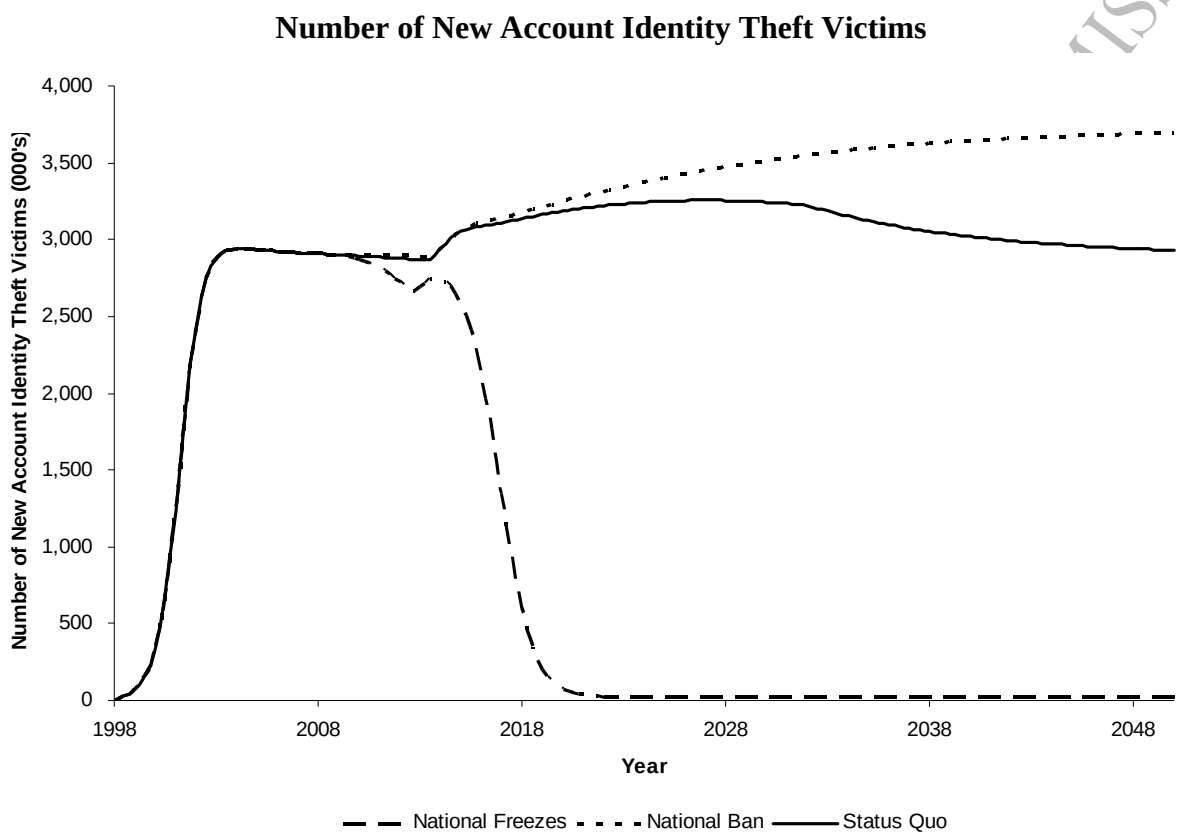

Figure 4. Fraction of individuals covered by a security freeze vs. reduction in theft conditional on credit bureaus being able and unable to influence the rate of theft, with and without the credit industry profit management loop.

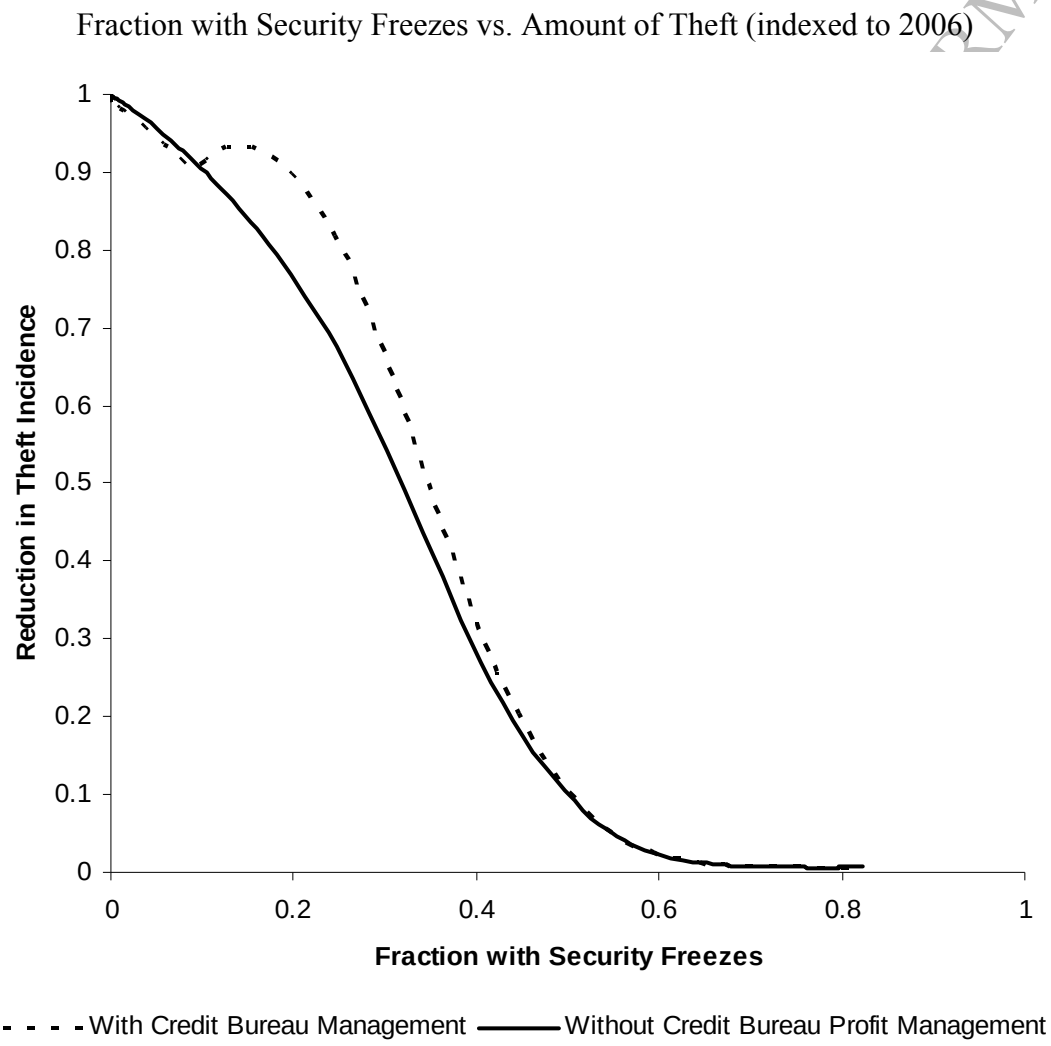

Figure 5. Monte carlo-based robustness check of the National Freeze scenario (5,000 runs).