CHRIS JAY HOOFNAGLE, IDENTITY THEFT: MAKING THE KNOWN UNKNOWNS KNOWN, 21 HARV. J.L. TECH. ___ (FORTHCOMING FALL 2007).

Identity Theft: Making the Known Unknowns Known

Chris Jay Hoofnagle[FNA1]
Senior Staff Attorney, Samuelson Law, Technology & Public Policy Clinic
Senior Fellow, Berkeley Center for Law and Technology

Center for Clinical Education
University of California, Berkeley
Boalt Hall School of Law, 396 Simon Hall
Berkeley, CA 94720-7200
choofnagle@law.berkeley.edu
510.643.0213 (voice) 510.643.4625 (fax)

Abstract

There is widespread agreement that identity theft causes financial damage to consumers, lending institutions, retail establishments, and the economy as a whole. Surprisingly, there is little good public information available about the scope of the crime and the actual damages it inflicts. The publicly available data on identity theft come mainly from survey research. Methodologically, these survey polls of the public suffer from being both under and overinclusive in measuring the problem. As a result, low estimates attribute tens of billions of dollars in costs to the economy and consumers, the highest estimates place losses in the hundreds of billions.

To identify proper interventions and appropriately allocate resources we need comprehensive, hard data on the scope and effect of identity theft. One way to provide concrete data is to require lending institutions to publicly report figures on identity theft. Such public reporting will help identify the relative need for intervention and the likely efficacy of interventions. These disclosures are necessary to provide a sound baseline for investment by businesses and action by regulators. They are also warranted because the public pays the price of identity theft directly when they are the victim, and indirectly through higher fees, interest rates, and because the losses are tax subsidized.

The author hypothesizes that if lending institutions reported limited information about identity theft, it would reveal that identity theft is both more prevalent and economically damaging than currently acknowledged, in part because of the rise of "synthetic identity theft," a form that cannot be measured by victim surveys because they are unaware of the crime. Furthermore, the disclosure requirement would birth an anti-identity theft market, and the prevalence and severity of the crime would decrease dramatically as institutions compete to offer the safest financial products to consumers.

[FNA1] This manuscript has benefited greatly from feedback by Professor Daniel J. Solove, Mark Hoofnagle, Susan Hutfless, Chris Walsh, Avivah Litan, and my colleagues at Boalt Hall, Professor Deirdre K. Mulligan, Maryanne McCormick and Jack Lerner.

Identity Theft: Making the Known Unknowns Known

1. Introduction

> *Reports that say that something hasn't happened are always interesting to me, because as we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns -- the ones we don't know we don't know*
>
> *--Donald Rumsfeld*[1]

There is widespread agreement that identity theft causes financial damage to consumers, creditors, retail establishments, and the economy as a whole.[2] It has been identified by the Federal Trade Commission as the fastest growing white collar crime, and numerous federal and state laws have been enacted to curb its incidence and severity.[3]

But, the contours of identity theft problem are known unknowns. We know that no one knows how much of it there is, the relative rates of credit card fraud or "new account" thefts, or how much the crime impacts the economy.

These known unknowns present serious problems. As a result, we cannot determine the scope of the crime and the resources that should be allocated to it. We cannot determine whether various consumer protection interventions have been effective.

---

[1] Secretary of Defense Donald Rumsfeld, Department of Defense News Briefing (Feb. 12, 2002), available at http://www.defenselink.mil/Transcripts/Transcript.aspx?TranscriptID=2636.

[2] GOVERNMENT ACCOUNTABILITY OFFICE, IDENTITY THEFT, AVAILABLE DATA INDICATE GROWTH IN PREVALENCE AND COST GAO-02-424T (Feb. 14, 2002), available at http://www.gao.gov/new.items/d02424t.pdf.

[3] FEDERAL TRADE COMMISSION, PRIVACY: TIPS FOR PROTECTING YOUR PERSONAL INFORMATION (Jan. 2002), available at http://www.ftc.gov/bcp/conline/pubs/alerts/privtipsalrt.htm; Graeme R. Newman & Megan M. McNally, *Identity Theft Literature Review*, January 2005, available at http://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf

We cannot tell whether consumers, regulators, and businesses are over or under reacting to the crime. We cannot determine whether identity theft is more or less prevalent, or more or less severe than a year ago. We cannot determine how the costs of the crime are being distributed back upon society.

These may seem like provocative and confusing statements. How could a crime that did not have a name just a decade ago now plague commerce, online and off? How can we know so little about it? How, despite its apparent prevalence and severity, can it not be measured properly by law enforcement, the public, industry, or policymakers?

The answer lies in the methods used to measure the problem. What we do know has been learned through telephone and internet surveys. While well-intentioned, and valuable for some purposes in the identity theft policy debate, these surveys cannot completely document the contours of the crime.

But more fundamentally, we are asking the wrong people about the crime. The surveys performed seek to obtain information about the crime from victims, individuals who have the most limited view of the problem. Victims often cannot tell how the crime occurred, how their information was stolen, or who stole it.

A solution can be found in gathering information from the entity that knows the most about the crime—the lending institution. If "lending institutions," used here to describe the entities that actually extend credit (such as banks and credit card companies) and control access to accounts (including payment companies such as Paypal and Western Union), were required to provide statistical data about the crime, a more complete and focused picture would emerge. Lending institutions have not provided this information because it could cause embarrassment and because it could attract unwanted

regulatory attention. Another important reason is the advent of "synthetic" identity theft. This new form of the crime, I argue below, has caused us to underestimate the prevalence and severity of identity theft greatly.

My proposal is to require lending institutions to disclose 1) how many identity theft incidences they suffered or avoided, 2) the form of identity theft attempted (i.e. new account fraud, credit card fraud, etc.) and the product targeted (mortgage loan, credit card, etc), and 3) the amount of loss suffered or avoided. As I will explain, these three categories of statistics can be elusive to lending institutions themselves, but even imperfect reporting of them by institutions will benefit public understanding of the crime.

My proposed intervention is relatively simple and does not require extensive regulatory mandates. While there are many challenges, practically and politically, to implementing it, it would result in great benefit to the public. It will enable benchmarking and the identification of additional consumer protections that work and those that do not. It will help regulators and law enforcement allocate the proper resources to fight the crime. It will help clear the air of suspicious polling mischief, the release of surveys that have used questionable assumptions to pin the blame of identity theft to the victims of the crime.

Finally, I believe that this approach will dramatically reduce identity theft. In providing more accurate identity theft numbers, identified by institution, a market will be born. Security will become a market differentiator, much like low interest rates and fee-free accounts. In this market, the carrots of consumer loyalty will be provided to institutions that provide the safest financial products.

And an enormous stick will be held over the institutions with the worse rates of identity theft. Just imagine the innovative approaches and dedication that will be paid to this problem by the institution that bears the ignominious mark of having the most identity theft.

2. The Known Knowns: Identity Theft

Formally defined at 18 USC §1028, identity theft is the knowing use of identification information of another to commit any unlawful activity. The Federal Trade Commission defines it more broadly as "A fraud committed or attempted using the identifying information of another person without authority."[4] For purposes of this paper,[5] it is more useful to think of identity theft as frauds that fall into two categories: new account fraud and account takeover. The two types have many variations, and different severities, depending on each situation.

New Account Fraud

First, in "new account fraud," an impostor opens lines of credit using personal information of another. This may include new credit card accounts, mortgages, or utilities, such as wireless phone accounts. New account fraud requires that the impostor have the victim's Social Security number, along with other identifying information, such as date of birth, address, and mother's maiden name. New account fraud, generally, is a serious problem for consumers. Because the new accounts appear on the victim's credit history, making it more difficult to obtain new credit such as mortgages, and sometimes

[4] 16 CFR § 603.2 (2006).

[5] Several commentators have defined many other variations of identity theft crimes, including "identity cloning" and "criminal identity theft" that are not relevant to this discussion. IDENTITY THEFT RESOURCE CENTER, IDENTITY THEFT: THE AFTERMATH 2003 (Sept. 23, 2003), available at http://www.idtheftcenter.org/idaftermath.pdf.

acting as a barrier to employment, it can have greater negative effects on consumers than account takeovers.

Synthetic identity theft is an important variation of new account fraud. Not enough is known about this form of new account fraud, but initial indications suggest that it is a growing problem. According to Mike Cook of ID Analytics, a company that specializes in reduction of fraud risk, synthetic fraud "is a larger problem than [standard new account] identity theft and is growing at a faster rate."[6]

In synthetic cases, the impostor creates a new identity using some information from a victim that is enhanced with fabricated personal information.[7] For instance, the impostor may use a real Social Security number, but a falsified name and address. Since this synthetic identity is based on some real information, and sometimes supplemented with artfully created credit histories, it can be used to apply for new credit accounts.

A sophisticated example of the crime is well illustrated by a case brought by the U.S. Attorney for the District of Arizona in August 2006:[8] In the still-ongoing case, two

[6] Mike Cook, *The Lowdown on Fraud Rings*, 10 Collections & Credit Risk 6 (Aug. 2005), available at http://www.idanalytics.com/pdf/CCRAugust05MikeCook.pdf.
[7] FDIC, PUTTING AN END TO ACCOUNT-HIJACKING IDENTITY THEFT (Dec. 14, 2004), available at http://www.fdic.gov/consumers/consumer/idtheftstudy/index.html; Fred H. Cate, *Information Security Breaches and the Threat to Consumers* (Sept. 2005), available at http://www.hunton.com/files/tbl_s47Details/FileUpload265/1280/Information_Security_Breaches.pdf.
[8] William Carlile, *Two Indicted in Credit-Card Scheme That Used SSNs From Credit Reports*, 5 Privacy & Security Law Report 1257, Sept. 11, 2006; Donald G. Aplin, Privacy, *Security Protection Will Remain Key Part of FTC's Agenda, Majoras Says*, 5 Privacy & Security Law Report 1552, Nov. 13, 2006.

men are charged with a variety of federal crimes for allegedly using real Social Security Numbers from credit reports combined with fabricated names to apply for credit cards.[9]

One of the men owned a small consumer reporting agency, and apparently has a high level of sophistication in credit practices.[10] The pair established credit histories for synthetic identities by reporting favorable payment information to consumer reporting agencies. In doing so, the synthetic identities appeared to be real people with a track record of paying bills. They then, it is alleged, obtained 250 credit cards from 15 banks, and charged $760,000 to these synthetic identities.[11]

As will be explained more fully below, synthetic identity fraud cannot always be detected by the individual whose Social Security number was used. This is because the synthetic identity is an amalgam of false and real information, which is sufficient to obtain credit, but may never be attributed to a specific victim's credit record. For instance, in this case, the defendants used real Social Security numbers but wholly fabricated names.[12] Below, from the indictment, it can be seen that a Social Security number assigned to a real person ("Haqqani Saifullah") was used to apply for a credit card for a synthetic identity ("Hanna Curin").[13]

Count	Date (on or about)	False Name	Amount of money obtained from use	Credit card #
1	05/02/2002	Hanna Curin (SSN 7483 assigned to Haqqani Saifullah)	$3,481.00	Fleet #0519

[9] *US v. Rose et al*, CR06-0787PHK-JAT (VAM) (D. Az. 2006), *indictment filed* Aug. 22, 2006.
[10] *Rose*, Indictment at 2.
[11] *Rose*, Indictment at 3-4.
[12] *Rose*, indictment at 5, 7-8.
[13] *Rose*, indictment at 5.

According to the U.S. Attorney's Office, "None of the individuals whose Social Security numbers were used suffered financial losses as a result of the scheme."[14]

Account Takeovers and Credit Card Fraud

Second, in "account takeovers," which we think most commonly occurs as credit card fraud, an impostor uses one of the victim's existing accounts. For instance, the impostor may steal a credit card number from the victim and use it without authorization. A variety of consumer protection laws and self-regulatory practices limit liability for financial account takeovers.[15] For example, consumers can dispute fraudulent charges and have them removed from a bill.

But account takeover is much broader than mere credit card fraud. For instance, "phishing" is the practice of tricking the victim into revealing passwords or other information so the thief can access or alter existing accounts.[16] In addition to credit cards, traditional checking and savings accounts are targeted by phishers, as are new payment systems and auction services, such as Paypal and eBay. Once the accountholder is tracked into revealing the password, the account can then be taken over by the thief, and emptied. In the case of credit accounts, consumers can dispute charges when they receive their bill. But when a non-credit account, such as a checking or savings account, is phished, the victim is left with no money and no ability to pay bills.

---

[14] William Carlile, *Two Indicted in Credit-Card Scheme That Used SSNs From Credit Reports*, 5 Privacy & Security Law Report 1257, Sept. 11, 2006

[15] See e.g. Regulation Z, 12 C.F.R. § 226; Regulation E, 12 C.F.R. § 205.

[16] FEDERAL TRADE COMMISSION, HOW NOT TO GET HOOKED BY A 'PHISHING' SCAM (Oct. 2006), available at http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.htm.

Despite regulatory protections for consumers' accounts, in many cases, consumers do not recover the full amount of the fraudulent charges. In 2004, according to Gartner, consumers recovered 80% of losses from Phishing attacks. In 2005, only 54% recovered the full amount of fraud.[17]

3. The Known Unknowns

Many attempts have been made to count the victims of identity theft, and the cost to the economy of the crime. Each attempt faced serious methodological challenges, leaving the public with only a hazy view of the crime. One of the most ambitious attempts was led by the Government Accountability Office in 2002. Investigators there interviewed employees of consumer reporting agencies, the Federal Trade Commission, the Social Security Administration, victims of the crime, and federal law enforcement to see whether reports of the crime had increased. They tried several innovative approaches, including determining the staffing levels of fraud departments. Data were sometimes contradictory; for instance, some consumer reporting agencies reported an increase in fraud department staffing, while others did not. Ultimately, the investigators concluded that both prevalence and cost of identity theft was on the rise.[18]

But despite these efforts, the GAO only observed the shadows of the crime. The core measurement problem with the GAO effort, and with other methods explained below, is one of data access. That is, the entities with the most information about the

---

[17] Robert McMillan, *Consumers to Lose $2.8 Billion to Phishers in 2006, Experts say phishing attacks continue to rise, getting more costly*, PC World, Nov. 9, 2006, available at http://www.pcworld.com/article/id,127799/article.html.

[18] GOVERNMENT ACCOUNTABILITY OFFICE, IDENTITY THEFT, AVAILABLE DATA INDICATE GROWTH IN PREVALENCE AND COST GAO-02-424T (Feb. 14, 2002), available at http://www.gao.gov/new.items/d02424t.pdf.

crime—lending institutions—don't release data on identity theft. This section explains why prevalence and severity of identity theft remains a known unknown.

Missing Data and Other Limits on Identity Theft Surveys

Surveys of victims are valuable for many reasons, including to determine what challenges victims face when recovering from the crime. However, such surveys are not optimal for measuring rates of identity theft. In fact, most identity theft probably escapes public polls, because of the rise of synthetic identity theft.[19]

Synthetic identity theft is elusive because individuals whose information was used never become aware of the crime. As explained above, synthetic identity theft involves fabricating identities. These identities typically are based on a real Social Security number, but a fake name and address. As a result, because "the combination of the name, address and Social Security number do not correspond to one particular consumer, the fraud is unreported [by a victim to a bank] and often goes undetected…financial losses stemming from synthetic identity fraud are difficult for organizations to label as fraud when the approved account becomes delinquent and eventually charges-off as a loss."[20] Consumer reporting agency Experian explains in a white paper: "…in a case of synthetic identity fraud in which identifies are fabricated and no victim steps forward to claim

---

[19] Javelin Research, the leading firm performing polling on identity theft, warns that its studies do not cover synthetic identity theft: "Javelin uses identity fraud as the term to describe the crime discussed in this report. Because this report's underlying survey was based on interviews with individuals who were the victims of fraud committed in their names; it will not include other categories of crime such as synthetic identity fraud." JAVELIN RESEARCH, 2006 IDENTITY FRAUD SURVEY REPORT, Jan. 2006. Since publishing the 2005 and 2006 survey reports, Javelin now claims that it does measure synthetic identity theft, but only when the fraudster uses the victim's true name. Chris Jay Hoofnagle, *Javelin's Bogus Analysis of Identity Theft*, A BROWN STUDY BLOG, Feb. 1, 2007, available at http://chrishoofnagle.com/blog/?p=680.

[20] Mike Cook, *The Lowdown on Fraud Rings*, 10 Collections & Credit Risk 6 (Aug. 2005), available at http://www.idanalytics.com/pdf/CCRAugust05MikeCook.pdf.

fraud, accounts are charged-off as a credit loss before the institution is aware of the problem."[21]

ID Analytics, a company that focuses on identity crimes, has made the most ambitious study of synthetic identity theft. ID Analytics examined 300 million credit applications submitted by individuals to lending institutions over two years. They found:

> *"...that 11.7% of successfully opened fraudulent account applications were opened using a real person's identity. The remaining 88.3% of the successfully opened fraudulent account applications appeared to be opened using a synthetic identity. Synthetic identity fraud also represented the majority of dollar losses: 73.8% of dollar losses were due to synthetic identity fraud, compared to 26.2% for true-name identity theft."*[22]

If ID Analytics is correct, most new account identity theft incidences and losses will never be detected by polls.

There are other limits to survey research on identity theft. For instance, it is not clear that the survey firms confirm that members of the sample were actually victims. This could be done by analyzing a subset of the population identified as victims, and inspecting police reports or other evidence of the crime.

Without confirmation of victim status, such studies may be overinclusive, and label a subject as a victim incorrectly. Survey subjects may say that they are a victim when they are really not, because they may be confused about suspicious events, or because they may have been a victim of a security breach and concluded that identity theft occurred.

---

[21] *See also,* EXPERIAN, PRECISE ID, AN INTEGRATED APPROACH TO THE WORLD OF IDENTITY RISK MANAGEMENT (undated), available at http://www.ftc.gov/bcp/workshops/techade/pdfs/Kirshbaum1.pdf.

[22] Mike Cook, *The Lowdown on Fraud Rings*, 10 Collections & Credit Risk 6 (Aug. 2005), available at http://www.idanalytics.com/pdf/CCRAugust05MikeCook.pdf.

Some other forms of identity theft are unlikely to be detected by the victim, and thus are underrepresented in polling. These include identity theft committed by immigrants in order to gain employment status, medical care, or the ability to rent an apartment.

All of these factors contribute to wildly disparate figures on the identity theft problem, making the scope and severity of the crime a known unknown. Estimates of loss from identity theft vary widely. In 2002, the FTC estimated based on a poll that the crime cost victims and businesses $52 billion. A 2003 study of actual victims counseled by the ITRC estimated the cost to be $279 billion.[23]

Law Enforcement Statistics Do Not Capture the Problem Either

For a variety of reasons, law enforcement statistics do not capture the contours of identity theft. First, the FTC has found that "Most victims of ID Theft do not report the crime to criminal authorities."[24] This may especially be the case with account takeovers, because the victim usually resolves the issue with a call to the institution without further incident.

---

[23] One of ITRC's clients had over $7,000,000 in fraud using his identity. IDENTITY THEFT RESOURCE CENTER, IDENTITY THEFT: THE AFTERMATH 2003 27-28 (Sept. 23, 2003), available at http://www.idtheftcenter.org/idaftermath.pdf. The differences between the FTC and ITRC studies may be attributable to differences in samples. FTC's study involves calling thousands of households in order to locate several hundred victims of identity crimes. In doing so, FTC locates many victims of account takeovers, crimes that are possibly less serious and easier to resolve than ITRC's sample. ITRC's sample was comprised of confirmed victims of identity theft who are self-selected, in that they contacted ITRC. It can be assumed that ITRC's sample suffered more serious forms of identity theft, because the victims took the time to seek out ITRC's assistance.

[24] FEDERAL TRADE COMMISSION, IDENTITY THEFT SURVEY REPORT 9 (Sept. 2003), available at http://www.ftc.gov/os/2003/09/synovatereport.pdf.

Second, when a victim does try to contact police, some law enforcement agencies are reluctant to take reports. They may view the lending institution as the victim.[25] Or, in cases where the theft took place in another jurisdiction, they may tell the victim to file the report elsewhere. In turn, police in the other jurisdiction then tell the victim to file where she lives. This runaround has caused California to require law enforcement by statute to take reports from victims.[26]

Third, the crime may be misclassified by businesses as a different type of loss to avoid embarrassment. The ITRC has observed: "Unfortunately, many commercial victims do not report the crime to law enforcement, considering it more fiscally advantageous to 'write off the loss.'"[27] Collins and Hoffman note that, "…even though this crime became epidemic on the last decade, many companies remain reluctant to report the thefts of their employees' or customers' identities for fear of losing business."[28] In addition to tarnishing a company's brand, severe identity theft losses are likely to attract unwanted regulatory attention. High levels of fraud may bring lending institutions' security and soundness into question, triggering examinations and costly compliance duties.

Fourth, even when fraud is detected, unless it reaches a certain severity, law enforcement will not begin an investigation. For instance, even a fraud event resulting in

---

[25] Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, Hearing Before the U.S. Senate Judiciary Subcommittee on Technology, Terrorism, and Government Information, Jul. 12, 2000 (testimony of Beth Givens, Director, Privacy Rights Clearinghouse), available at http://www.privacyrights.org/ar/id_theft.htm.
[26] See e.g. Cal. Penal Code 530.6(a)(2007).
[27] IDENTITY THEFT RESOURCE CENTER, IDENTITY THEFT: THE AFTERMATH 2003 5 (Sept. 23, 2003), available at http://www.idtheftcenter.org/idaftermath.pdf.
[28] Collins, J.M. and Hoffman, S.K. (2004) *Identity Theft: Predator Profiles*, Submitted to Security Journal. Manuscript available from Judith Collins, - judithc@msu.edu.

$50,000 in loss will not necessarily trigger an investigation in Southern California.[29] In limited cases, identity thieves are pursued and restitution may be collected for the costs, but these situations are rare. The Gartner Group estimated in 2003 that "criminals still have a one out of 700 chance of getting caught by federal authorities."[30] This lack of response from law enforcement causes some commercial victims to not report the crime.

Fifth, for various data collection and management issues, law enforcement often does not have an accurate picture of the identity theft problem. In a 2002 GAO report, investigators concluded that "[g]enerally, federal law enforcement agencies do not have information systems that specifically track identity theft cases."[31] One reason is that identity theft may not be a "stand-alone crime;" it may be committed as part of a larger criminal enterprise. Thus, the crime may be included in reporting of other types of financial fraud.[32]

For all the above reasons, law enforcement cannot completely map the known unknowns of identity theft.

4. Making the Unknown Knowns Known

Mandated Reporting of Identity Theft Incidences and Severity

[29] Remarks of Joe Majka, Vice President, Risk Management and Fraud Control Department, Visa, Teaming Up Against Identity Theft, A Summit on Solutions (Feb. 23, 2006).
[30] Avivah Litan, *Underreporting of Identity Theft Rewards the Thieves*, Gartner Group Research ID: M-20-3244, Jul. 7, 2003.
[31] GOVERNMENT ACCOUNTABILITY OFFICE, IDENTITY THEFT, AVAILABLE DATA INDICATE GROWTH IN PREVALENCE AND COST GAO-02-424T 2 (Feb. 14, 2002), available at http://www.gao.gov/new.items/d02424t.pdf.
[32] GOVERNMENT ACCOUNTABILITY OFFICE, IDENTITY THEFT, AVAILABLE DATA INDICATE GROWTH IN PREVALENCE AND COST GAO-02-424T 2 (Feb. 14, 2002), available at http://www.gao.gov/new.items/d02424t.pdf.

In section three, I explained why public polling and law enforcement statistics only offer a limited view of the identity theft problem. This limited view would be broadened if lending institutions themselves reported on identity theft. Lending institutions, after all, are victims of identity theft. They are the hub for information about the crime, because they actually lend the money to the thief and experience nonpayment. They account for this nonpayment by either absorbing the loss, or by charging it back to a merchant where the thief purchased goods.

Expanding on this basic accounting, and making it publicly available, will unmask the known unknowns of identity theft.

a. Incidences Suffered or Avoided

I propose three types of reporting: first, lending institutions should disclose how many identity theft incidences they suffered or avoided. By this, I mean that each time the institution identifies an incidence of account takeover or new account fraud, it should be recorded and reported. For instance, when a consumer calls to report fraudulent charges on a credit card, on an account hijacked by a fraudster, or an account opened in their name, this fact should be reported.

Synthetic identity fraud should be tracked as well, but in such cases, a consumer does not always call to complain of fraudulent charges or accounts. Therefore, the institution itself must identify these cases. Avivah Litan has proposed a solution to identifying synthetic cases. In 2003, she wrote that institutions should reclassify all loans that are late by 180 days from bad credit losses to identity theft fraud by default. That is, unless there is evidence otherwise, institutions should treat late accounts as identity theft incidents: "Such an action will likely raise creditors' appreciation of identity theft fraud,

while reducing their loan and credit losses. It will also likely motivate creditors to attack identity theft fraud with effective solutions."[33]

Litan's solution may appear to be overbroad. It would appear to classify some bad credit losses—accounts opened by ordinary deadbeats—as synthetic identity theft. But in at least one synthetic identity theft situation, criminals made minimum payments on the accounts so that the credit cards acquired would continue to be active.[34] This tactic means that even accounts that appear to be held by legitimate customers who get by through paying the minimum payment may be synthetic identity thieves. Reporting will require lending institutions to perform more investigation to distinguish between ordinary deadbeats and those who never intend to pay the full bill.

This first type of reporting also seeks to document "avoided" incidences. These are situations where automated systems block charges that are recognized as fraud, known failed attempts to hijack accounts, and where systems reject a credit application as fraudulent. Below, in section six, I will argue why this tracking will benefit institutions by allowing them to document their effectiveness in fighting identity theft.

b. The Form of Identity Theft Attempted and the Product Targeted

Second, institutions should report upon the form of identity theft that was attempted and the product targeted by the fraudster. At the most general level, institutions could identify two types of fraud—new account fraud and account takeover. In some cases, both types may be present, and that fact could be reported.

---

[33] Avivah Litan, *Reduce Identity Theft by Rectifying Too-Easy Credit Issuance*, Gartner, Inc., Sept. 4, 2003, available at http://www.gartner.com/resources/117100/117132/117132.pdf.

[34] *DOJ Charges Three California Men In $1.4 Million Credit Card Fraud*, 2 Privacy & Security Law Report 357, Apr. 7, 2003.

As we understand more about identity theft, and as the crime evolves, this reporting could expand to categorize more types. For instance, institutions could include information on reporting forms where they suspect "friendly" or "familiar" fraud, a situation where the accountholder has allowed another to make a charge, but still reports it as fraudulent. Institutions would be free to recognize these variations on the two dominant categories and report them voluntarily.

This second form of reporting seeks data on the "product targeted." By this, I mean the type of financial service that the thief sought to obtain. This may be a new or existing credit card, an in-store offer of credit, a mortgage loan, the use of "convenience checks," and so on. I will explain in section six why identifying the product targeted will help tailor interventions to the types of financial fraud that present the most risk.

c. The Amount of Loss Suffered or Avoided

This third form of reporting is largely self-explanatory: if a consumer identifies $100 in fraudulent charges, the institution should report that amount. In synthetic situations, the institution should report the actual losses from the theft. Avoided losses could be calculated based on the amount of an attempted charge, or in the case of new accounts, the maximum credit line considered for the applicant.

Who Reports and To Whom?

Lending institutions are the appropriate entity to report, because they are victims of identity theft too, and because they have the most information about the crime. A possible alternative would be to have consumer reporting agencies disclose the figures. However, this is a suboptimal solution, because consumer reporting agencies do not always learn of identity theft, especially in account takeover situations. Even in new

account fraud identity theft, significant numbers of victims never file fraud alerts or inform the consumer reporting agency of the crime.

Reporting duties are further complicated because modern financial services companies engage in sophisticated marketing relationships through affinity cards, joint marketing agreements with other companies, and the like. For instance, a college may offer alumni an affinity credit card issued by a partner bank. Or, a department store may offer a discount on purchases in exchange for a customer's enrollment in a store credit card. Still, the reporting entity should be the lending institution, not the affinity entity or the department store, because it is the company that is actually extending the financial product.

The data should be reported to a financial regulator, such as the Federal Financial Institutions Examination Council ("FFIEC"). Lending institutions regularly report other data on financial stability to the FFIEC. The data could be reported on a quarterly term. It should be publicly available on the FFIEC website, as other lending institution data currently is. And finally, the data should be viewable by individual institution, not by the industry in the aggregate; it should identify where the attempted fraud took place; it should also support analysis based on the number of customers the institution has, the number of accounts it has, and its market capitalization.[35]

[35] Chris Walsh suggests that anonymized, case-level information be kept by banks in order to do studies of specific studies of identity theft incidences. Email from Chris Walsh, Information Security Consultant, to Chris Hoofnagle, Senior Staff Attorney, Samuelson Clinic (Feb. 20, 2007) (on file with author).

5. The Challenges of the Reporting Approach

Several challenges, some political and some practical, are raised by my proposal to have lending institutions report statistical data on identity theft incidences. In this section, I address these challenges. In the next, I argue that the benefits of reporting outweigh the challenges faced by the proposal.

Institutions Themselves Are Not Always Aware of Identity Theft

The measurement problem is more complex than I have portrayed thus far. This is because many institutions cannot always tell when identity theft has occurred.

Accounts used by identity thieves eventually become delinquent. Institutions cannot always determine whether these delinquent accounts are the result of an inability to pay, or an unwillingness to pay. Detection may also be delayed until the institution engages in its regular accounting: "Identity theft…can go undetected for weeks or months—for a business, often not until the end of a reporting quarter"[36]

Avivah Litan has elaborated on this problem: "Many banks, credit card issuers, cell phone service providers and other enterprises that extend financial credit to consumers don't recognize most identity theft fraud for what it is…Instead they mistakenly write it off as credit losses, causing a serious disconnect between the magnitude of identity theft that innocent consumers experience and the industry's proper recognition of the crime. This causes a disincentive to fix the problem with the urgency it requires."[37]

---

[36] Collins, J.M. and Hoffman, S.K. (2004*) Identity Theft: Predator Profiles* 4, Submitted to Security Journal. Manuscript available from Judith Collins, - judithc@msu.edu.
[37] Gartner, Inc., *Gartner Says Identity Theft Is Up Nearly 80 Percent, 7 Million U.S. Adults Were Identity Theft Victims in the Past 12 Months*, Jul. 21, 2003, available at

This limitation on detection will affect my proposal. Of course, all systems of measurement are imperfect. But even flawed reporting from the lending institutions would be preferable to no reporting at all, and the continued reliance on inaccurate polling methods. In addition to being more accurate, reporting will provide additional benefits described in section six.

Reporting Could Enable Fraud

There is the argument that in providing statistics on products most vulnerable to identity theft, reporting may provide a "roadmap" for fraudsters. Thieves may target instant credit opportunities or steal convenience checks in the mail because statistics show that it is easy to commit identity theft with them.

But this roadmap already exists. Methods of identity theft are well known, and in the grasp of even unsophisticated criminals, as evidenced by the prevalence of the crime, and the amount of economic loss than even the lowest estimates have found. Furthermore, the reporting requirements described in this article are basic; they do not provide specific information on tactics, methods or vulnerabilities. They are unlikely to be of more use to fraudsters than ordinary newspaper reporting on methods of identity theft.

Reporting Will Pitch Lending Institutions Against Victims

Professor Daniel Solove has argued in response to my proposal that if lending institutions have to report information about identity theft losses, it will create bad incentives: the institutions will be less likely to accept victims' claims of identity theft, and try to have the victim pay for fraudulent charges made by others. Victims will be

---

http://www.gartner.com/5_about/press_releases/pr21july2003a.jsp (last visited Dec. 19, 2006).

viewed skeptically and treated as criminals themselves, in order to drive down the number of transactions that are reported as fraudulent.

Solove's objection is a serious one. It may be the case that existing protections for consumers, such as statutory liability caps for fraudulent charges,[38] will have to be revisited. More serious disincentives to frivolous or unsubstantiated denials of victims' claims may have to be established. One could imagine a lending institution analogue to bad faith denials of insurance claims, where a wronged victim could collect damages where the lending institution rejected a victim's dispute of fraudulent charges without justification.

Alternatively, the duty to report could be implemented so that lending institutions have to identify all situations where the victim challenged a charge as fraudulent. In cases where the institution suspects that the victim really made the charges, the institution could report these incidents as "familiar" fraud to distinguish them from cases where identity theft is clearly present.

Still, Solove's argument may undervalue the power of competition to correct consumer protection issues. If a certain institution develops a reputation for challenging consumers' good faith claims of fraud, that institution could lose customers to one that is more solicitous to victims.

[38] Under the Truth in Lending Act, a implemented by "Regulation Z," consumers are liable for a maximum of $50 for fraudulent charges. The burden of proof is upon the issuer to show that fraud is not present. 15 USC § 1643 (2007). In practice, the major issuers have waived the potential $50 liability.

The Market Will Solve the Identity Theft Problem

Some may argue that lenders already have sufficient incentives to solve identity theft. Reporting simply adds regulatory burden to institutions, and are costly and unnecessary. Additionally, consumers don't bear the costs of identity theft, which are usually paid by lending institutions and merchants. A critic may argue that this particularly is true in synthetic identity theft cases, because the person whose information was used never becomes aware of the crime.

Whether the market will address identity theft largely depends the known unknowns of the crime. Currently we don't know the scope of the problem. We do know that it is a big problem and that the losses are estimated in the tens of billions. Without reporting, we cannot tell whether the market is addressing the problem. Reporting will elucidate the scope of the problem and its trends, and as explained below, create a real market for identity theft prevention.

Furthermore, understanding synthetic identity theft is important, because it demonstrates problems in the credit granting process. If we can understand why synthetic identity theft occurs, it will inform efforts to eliminate other forms of identity theft.

The fact that a synthetic identity thief can use a fake name in combination with a real Social Security number to obtain credit cards suggests that lending institutions are not authenticating the *identities* of credit applicants. This has serious public policy implications. In the public policy debate, lending institutions oppose privacy legislation,

arguing that increased privacy rights can prevent fraud prevention efforts.[39] But if lending institutions are only engaging in authentication of the Social Security number (ensuring that the number is issued to a live person, and that the credit applicant has a date of birth consistent with the number) rather than identity authentication (ensuring that the number is issued to the correct person), it means that lending institutions are not using all the tools available to them to prevent identity theft. Perhaps additional privacy laws will not harm their anti-fraud efforts, because they are not currently using already available information to authenticate the identities of credit applicants.

The reporting proposed in this paper builds upon "red flag" guidelines that federal financial regulators are developing for lenders.[40] These red flags are warnings of certain suspicious behavior that may indicate fraud is about to occur. They include situations where a consumer makes an application for credit and a change of address at the same time. In such situations, institutions must take more steps to ensure that the application is not fraudulent.

I also object to the notion that consumers do not bear the cost of identity theft. Consumers ultimately pay for the crime through lost time, inconvenience, higher financial services fees, and sometimes through out-of-pocket costs.[41] Fees for financial

---

[39] Hjalma Johnson, *Banking and the Future of Financial Privacy: A Commitment to Our Customers*, American Bankers Association (Nov. 15, 1999), available at http://www.aba.com/Press+Room/PR_Privacy_HJSpeech.htm; AMERICAN BANKERS ASSOCIATION, THE DEVASTATING EFFECT OF OPT-IN RESTRICTIONS (n.d.), available at http://www.aba.com/Industry+Issues/GR_PR_Opt-in.htm.

[40] Federal Reserve Board, *Agencies Propose Rules on Identity Theft Red Flags and Notices of Address Discrepancy*, Jul. 18, 2006, available at http://www.federalreserve.gov/BOARDDOCS/PRESS/bcreg/2006/20060718/default.htm

[41] The FTC found that the average victim spent $500 of their own money, and 30 hours of time resolving identity theft incidences. FEDERAL TRADE COMMISSION, IDENTITY THEFT

services products have continued to rise;[42] if identity theft rates were reduced, perhaps these fees would be lower.

Finally, there is another, largely unknown way in which we all pay for identity theft that causes the market not to correct the problem: lending institutions write their losses off against corporate income taxes. Accordingly, identity theft is tax-subsidized; it is deducted from earned income like any ordinary business expense. It is not a true loss to lending institutions unless the burden is greater than an institution's total tax liability.

6. The Benefits of the Reporting Approach

Reporting Will Identify the Most Vulnerable Practices

While there are challenges to identity theft reporting, I believe that the disadvantages are outweighed by other factors. Reporting creates several new opportunities that can be leveraged in the fight against identity theft.

First, reporting will make it possible for institutions, regulators, and the public to identify the practices most vulnerable to theft. It may be the case that instant credit opportunities, which can be completed online in minutes, are far more likely to be the target of fraud than mortgage loans, which typically require more due diligence. If this is the case, interventions can be tailored to the level of risk involved with different products. For instance, regulators might require lenders to collect more personal information for

---

SURVEY REPORT 6 (Sept. 2003), available at http://www.ftc.gov/os/2003/09/synovatereport.pdf.

[42] "Of the fourteen fees for which comparisons are available…multistate banks charged significantly higher fees in eight cases and in no case charged a significantly lower fee." FEDERAL RESERVE, ANNUAL REPORT TO THE CONGRESS ON RETAIL FEES AND SERVICES OF DEPOSITORY INSTITUTIONS 8 (June 2003), available at http://www.federalreserve.gov/boarddocs/rptcongress/2003fees.pdf

instant credit applications, or cap the amount of money that can be lent on a new instant credit account until a first payment is received.

Reporting Will Provide Metrics for Interventions

Second, reporting will help all parties decide whether interventions are appropriate, too burdensome, or in need of strengthening. For instance, in California, lenders of in-store instant credit must collect at least three types of personal information from an applicant before granting a new account.[43] The point of this provision is to give retailers incentives to avoid the crime by properly identifying new customers. But, has this provision been effective? Are three identifiers enough, or should more be collected? By identifying the number of fraud attempts and their vectors, one could determine whether this regulation contributes to better security by comparing statistics from California and other states.

Some practices might be so prone to attracting identity theft that they should be stopped entirely. For instance, institutions regularly send unsolicited pre-approved credit card offers to addresses that are not up-to-date. They also send unsolicited "convenience checks." These can be lifted from the mail and used by even unsophisticated thieves.[44] It

[43] Cal. Civ. Code 1785.14.1 (2007).

[44] One consumer took an unsolicited credit card offer, ripped it up, reassembled it, and then submitted it to a bank with a change of address. The bank issued the card, and even sent it to the different address, thus demonstrating that a thief could easily use even a torn-up offer for fraud. Bob Sullivan, *Even torn-up credit card applications aren't safe*, MSNBC, Mar. 14, 2006, available at http://redtape.msnbc.com/2006/03/what_if_a_despe.html. In a different case, Chase Manhattan bank issued a platinum visa card to "Clifford J. Dawg." In this instance, the owner of the dog had signed up for a free e-mail account in his pet's name and later received a pre-approved offer of credit for "Clifford J. Dawg." The owner found this humorous and responded to the pre-approved offer, listing nine zeros for the dog's Social Security number, the "Pupperoni Factory" as employer, and "Pugsy Malone" as the mother's maiden name. The owner also wrote on the approval: "You are sending an

may be the case that these practices cause too much fraud, and should be subject to consumer consent before they are sent.

Currently, we have no tools to do a meaningful cost-benefit analysis of these regulatory interventions. Reporting is the best method to get the data needed to make smart decisions.

Reporting Will Eliminate Some Polling Mischief

Identity theft is a high-stakes issue in the public policy world. It is a popular issue for political candidates, who have proposed many laws with serious implications for lending institutions. Because identity theft brings regulatory attention to lending institutions, there is great pressure to redirect that attention elsewhere.

One tactic is to issue "press release" surveys, research with questionable methods that take the regulatory heat off of lending institutions.[45] In this field, that function is being performed by Javelin Research, which has released polls sponsored by the financial service industry showing that identity theft is on the decline.[46] But Javelin Research's polls do not reflect synthetic identity theft, for the reasons explained in section three.[47]

---

application to a dog! Ha ha ha." The card arrived three weeks later. *Dog Gets Carded*, Wash. Times (Jan. 30, 2004), available at http://washingtontimes.com/upi-breaking/20040129-031535-6234r.htm; *Dog Issued Credit Card, Owner Sends In Pre-Approved Application As Joke*, NBC San Diego (Jan. 28, 2004), available at http://www.nbcsandiego.com/money/2800173/detail.html.

[45] For an in depth discussion of the "market" for policy research, *see* Oscar H. Gandy, Jr. *The role of theory in the policy process. A response to Professor Westin*. pp. 99-106 in C. Firestone and J. Schement (Eds.). Toward an Information Bill of Rights and Responsibilities. Washington DC: The Aspen Institute Communications and Society Program, 1995.

[46] Javelin Research, *U.S. identity theft losses fall: study, Feb. 1, 2007*, available at http://www.javelinstrategy.com/2007/02/01/us-identity-theft-losses-fall-study/#more-607.

[47] See supra footnote 7.

However, if the group can convince policymakers that identity theft is on the decline, it may protect the study's sponsors (Visa) from regulatory interventions.

Contrary to the existing literature,[48] Javelin Research also makes the bold claim that most identity theft is committed by friends or family members of the victim.[49] The implication of this argument is that somehow the victim is at fault for not securing information from friends and family members. The point here is to convince policymakers to take the focus off the role of the lending institution in identity theft, and place it on the victim. But Javelin Research's observations on whether the crime is connected to the victim are based on responses of a very small subset of the sample of victims that are generalized to the entire population.[50] The FTC has characterized Javelin Research's conclusion as "misleading."[51]

---

[48] The FDIC reported in 2004 that: "Some industry analysts and security professionals estimate that 65 to 70 percent of identity theft is committed with confidential information stolen by employees or participants in transactions or services. In a survey conducted in 2003, an estimated half of all workers and managers who had access to customer information said that it would be either “easy” or “extremely easy” for workers to remove sensitive data from corporate databases. Two-thirds of the respondents believed that their coworkers, not hackers, posed the greatest risk to consumer privacy. Insiders can sell the information or use it directly to commit identity theft. Because of the increased networking of internal operations and pervasiveness of huge customer databases, financial institution employees have access to more customer information than ever before. The exact size of the problem is unknown, but fraud is sometimes perpetrated by financial institution insiders, often in ways that require little technical sophistication." FDIC, PUTTING AN END TO ACCOUNT-HIJACKING IDENTITY THEFT (Dec. 14, 2004), available at http://www.fdic.gov/consumers/consumer/idtheftstudy/index.html.

[49] JAVELIN RESEARCH, 2007 IDENTITY FRAUD SURVEY REPORT, Feb. 2007; JAVELIN RESEARCH, 2006 IDENTITY FRAUD SURVEY REPORT, Jan. 2006; JAVELIN RESEARCH, 2005 IDENTITY FRAUD SURVEY REPORT, Jan. 2005.

[50] For instance, in the group's 2007 survey, only 144 of the 469 victims identified knew who stole their identity. Javelin Research, *U.S. identity theft losses fall: study*, Feb. 1, 2007, available at http://www.javelinstrategy.com/2007/02/01/us-identity-theft-losses-fall-study/#more-607. This problem with this approach is that in order to generalize from this small sample, the researcher has to show that the data are exchangeable. That is, the data about small subset of people who knew the thief must be similar to the larger portion

With reporting, better information will be provided, and we could really know whether regulatory interventions are still justified. Reporting will limit specious "press release" surveys from affecting the policy debate.

Reporting Will Dramatically Reduce Identity Theft, As A True Market For Protecting Consumers Will Arise

Elsewhere, I have written that identity theft debates ignore the role of the financial institution in the fraud.[52] While one should be careful not to "blame the victim" of a crime, it is evident that lax lending standards contribute to identity theft, and thus, institutional practices deserve scrutiny in the debate.[53]

---

who did not. Chris Jay Hoofnagle, *Javelin's Bogus Analysis of Identity Theft*, Feb. 2, 2007, available at http://chrishoofnagle.com/blog/?p=680

[51] Email message from Claudia Bourne Farrell, Office of Public Affairs, Federal Trade Commission, to Robin Sidel, Correspondent, The Wall Street Journal, Oct. 20, 2005, available at http://chrishoofnagle.com/blog/wp-content/uploads/2007/02/ftc_email_on_javelin.pdf

[52] Hoofnagle, Chris Jay, "Putting Identity Theft on Ice: Freezing Credit Reports to Prevent Lending to Impostors" in SECURING PRIVACY IN THE INTERNET AGE, Stanford University Press, forthcoming 2007, available at http://ssrn.com/abstract=650162.

[53] A victim responding to ITRC's 2003 survey illustrates this problem: "…the credit card was issued with just a version of my name and social, all over the phone, without the requirement to present personally positive picture ID, a signature, or a fingerprint. The card was then sent to an address that could not be verified on my credit report, and a second card issued at the same time under another surname. Sears Gold Master Card gave the police nothing to work with." IDENTITY THEFT RESOURCE CENTER, IDENTITY THEFT: THE AFTERMATH 2003 42 (Sept. 23, 2003), available at http://www.idtheftcenter.org/idaftermath.pdf. The problem of negligent granting of credit has been explored in numerous cases, but courts have been unwilling to assign liability to lenders for their role in facilitating identity theft. *See Vazquez-Garcia v. Trans Union de Puerto Rico*, 222 F. Supp. 2d 150, 153 (D. Puerto Rico 2002) (impostor successfully obtained credit with matching Social Security Number but incorrect date of birth and address); *United States v. Peyton*, 353 F.3d 1080 (9th Cir. 2003) (impostors obtained six American Express cards using correct name and Social Security Number but directed all six to be sent to the impostors' home); *Aylward v. Fleet Bank*, 122 F.3d 616 (8th Cir. 1997) (bank issued two credit cards based on matching name and Social Security Number but incorrect address); *Nelski v. Pelland*, 2004 U.S. App. LEXIS 663 (6th Cir. 2004) (phone company issued credit to impostor using victim's name but

Above, in section two, I detailed a synthetic identity case where 250 credit cards were obtained using real Social Security numbers but fake names. One of the incidents involved using the Social Security number of "Haqqani Saifullah" to obtain a credit card in "Hanna Curin's" name.[54] These names are not similar in any way. One would hope that thieves couldn't just fabricate information in their quest for credit cards, but apparently they can. Such incidents should make one question whether lending institutions are doing an appropriate job in screening applications for fraud.

Many have observed that identity theft is an easy crime to commit: "identity theft is a low risk, easily conducted crime and apprehension is difficult if not impossible," observes Collins and Hofmann.[55] Although the problem is often framed as a battle between sophisticated computer hackers and vigilant banks, in reality, most identity theft occurs offline,[56] and a surprising amount is committed by street-level criminals, sometimes in the midst of methamphetamine binges.[57]

---

slightly different Social Security Number); *Dimezza v. First USA Bank, Inc.*, 103 F. Supp. 2d 1296 (D.N.M. 2000) (impostor obtained credit with Social Security Number match but incorrect address).

[54] *Rose*, indictment at 5.

[55] Collins, J.M. and Hoffman, S.K. (2004) *Identity Theft: Predator Profiles* 9, Submitted to Security Journal. Manuscript available from Judith Collins, - judithc@msu.edu.

[56] James van Dyke, *New Research Shows That Identity Theft Is More Prevalent Offline with Paper than Online*, Javelin Strategy Press Release, Jan. 26, 2005, available at http://www.bbb.org/alerts/article.asp?ID=565.

[57] John Leland, *Stolen Lives, Meth Users, Attuned to Detail, Add Another Habit: ID Theft*, N.Y. Times, Jul. 11, 2006, available at http://www.nytimes.com/2006/07/11/us/11meth.html; "Of the n = 1,037 perpetrators, n = 155 (15%) were reported as being involved in narcotic and drug dealings (Table 10). In 2001, researchers in the MSU Identity Theft Crime and Research Lab first became aware, through investigations and from other reports, of the link between identity theft and methamphetamine trafficking. Increasingly, reports associated especially with methamphetamine labs implicate perpetrators of identity theft. Today, the use of stolen identities for the production, sale, and to support the use of methamphetamine habits is epidemic." Collins, J.M. and Hoffman, S.K. (2004) Identity Theft: Predator Profiles 15,

Institutions' role in identity theft became so suspect in recent years that analysts suggested that they were not screening credit applications for fraud. For instance, Avivah Litan wrote in 2003 that banks should implement fraud screening systems: "Most importantly, however, banks and FSPs (financial service providers) must implement solutions that effectively screen for application fraud, so they don't wrongfully extend credit to identify thieves…Without industry prevention efforts, consumers whose identities have been stolen will continue to bear the brunt of social and indirect economic costs." [58]

Reporting will enable institutions to distinguish themselves as leaders in fighting identity theft. With statistics showing relative risks of fraud from each institution, keyed to the number of accounts and capitalization the lender has, consumers will be able to make distinctions in the marketplace. Currently, there is no way to do so.[59]

7. Conclusion

The public and policymakers continue to know very little about the scope, forms, and severity of the fastest growing white collar crime, identity theft. As a result, policymakers, the public, and businesses cannot gauge the seriousness of the crime and respond appropriately. Misperceptions of the crime endure because it is measured with

---

Submitted to Security Journal. Manuscript available from Judith Collins, - judithc@msu.edu.

[58] GARTNER, INC., GARTNER SAYS IDENTITY THEFT IS UP NEARLY 80 PERCENT, 7 MILLION U.S. ADULTS WERE IDENTITY THEFT VICTIMS IN THE PAST 12 MONTHS, Jul. 21, 2003, available at http://www.gartner.com/5_about/press_releases/pr21july2003a.jsp (last visited Dec. 19, 2006).

[59] Javelin Research does produce a report called the "Javelin Identity Safety Scorecards" to judge institutions' protections against account takeover and efforts to remedy identity fraud. While this information is helpful, it does not provide actual data on the rates of identity theft.

public polling surveys of victims. This method is both under and overinclusive in measuring the crime.

A solution can be found in requiring lending institutions, the entities with the most information about identity theft, to make public reports about the crime will contribute to understanding of identity theft. All that is required to make the known unknowns of identity theft known is the reporting of: 1) how many identity theft incidences were suffered or avoided, 2) the form of identity theft attempted and the product targeted, and 3) the amount of loss suffered or avoided.

With such reporting, our understanding of the crime will be much more nuanced. Public policy interventions could be tailored to the crime's seriousness.

More importantly, an anti-identity theft market will be born. Lending institutions will be able to compete to offer the safest products, and consumers will be able to choose among them according to their comfort with risk.