Harvard Journal of Law & Technology
Volume 21, Number 1 Fall 2007

IDENTITY THEFT: MAKING THE KNOWN UNKNOWNS KNOWN

Chris Jay Hoofnagle[*]

TABLE OF CONTENTS

---

* Senior Staff Attorney, Samuelson Law, Technology & Public Policy Clinic; Senior Fellow, Berkeley Center for Law and Technology, University of California-Berkeley Boalt Hall School of Law. This Article has benefited greatly from feedback by Professor Daniel J. Solove, Mark Hoofnagle, Susan Hutfless, Chris Walsh, and Avivah Litan; my colleagues at Boalt Hall, Professor Deirdre K. Mulligan, Maryanne McCormick, and Jack Lerner; and the student editors at the *Harvard Journal of Law & Technology*. The work of the Samuelson Clinic is supported by the California Consumer Protection Foundation, the Rose Foundation for Communities and the Environment, and the National Science Foundation's Team for Research in Ubiquitous Secure Technology.

I. 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.[1]

There is widespread agreement that identity theft causes financial damage to consumers, creditors, retail establishments, and the economy as a whole.[2] The Federal Trade Commission ("FTC") has identified it as the fastest growing white collar crime;[3] federal and state governments have enacted numerous laws to curb its incidence and severity.[4]

The contours of the identity theft problem, however, are known unknowns: no one knows the prevalence of identity theft, the relative rates of "new account fraud" and "account takeover,"[5] or the effect this crime has on the economy. What is more, the advent of "synthetic" identity theft[6] has exacerbated these measurement difficulties.

---

1. Donald H. Rumsfeld, U.S. Sec'y of Defense, Department of Defense News Briefing (Feb. 12, 2002), http://www.defenselink.mil/transcripts/transcript.aspx?transcriptid=2636.

2. *See, e.g.*, *Privacy, Identity Theft, and the Protection of Your Personal Information in the 21st Century: Hearing Before the Subcomm. on Tech., Terrorism, and Gov't Information of the S. Comm. on the Judiciary*, 107th Cong. 12–14 (2002) [hereinafter *Stana Testimony*] (testimony of Richard M. Stana, Director, Justice Issues, General Accounting Office).

3. OFFICE OF CONSUMER & BUS. EDUC., FTC, PRIVACY: TIPS FOR PROTECTING YOUR PERSONAL INFORMATION 1 (2002) [hereinafter FTC REPORT], *available at* http://www.ftc.gov/bcp/conline/pubs/alerts/privtipsalrt.pdf.

4. *See* GRAEME R. NEWMAN & MEGAN M. MCNALLY, IDENTITY THEFT LITERATURE REVIEW 63–68 (2005), *available at* http://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf.

5. This Article discusses two types of identity theft: "new account fraud," where an impostor opens lines of credit in the victim's name, and "account takeover," where an impostor uses an established account, such as a credit card issued to a victim. *See Identity Theft: How to Protect and Restore Your Good Name: Hearing Before the Subcomm. on Tech., Terrorism, and Gov't Information of the S. Comm. on the Judiciary*, 106th Cong. 33–34 (2000) [hereinafter *Givens Testimony*] (testimony of Beth Givens, Director, Privacy Rights Clearinghouse). Both types of fraud are subsets of the crime of identity theft. This distinction is critical for policy purposes, because, historically, the costs of credit card fraud have been mostly borne by retailers and banks, whereas the costs of new account fraud could directly harm consumers. *See infra* Part II. This Article is not concerned with other types of identity theft, such as criminal record identity theft, where an impostor attributes an arrest or crime to a victim. *See, e.g.*, IDENTITY THEFT RES. CTR., IDENTITY THEFT: THE AFTERMATH 2003, at 5 (2003) [hereinafter ITRC], http://www.idtheftcenter.org/artman2/uploads/1/The_Aftermath_2003.pdf.

6. "Identity theft" describes the use of another individual's personal information for fraudulent purposes. *See, e.g.*, Jennifer Lynch, *Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks*, 20 BERKELEY TECH. L.J. 259, 260 (2005). Although there is no authoritative definition of synthetic identity theft, cases typically involve the use of an individual's real Social Security Number and date of birth with a false name and address. This blend of real and fabricated personal information can be used to apply for new accounts and create new credit files that credit issuers may

These known unknowns present serious problems. They hamper attempts to evaluate the scope of the crime and to allocate law enforcement resources more efficiently. They also prevent us from determining whether various consumer protection interventions have been effective. Because of these unknowns, we cannot tell whether consumers, regulators, and businesses are over- or under-reacting to the crime. They prevent us from evaluating how the costs of the crime are distributed in society. These unknowns even foreclose the basic determination of whether the prevalence or severity of identity theft has changed over time.

Why, despite increases in identity theft, are law enforcement, the public, industry, or policymakers unable to measure the crime accurately? This Article argues that the answer lies in the methods used to measure the problem. What we do know has been learned through telephone and Internet surveys; however, few in-depth studies have been done.[7] While well-intentioned and valuable for some purposes in the identity theft policy debate, these surveys cannot completely document the contours of the crime.

More fundamentally, however, we are asking the wrong people about the crime. The surveys seek to obtain information about identity theft from its victims — individuals who have the most limited view of the problem. Victims often do not know how their personal data were stolen or who stole the information.

Financial institutions are in a better position to report information on identity theft. If lenders and organizations that control access to accounts (including payment companies such as PayPal and Western Union) were required to provide statistics about identity theft, a more complete and detailed picture would emerge. However, these data have significant potential to cause embarrassment and attract unwanted regulatory attention, which may explain why these institutions have not made these data publicly available.

This Article proposes three disclosure requirements for financial institutions: (1) the number of identity theft incidents suffered or avoided; (2) the forms of identity theft attempted and the financial products targeted (e.g., mortgage loan or credit card); and (3) the amount of loss suffered or avoided. This proposal is relatively simple and does not require extensive regulatory mandates. While its implementation might face several practical and political challenges, improved reporting of identity theft would result in four benefits to the public. First, it would identify the business practices most vulnerable to fraud. Second, it would help to identify the consumer protections

---

believe represent real people. See *infra* Part II.A for a more in-depth explanation of synthetic identity theft.

7. *See, e.g.*, SYNOVATE, INC., FEDERAL TRADE COMMISSION — IDENTITY THEFT SURVEY REPORT 3 (2003), *available at* http://www.ftc.gov/os/2003/09/synovatereport.pdf.

that work and those that do not, and thus assist regulators and law enforcement agencies in allocating resources to combat the crime. Third, improved reporting would help focus public attention on the root causes of the crime. In particular, it could provide a potential counterpoint to the conclusions of some victim surveys that have relied on questionable assumptions and asserted that the fault for identity theft lies with the victims.[8]

Finally, providing more accurate, institution-level statistics on identity theft would make the security of personal information a new product differentiator, similar to low interest rates and fee-free accounts. It would enable benchmarking of financial institutions using that factor so that consumers could tell which institutions have the highest and lowest rates of fraud. Assuming that the market is competitive, it is likely that lenders that provide the safest financial products would be rewarded with consumer loyalty. This rubric would also pressure institutions bearing the ignominious mark of having the most identity theft to adapt or to be driven from the marketplace.

II. THE KNOWN KNOWNS: IDENTITY THEFT

Congress articulated the legal definition of identity theft in 18 U.S.C. § 1028, which criminalizes certain knowing uses of another's identification information.[9] FTC defines identity theft more broadly as "a fraud committed or attempted using the identifying information of another person without authority."[10] For the purposes of this Article, it is useful to think of identity theft as a type of fraud with two distinct categories: new account fraud and account takeover.

A. New Account Fraud

In new account fraud, an impostor opens lines of credit using the personal information of another.[11] Such lines of credit may include new credit card accounts, mortgages, or utilities. These types of credit require that the impostor have the victim's Social Security number

8. *See infra* Part VI.C; A Brown Study Blog, *Javelin's Bogus Analysis of Identity Theft*, http://chrishoofnagle.com/blog/?p=680 (Feb. 2, 2007) [hereinafter Brown Study Blog, *Javelin's Bogus Analysis*]; A Brown Study Blog, *Javelin Strategy: Raising Lysenko*, http://chrishoofnagle.com/blog/?p=682 (Feb. 27, 2007).

9. 18 U.S.C.A. § 1028 (West Supp. 2007). Identification information is broadly defined as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual." *Id.* § 1028(d)(7).

10. 16 C.F.R. § 603.2(a) (2007).

11. *See generally Protecting Social Security Numbers from Identity Theft: Hearing Before the Subcomm. on Social Security of the H. Comm. on Ways & Means*, 110th Cong. (2007) [hereinafter *Winston Statement*] (statement of Joel Winston, Associate Director, Division of Privacy and Identity Protection, FTC).

("SSN").[12] Generally, new account fraud is a serious problem for consumers, because the fraudulent accounts may appear on the victim's credit history, making it more difficult to obtain new credit. The impostor's use of the accounts may also act as a barrier to employment.[13]

An important subset of new account fraud is synthetic identity theft. While common new account fraud involves use of the victim's true name, in the case of synthetic identity theft, an impostor uses the victim's SSN with a fake name, thus creating a new, "synthetic" identity.[14] Alternatively, an impostor can create an identity from scratch, using entirely fabricated information.[15] A synthetic identity — sometimes supplemented with artfully created credit histories — can then be used to apply for credit. While it may sound improbable, this approach to opening new lines of credit is generally successful for two reasons. First, some lenders will give accounts to individuals with no credit history.[16] A synthetic identity simply has a "thinner" credit file — a characteristic consistent with a legitimate new customer who is just entering the credit market.[17] Second, the use of a real SSN may allow impostors to satisfy a lender's security measures; there is mounting evidence that credit issuers use the SSN for both identification and authentication, that is, to locate the applicant's credit file and to prove that the credit file belongs to the applicant.[18]

Not enough is known about synthetic identity theft, but initial indications suggest that it is a growing problem. According to Mike Cook of ID Analytics, a company that specializes in the reduction of fraud risk to businesses, synthetic identity theft "is a larger problem

---

12. *See* Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227, 1252 (2003).

13. *See* Press Release, White House Office of the Press Sec'y, Fact Sheet: The President's Identity Theft Task Force (May 10, 2006), http://www.whitehouse.gov/news/releases/2006/05/20060510-6.html.

14. *See* FRED H. CATE, THE CTR. FOR INFO. POLICY LEADERSHIP, HUNTON & WILLIAMS LLP, INFORMATION SECURITY BREACHES AND THE THREAT TO CONSUMERS 5–7 (2005), http://www.hunton.com/files/tbl_s47Details/FileUpload265/1280/Information_Security_Breaches.pdf.

15. TECH. SUPERVISION BRANCH, FED. DEPOSIT INSURANCE CORP., PUTTING AN END TO ACCOUNT-HIJACKING IDENTITY THEFT 4 n.2 (Dec. 14, 2004) [hereinafter FDIC REPORT], *available at* http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf ("[A] synthetic identity is a completely fabricated identity that does not correspond to any actual person.").

16. *See, e.g.*, Credit Card Offers for People with Bad Credit, http://www.creditcardguide.com/index_needcredit.html (last visited Dec. 1, 2007).

17. *See* Mike Cook, *The Lowdown on Fraud Rings*, 10 COLLECTIONS & CREDIT RISK 20, 24 (2005).

18. *See* Letter from Chris Jay Hoofnagle, Sr. Staff Att'y, Samuelson Law, Tech. & Publ. Policy Clinic to FTC, Office of the Sec'y (Sept. 5, 2007) (on file with the *Harvard Journal of Law & Technology*); Lesley Mitchell, *New Wrinkle in ID Theft: Thieves Pair Your SS Number with Their Name, Buy with Credit, Never Get Caught*, SALT LAKE TRIB., June 6, 2004, at E1 ("[B]usinesses granting credit do little to ensure names and Social Security numbers match and credit bureaus allow perpetrators to establish credit files using other people's Social Security numbers.").

than [common new account fraud] and is growing at a faster rate."[19] While there are no reliable figures documenting losses from synthetic identity theft, some experts estimate that "synthetic schemes constitute at least 20% of credit charge-offs and 80% of losses from credit-card fraud."[20]

United States v. Rose, a recent case brought by the U.S. Attorney for the District of Arizona, illustrates the problem of synthetic identity theft.[21] The indictment charged two men with a variety of federal crimes for allegedly combining fabricated names with real SSNs from credit reports in order to apply for credit cards.[22] One of the defendants owned a small consumer reporting agency,[23] and apparently had a high level of sophistication with credit practices. The pair established credit histories for the synthetic identities by reporting favorable payment information to consumer reporting agencies.[24] These reports made the synthetic identities appear to be real people with records of paying bills. The defendants then allegedly obtained 250 credit cards from 15 banks, and charged $760,000 to these synthetic identities.[25]

As explained in more detail in Part III.A, synthetic identity theft cannot always be detected by the individual whose SSN was used. This difficulty arises because the synthetic identity is an amalgam of false and real information; while sufficient to obtain credit, the identity, and the corresponding losses, may never be attributed to a real individual. In *Rose*, the defendants used real SSNs but wholly fabricated names.[26] For example, the SSN of identity theft victim Haqqani Saifullah was used to apply for a credit card for Hanna Curin, a synthetic identity.[27] None of the individuals whose SSNs were used by the defendants, however, suffered financially from the theft.[28]

As the *Rose* case illustrates, individuals whose identifying information is used to construct synthetic identities may not suffer direct financial losses as a result of the crime. However, victims of synthetic identity theft may suffer non-monetary losses. For instance, a debt

---

19. *See* Cook, *supra* note 17, at 24.

20. Christopher Conkey, *The Borrower Who Never Was; Synthetic-Identity Fraud Hits Credit Bureaus, Banks; A Night at the Ritz-Carlton*, WALL ST. J., Oct. 29, 2007, at B1, *available at* http://online.wsj.com/article/SB119362045526074445.html.

21. *See* William Carlile, *Two Indicted in Credit-Card Scheme that Used SSNs from Credit Reports*, 5 Privacy & Security L. Rep. (BNA) 1257 (Sept. 11, 2006); Conkey, *supra* note 20.

22. *See* Indictment *passim*, United States v. Rose, No. CR06-0787PHX (D. Ariz. Aug. 22, 2006) [hereinafter Rose Indictment] (on file with the *Harvard Journal of Law & Technology*).

23. *Id.* at 2.

24. *Id.*

25. *Id.* at 3–4.

26. *See id.* at 4–5, 7–8.

27. *Id.* at 5.

28. Carlile, *supra* note 21, at 1257.

collector attempting to recover funds associated with the synthetic identity's account may, in searching for the debtor, attribute the account to the real owner of the SSN. Such contacts from debt collectors may cause reputational harm and emotional distress, in addition to wasting the victim's time and resources.[29]

B. Account Takeover

In an account takeover, an impostor uses one of the victim's existing financial accounts. While credit card fraud is the most common example,[30] account takeover is a much broader category. In particular, it includes "phishing," the practice of tricking a victim into revealing passwords or other personal data that allow the thief to access or alter the victim's existing accounts.[31] In addition to credit cards, phishers target traditional checking and savings accounts, as well as payment systems and auction services such as PayPal and eBay.[32]

The impact of an account takeover on the consumer victim depends on the type of account targeted. Generally, this type of identity theft is less harmful to its victims than new account fraud.[33] A variety of consumer protection laws and self-regulatory practices limit liability for financial account takeovers.[34] For example, under federal law, consumers are only liable for fifty dollars in fraudulent credit card

---

29. *See generally* Solove, *supra* note 12; *see also* OFFICE OF CMTY. ORIENTED POLICING SERVS., U.S. DEP'T OF JUSTICE, A NATIONAL STRATEGY TO COMBAT IDENTITY THEFT 23 (2006), *available at* http://www.cops.usdoj.gov/mime/open.pdf?Item=1732.

30. *See* SYNOVATE, *supra* note 7, at 11–12.

31. *See* OFFICE OF CONSUMER & BUS. EDUC., FTC, HOW NOT TO GET HOOKED BY A 'PHISHING' SCAM 1 (2006), *available at* http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.pdf.

32. *See* SYNOVATE, *supra* note 7, at 4–5; Scott Ferguson, *Study: eBay, PayPal Remain Top Phishing Targets*, EWEEK.COM, July 27, 2006, http://www.eweek.com/article2/0,1759,1995374,00.asp.

33. Many commentators characterize new account fraud as being typically, or even categorically, more harmful to consumers than existing account crimes. *See, e.g.*, *Winston Statement*, *supra* note 11. This may be less true in the case of synthetic identity theft if the losses are not attributed to a real victim. Furthermore, existing account fraud can at least temporarily exhaust a victim's bank account, resulting in bounced checks and missed housing payments. Financial services expert Avivah Litan has documented a decline in fraud recovery rates for victims of existing account fraud, which means that victims of these crimes in many cases experience substantial, direct financial losses from the fraud. *See* Press Release, Gartner, Inc., Gartner Says Number of Phishing E-Mails Sent to U.S. Adults Nearly Doubles in Just Two Years (Nov. 9, 2006), http://www.gartner.com/it/page.jsp?id=498245.

34. *See, e.g.*, Electronic Fund Transfers (Regulation E), 12 C.F.R. § 205 (2007); Truth in Lending (Regulation Z), *id.* § 226; American Express — Fraud Protection Center, https://www124.americanexpress.com/cards/cda/dynamic.jsp?name=FraudProtectionGuarantee_SharedDetailsALL&type=intBenefitDetail (last visited Dec. 1, 2007) (offering zero liability for use of credit card without cardholder consent). In addition, many financial institutions employ systems to detect fraudulent access to accounts, and most major U.S. banks participate in the Anti-Phishing Working Group. *See* Anti-Phishing Working Group, http://www.antiphishing.org (last visited Dec. 1, 2007).

charges if the consumer reports the loss to the financial institution within two business days.[35] In addition, consumers can dispute credit card charges when they receive their statements. In contrast, takeover of a non-credit account, such as a checking or savings account, may leave the victim with no money and consequently no ability to pay bills. Furthermore, despite regulatory protections for consumers' non-credit accounts, in many cases consumers do not recover the full amount of the fraudulent charges. In 2005, on average, consumers recovered only 80% of their losses from phishing attacks.[36] In 2006, the number dropped to 54%.[37]

III. THE KNOWN UNKNOWNS

Numerous attempts have been made to count the victims of identity theft and to estimate the cost of the crime to the economy.[38] Many of the studies have suffered from a fundamental lack of data access — they did not use data from financial institutions, which are the entities with the most information about the crime.[39] This methodological flaw can help explain why the prevalence and severity of identity theft have remained known unknowns.

A. Missing Data and Other Limitations of Identity Theft Surveys

Surveys of identity theft victims have been widely employed to map the contours of identity theft.[40] Such studies are clearly valuable because they explicate the challenges faced by victims recovering from the crime. However, victim surveys do not capture synthetic identity theft, a critical piece of the crime.[41] Synthetic identity theft is elusive because the individuals whose information was used may never become aware of the crime, and thus do not convey a victim

35. 12 C.F.R. § 205.6(b)(1).

36. Press Release, Gartner, *supra* note 33.

37. *Id.*

38. *See Stana Testimony*, *supra* note 2, at 6–17; RUBINA JOHANNES, JAVELIN STRATEGY & RESEARCH INC., 2006 IDENTITY FRAUD REPORT 50 (Mary T. Monahan ed., 2006) (on file with the *Harvard Journal of Law & Technology*); SYNOVATE, *supra* note 7, at 10–16, 38–48.

39. *But see* ID ANALYTICS INC., NATIONAL FRAUD RING ANALYSIS: UNDERSTANDING BEHAVIORAL PATTERNS 3–4 (2005), *available at* http://www.idanalytics.com/assets/pdf/National_Fraud_Ring_Analysis_Overview.pdf (using over 300 million account applications received from credit card, wireless carrier, and instant lending companies).

40. *See supra* note 38 and accompanying text.

41. Javelin Research, the leading firm that administers polls on identity theft, claims that its survey can measure some instances of synthetic identity theft in which the thief uses a mixture of true and fabricated information. However, Javelin acknowledges that its survey does not capture instances of synthetic identity theft "based upon a wholly fictitious identity." RACHEL KIM, JAVELIN STRATEGY & RESEARCH INC., 2007 IDENTITY FRAUD SURVEY REPORT — CONSUMER VERSION 10 (2007) (on file with the *Harvard Journal of Law & Technology*).

story to a polling organization.[42] Individuals whose data were used to create the synthetic identity rarely, if ever, report the crime to law enforcement agencies because "the combination of the name, address and Social Security number do[es] not correspond to one particular consumer."[43] As a result, the fraud often goes undetected. Financial institutions are also unlikely to report the theft. As the consumer reporting agency Experian explains, "no victim steps forward to claim fraud," so the "accounts are charged-off as a credit loss before the institution is aware of the problem."[44]

In 2002, the Government Accountability Office ("GAO") attempted to determine whether reports from victims of identity theft had increased.[45] The GAO study relied on interviews with employees of consumer reporting agencies, FTC, the Social Security Administration, victims of the crime, and federal law enforcement representatives.[46] GAO investigators employed several innovative methods, such as tracking the staffing levels of fraud departments of the consumer reporting agencies.[47] The results were contradictory: some consumer reporting agencies increased the number of staff in their fraud departments, while others did not.[48] Although the GAO only observed the shadows of the crime, its investigators concluded that both the prevalence and cost of identity theft were increasing.[49]

ID Analytics authored the most ambitious study of synthetic identity theft to date.[50] Having examined more than 300 million credit applications submitted by individuals to financial institutions over 2 years, the firm 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

42. *See* Thomas Oscherwitz, *Synthetic Identity Fraud: Unseen Identity Challenge,* BANK SECURITY NEWS, Apr. 2005, at 1 (on file with the *Harvard Journal of Law & Technology*).

43. Cook, *supra* note 17, at 24.

44. EXPERIAN, AN INTEGRATED APPROACH TO THE WORLD OF IDENTITY RISK MANAGEMENT (2005), http://www.experian.com/products/precise_id.html (click on hyperlink to White Paper) (last visited Dec. 1, 2007).

45. *See Stana Testimony*, *supra* note 2, at 6–17 (incorporating the GAO study into the record).

46. *Id.* at 9.

47. *Id.* at 12.

48. *Id.*

49. *See id.* at 14.

50. ID ANALYTICS, *supra* note 39, at 4.

> fraud, compared to 26.2% for true-name identity theft.[51]

If these findings are accurate, most instances of new account fraud and their attendant financial losses will never be detected by polls of victims, because there are no real consumer victims and the financial institution generally is not polled or is unaware that the fraud occurred.

Survey research on identity theft has other limitations. For instance, it is not clear that the surveyors confirm that members of the sample were actually victims.[52] Thus, such studies may be overinclusive: surveys may incorrectly include subjects who may be confused about suspicious events or those who may have been victims of a security breach,[53] not identity theft.[54] A better approach would focus on victims whose poll results are supported by reliable evidence, such as police reports.

All of these factors contribute to the wildly disparate estimates of the identity theft problem. For example, a 2003 poll found that identity theft had cost victims and businesses $47 billion in the previous 12 months.[55] In contrast, a 2003 study of a small sample of actual victims counseled by the Identity Theft Resource Center ("ITRC") estimated the total losses to businesses from identity theft to be $279 billion.[56] These factors make the scope and severity of the crime a known unknown.

B. Law Enforcement Statistics Do Not Capture the Problem

For a variety of reasons, law enforcement statistics do not capture the contours of identity theft. First, one study has found that "[m]ost victims of ID Theft do not report the crime to criminal authorities."[57]

---

51. Cook, *supra* note 17, at 24.

52. *Compare* SYNOVATE, *supra* note 7, at 3, *with* ITRC, *supra* note 5, at 48.

53. For purposes of California's security breach notification law, a security breach occurs when certain sensitive personal information is accessed by someone without authority. *See* CAL. CIV. CODE § 1798.82 (West 2007).

54. A security breach does not necessarily result in identity theft. *See* Brendan St. Amant, Recent Development, *The Misplaced Role of Identity Theft in Triggering Public Notice of Database Breaches*, 44 HARV. J. ON LEGIS. 505, 511 (2007).

55. SYNOVATE, *supra* note 7, at 7.

56. ITRC, *supra* note 5, at 27. The differences between the Synovate and ITRC studies may be attributed to differences in the data samples. Data for the Synovate study were acquired by calling thousands of households in order to locate several hundred victims of identity theft. In doing so, Synovate included many victims of account takeover, which is a less serious crime that is easier to resolve than the crimes included in ITRC's sample. The ITRC sampled confirmed victims of identity theft who had contacted the ITRC. Arguably, victims in ITRC's sample suffered more serious forms of identity theft because they sought assistance from the ITRC. *Compare* SYNOVATE, *supra* note 7, at 3, *with* ITRC, *supra* note 5, at 48.

57. SYNOVATE, *supra* note 7, at 9.

This may be especially true with respect to account takeovers, because the victim can often limit the effects of that type of identity theft with a call to the financial institution.[58] The ability to easily resolve the issue probably decreases the incentive to report the crime.

Second, when a victim does try to contact the authorities, some law enforcement agencies may view the financial institution as the victim and hesitate to file a report.[59] If the identity theft took place in another jurisdiction, police may tell the victim to file the report there; in turn, police in that jurisdiction may then tell the victim to file the report in the jurisdiction in which he lives.[60] This runaround has caused many states to adopt statutes requiring law enforcement agencies to take reports upon request from victims residing in their jurisdictions.[61]

Third, financial institutions may fail to report the crime and instead misclassify it as a different, non-fraudulent type of loss to avoid reputational injury. As the ITRC has observed, "[u]nfortunately, many commercial victims do not report the crime to law enforcement, considering it more fiscally advantageous to 'write off the loss.'"[62] Some commentators note that "even though this crime became epidemic [in] the last decade, many companies remain reluctant to report the thefts of their employees' or customers' identities for fear of losing business."[63] In addition to tarnishing a company's brand, severe identity theft losses may undermine confidence in the security and fiscal soundness of the financial institution. Such losses are likely to trigger unwanted examinations and costly compliance duties by federal regulators.[64]

Fourth, even when fraud is detected, the Federal Bureau of Investigation ("FBI") or local law enforcement may decline to investigate unless the fraud exceeds a certain degree of severity, due to insufficient resources.[65] Law enforcement's failure to respond may deter some commercial victims from reporting the crime at all. Only in rare

---

58. *See id.* at 26.

59. *Givens Testimony*, *supra* note 5, at 34.

60. *See* OFFICE OF CMTY. ORIENTED POLICING SERVS., *supra* note 29, at 17.

61. *See, e.g.*, CAL. PENAL CODE § 530.6(a) (West 2007); *see also* OFFICE OF CMTY. ORIENTED POLICING SERVS., *supra* note 29, at 17–21.

62. ITRC, *supra* note 5, at 5.

63. Judith M. Collins & Sandra K. Hoffman, Identity Theft: Predator Profiles 3 (Dec. 2004) (unpublished manuscript, on file with the *Harvard Journal of Law & Technology*).

64. *See, e.g.*, 12 U.S.C. § 1831p-1 (2000) (empowering the Federal Deposit Insurance Corporation to establish standards for "safety and soundness" to address the risks associated with operating a financial institution).

65. *See, e.g.*, JANINE BENNER ET AL., PRIVACY RIGHTS CLEARINGHOUSE, NOWHERE TO TURN: VICTIMS SPEAK OUT ON IDENTITY THEFT § 3 (2000), *available at* http://www.privacyrights.org/ar/idtheft2000.htm. For instance, in Southern California even a fraudulent event resulting in a $50,000 loss will not necessarily trigger an investigation. Joseph Majka, Vice President, Visa, Inc. Fraud Control, Remarks at the Summit on Solutions: Teaming Up Against Identity Theft (Feb. 23, 2006).

cases are identity thieves pursued and restitution sought: in 2003, the Gartner Group estimated that "criminals still have a one out of 700 chance of getting caught by federal authorities."[66] Of the identity thieves caught, perhaps half actually serve time in prison.[67]

Fifth, identity theft presents a number of data collection and management issues. In 2002, the GAO reported that "[g]enerally, federal law enforcement agencies do not have information systems that specifically track identity theft cases."[68] This is partly because identity theft typically is not a "stand-alone crime"; it is often committed as part of a larger criminal enterprise.[69] Thus, the crime may be included in the reporting of other types of financial fraud.

IV. MAKING THE KNOWN UNKNOWNS KNOWN

A. Mandated Public Reporting of Identity Theft Incidence and Severity

The limited insights provided by public polling and law enforcement statistics would be improved by requiring financial institutions to publicly report identity theft. Lenders, after all, are also victims. They are a focal point for information about the crime because they lend the money to the thief and experience nonpayment. Eventually, this loss must be documented in order to calculate the institution's profitability; however, there is currently no requirement that financial institutions specifically enumerate or reveal these losses to the government or the public.[70]

---

66. AVIVAH LITAN, GARTNER, INC., UNDERREPORTING OF IDENTITY THEFT REWARDS THE THIEVES 1 (2003), *available at* http://www.gartner.com/press_gartner/images/116066.pdf.

67. In a study involving 933 defendants in 517 Secret Service cases against alleged identity thieves, 51% received a sentence of incarceration. GARY R. GORDON ET AL., IDENTITY FRAUD TRENDS AND PATTERNS: BUILDING A DATA-BASED FOUNDATION FOR PROACTIVE ENFORCEMENT 23 (Oct. 22, 2007), *available at* http://www.utica.edu/academic/institutes/cimip/publications/index.cfm?action=form&paper=6.

68. *Stana Testimony*, *supra* note 2, at 10.

69. *Id.*

70. The reporting proposed in this Article complements the "red flag" guidelines that federal financial regulators are developing for lenders. Initially proposed in 2006, the guidelines describe "patterns, practices, and specific forms of activity that indicate the possible existence of identity theft" and require financial institutions to create an identity theft prevention program to address such risks. These guidelines do not require the reporting of identity theft incidents in the manner proposed in this Article. *See* Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, 71 Fed. Reg. 40786, 40788 (proposed July 18, 2006) (to be codified at 12 C.F.R. pts. 41, 222, 334, 571, 717); Press Release, Bd. of Governors of the Fed. Reserve Sys., Fed. Reserve Bd. et al., Agencies Propose Rules on Identity Theft Red Flags and Notices of Address Discrepancy (July 18, 2006), http://www.federalreserve.gov/newsevents/press/bcreg/bcreg20060718a1.pdf. Reporting on the incidence and severity of identity theft offers an opportunity to benchmark the success of the potentially costly red flag program. The regu-

Financial institutions account for nonpayment caused by identity theft either by absorbing the loss or by charging the loss back to the merchant from whom the thief purchased the goods. Lenders should be required to expand upon this basic financial accounting by tracking: (1) the number of incidents suffered or avoided; (2) the forms of identity theft attempted and the financial products targeted by the perpetrator; and (3) the amount of loss suffered or avoided. Furthermore, these data should be made publicly available through disclosures to a financial regulator. Such reporting would help unmask the known unknowns of identity theft.

The first part of this Article's proposal requires financial institutions to disclose the number of incidents of identity theft they suffered or avoided. In particular, the lender should record and report each incident of account takeover or new account fraud. Additionally, reports should indicate how the identity theft was discovered, such as via automatic detection by the financial institution, a third-party report, or report filed by the consumer victim. Tracking the method of detection should help avoid double-counting incidents in which reports were made to the lender as well as directly to law enforcement authorities.

This type of reporting also documents avoided incidents of identity theft. These include blocked charges that are automatically recognized as fraudulent, known failed attempts to hijack accounts, and rejections of fraudulent credit applications.

Synthetic identity theft should be tracked as well. Tracking this type of identity theft is more difficult because victims do not usually call to complain of fraudulent charges or accounts. Therefore, the institution itself must identify these cases. Placing the responsibility on the institution, however, does not answer the question of how the institution can or should go about making such identifications. Avivah Litan recently proposed a solution: she argues for a default classification system in which institutions classify all loans that are late by 180 days as identity theft, rather than write them off as bad credit losses.[71] That is, unless there is evidence to the contrary, institutions should treat late accounts as identity theft incidents: "[s]uch 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."[72]

Unfortunately, Litan's solution is probably both over-inclusive and under-inclusive. On one hand, it may incorrectly classify certain bad credit losses — accounts opened by ordinary deadbeats — as syn-

---

lating agencies could then determine whether certain red flags are more likely to be associated with identity theft than others, and adjust the duty to mitigate risk accordingly.

71. AVIVAH LITAN, GARTNER, INC., REDUCE IDENTITY THEFT BY RECTIFYING TOO-EASY CREDIT ISSUANCE 2 (2003), *available at* http://www.gartner.com/resources/117100/117132/117132.pdf.

72. *Id.*

thetic identity theft. On the other hand, Litan's solution will fail to detect actual cases of ongoing synthetic identity theft. In particular, synthetic identity thieves who pay the minimum amount on their accounts will appear to be classified as legitimate customers.[73]

Effective reporting will require financial institutions to perform more thorough investigations to distinguish between ordinary borrowers and those who never intended to pay the full bill. For instance, the lender could use a verification service[74] to confirm that the SSN provided in the application matches the identity of the person who holds the account, call the phone numbers provided by the applicant to determine whether they belong to accountholder, and review the applicant's credit report for signs of fraud, such as a high volume of new credit applications. Nevertheless, Litan's approach may be the most effective for ensuring that synthetic identity theft is not misclassified as bad debt.

Second, institutions should disclose the forms of identity theft attempted and the products or types of financial service targeted by the thief ("targeted product"). This requirement will facilitate categorization of the crime. At the most general level, institutions could identify two types of fraud — new account fraud and account takeover. As we learn more about identity theft, and as the crime evolves, reporting upon the form of identity theft could expand to include more categories. For instance, institutions could begin to report suspected "friendly" or "familiar" fraud, which occurs when the accountholder permitted another to use his account but then reports the charge as fraudulent.[75] Institutions would be free to recognize such variations on the two dominant categories and report them voluntarily. For this information to be meaningful, however, regulators must develop a standard set of definitions to describe categories of identity theft and institutions must use those definitions when classifying and reporting crimes. Regulators should not only define common forms of identity theft, but also continually adapt and add categories to account for the evolving nature of the crime. Standard definitions, accompanied by instructions on how institutions should apply them, would promote uniformity and allow meaningful comparisons of fraud rates over time.

This form of reporting will also provide data on the targeted product, such as a new or existing credit card, an in-store offer of credit, a mortgage loan, or the use of "convenience checks." Part VI

---

73. In at least one case, identity thieves made the minimum payments on the accounts so that the credit cards would continue to be active. *See DOJ Charges Three California Men in $1.4 Million Credit Card Fraud*, 2 Privacy & Security L. Rep. (BNA) 357 (Apr. 7, 2003).

74. *See, e.g.*, Employer W-2 Filing Instructions & Information – Social Security Number Verification, http://www.ssa.gov/employer/ssnv.htm (last visited Dec. 1, 2007) (describing a free SSN verification service for wage reporting purposes only).

75. *See* ITRC, *supra* note 5, at 21.

explains how identifying the targeted product will help tailor preventive measures to the types of financial products that present the most risk.

Third, institutions should report the amount of loss suffered or avoided. If, for example, a consumer identifies $100 in fraudulent charges, the institution should report that amount. Likewise, in synthetic identity theft situations, the institution should report the actual losses from the theft. In the case of avoided losses, institutions could report the amount of an attempted charge, or, in the case of new accounts, institutions could report the maximum credit line for which the applicant would have been eligible.

B. Who Should Report and to Whom

As discussed above, financial institutions are the appropriate entity to report identity theft, because they themselves are victims of identity theft and have the most information about the crime.[76] The lender has the most contact with the impostor, and has possession of not only the fraudulent credit application, but also any supporting identification information, the transaction history of the account, and the address left by the impostor to which the account documentation and card were sent. No other participant, except for the criminal himself, has as much information about the crime. Together, these factors make the financial institution the most appropriate reporting entity.

A possible alternative to the reporting requirements for financial institutions would be to require consumer reporting agencies[77] to disclose the figures. This is a suboptimal solution: consumer reporting agencies do not always learn of identity theft, especially in account takeover situations, because victims typically do not inform a credit reporting agency of credit card fraud.[78] Even with new account fraud,

---

76. Reporting duties are often further complicated because modern financial services companies engage in sophisticated marketing relationships through affinity cards and joint marketing agreements with other companies. For instance, a college may offer its alumni an affinity credit card issued by a partner bank. *See, e.g.*, Harvard Alumni Assoc., Harvard World MasterCard, https://www.juniper.com/app/japply/lp/20046.jsp (last visited Dec. 1, 2007) (offering the Harvard Card, which is sponsored by the Harvard Alumni Association and issued by Barclays Bank Delaware). Or, a department store may offer a discount on purchases in exchange for a customer's enrollment in a store credit card. *See, e.g.*, Macy's — Apply Now, https://www.macys.com/service/credit/applynow/index.ognc (last visited Dec. 1, 2007) (offering a 10% sign-up discount for newly approved holders of the Macy's card). In such cases, the reporting entity should be the financial institution, not the affinity entity or the department store, because it is the organization that is actually extending credit.

77. A consumer reporting agency includes any person, organization or agency that "regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties." 15 U.S.C. 1681a (2000).

78. SYNOVATE, *supra* note 7, at 9.

a significant number of victims never file fraud alerts[79] or inform the consumer reporting agency of the crime.[80]

The data compiled by financial institutions should be regularly reported to a financial regulator, such as the Federal Financial Institutions Examination Council ("FFIEC").[81] Since financial institutions already file regular reports containing other data on financial stability with the FFIEC, this agency is a natural choice for aggregating this related information.[82] This basic reporting requirement will enable the FFIEC and other federal regulators to request more information if they detect new or suspicious trends.

Because this proposal only calls for disclosure of incident-level data that do not include any specific details about the methods of attack or tactics used by criminals to commit identity theft, the information provided to the FFIEC could be shared with the public. For example, it could be posted on the FFIEC website.[83] Arguably, it is not critical for individual consumers to check this website regularly, as long as the information is accessible to the press, which can then convey it to the general public.

Ideally, the interface for accessing the data would allow users to view the information by individual institution, rather than by the industry in the aggregate. Further, the statistics should identify the general physical location and medium by which the attempted fraud took place. Finally, the data analysis for each lender should compute the crime rates and risks in terms of the lender's number of customers, number of accounts, and market capitalization.[84]

V. THE CHALLENGES OF THE REPORTING APPROACH

Several challenges, some political and some practical, are associated with this proposal.

---

79. A fraud alert is a notation a consumer can have placed on his credit report. When a business sees a fraud alert on a consumer's credit report, it must verify the consumer's identity before issuing any credit. *See* FTC, Identity Theft Victims: Immediate Steps, http://www.consumer.gov/idtheft/con_steps.htm (last visited Dec. 1, 2007).

80. SYNOVATE, *supra* note 7, at 9.

81. *See* FFIEC Home Page, http://www.ffiec.gov (last visited Dec. 1, 2007) ("The Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by [financial regulators].").

82. *See, e.g.*, FFIEC Forms, http://www.ffiec.gov/ffiec_report_forms.htm (last visited Dec. 1, 2007).

83. The FFIEC website currently makes a wealth of financial information reported by banks available to the public. *See, e.g.*, FFIEC Reports, http://www.ffiec.gov/reports.htm (last visited Dec. 1, 2007).

84. Chris Walsh proposes that banks keep anonymized, case-specific information so that studies may be conducted about particular identity theft incidents. E-mail from Chris Walsh, Info. Security Practitioner, to Chris Jay Hoofnagle (Feb. 20, 2007, 06:27:38 CST) (on file with author).

A. Institutions Themselves Are Not Always Aware of Identity Theft

The proposed reporting solution is complicated by a measurement problem. Many institutions cannot always verify when identity theft has occurred. For instance, accounts used by identity thieves typically go unpaid and eventually become delinquent.[85] However, institutions cannot always determine whether delinquent accounts are the result of an inability to pay or fraudulent activity. 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.[86]

The detection that does occur may be delayed until the institution engages in its regular accounting, which for businesses may mean until the end of a reporting quarter.[87]

While these limitations on detection affect this proposal, all measurement systems are imperfect. Even if detection of fraudulent accounts is delayed by weeks or months, regular reporting will still produce a timely review of the performance of financial institutions. The lack of regular reporting increases reliance on other, less accurate methods; in comparison to existing alternatives, even flawed reporting by financial institutions would be preferable to no reporting at all.

B. Reporting Could Enable Fraud

Arguably, by publishing statistics that identify which products are most vulnerable to identity theft, the proposed reporting requirements provide a roadmap for criminals.[88] According to this hypothesis, thieves may adopt certain methods or target certain products based on publicly available data that identify vulnerabilities. The concern is that thieves will target certain types of accounts, such as convenience

85. Cook, *supra* note 17, at 24.

86. Press Release, Gartner, Inc., Gartner Says Identity Theft Is Up Nearly 80 Percent (July 21, 2003), http://www.gartner.com/5_about/press_releases/pr21july2003a.jsp.

87. Collins & Hoffman, *supra* note 63, at 4.

88. *See, e.g.*, Betty Joyce Nash, *Identity Theft*, REGION FOCUS, Winter 2006, at 43.

checks or pre-approved offers of credit, because, statistically, these products will appear easier or less costly to exploit, or because the associated risk of prosecution is low. Alternatively, publicly-available statistics on identity theft could lead criminals to target products with lower fraud rates, in the hope that security efforts will be focused on higher-risk products.

This argument, however, ignores the reality that such a roadmap already exists. Methods of identity theft are well known and available to even unsophisticated criminals,[89] as evidenced by the prevalence of the crime and the magnitude of the resulting economic loss. Furthermore, the reporting requirements described in this Article are unlikely to disclose any specific information on victims, tactics, methods or vulnerabilities. The statistics that would become publicly available if this Article's proposal were adopted would be similar to existing data sets on other types of crime, such as the FBI's Uniform Crime Reports[90] or the Bureau of Justice Statistics' National Crime Victimization Survey.[91] No one could plausibly argue that the public availability of these studies causes more violent crime. Such reporting does not provide instructions on how to commit crimes; it merely informs the public that the crimes occurred and enables academics and policymakers to recognize and study trends in crime. The type of identity theft reporting advocated in this Article similarly focuses more on the incidence of crime, rather than on methods of committing it. It is unlikely to help criminals any more than ordinary newspaper reporting on identity theft.

Proponents of restricting access to information about identity theft believe that greater security can be attained through obscurity. In this view, hiding vulnerabilities about the credit system will make it more difficult for thieves to engage in identity theft. However, this argument overlooks the possibility that obscuring vulnerabilities may weaken the integrity of the system. As Professor Peter Swire explains, secrecy may complement or enhance security in situations where someone attacks a physical facility in person or attempts to hack a computer for the first time.[92] However, obscurity may harm security in situations where attackers can attempt to break into a system multiple times because there is minimal likelihood of being caught, learning from each unsuccessful event in the process.[93] Such is the case

89. *See infra* Part VI.D.

90. FBI, U.S. DEP'T OF JUSTICE, UNIFORM CRIME REPORTS: CRIME IN THE UNITED STATES, *available at* http://www.fbi.gov/ucr/ucr.htm (summarizing annual crime statistics obtained from law enforcement agencies across the United States).

91. BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE, CRIME AND VICTIMS STATISTICS, *available at* http://www.ojp.usdoj.gov/bjs/cvict.htm (summarizing data on crimes obtained from surveys of households in the United States).

92. *See* Peter P. Swire, *A Model for When Disclosure Helps Security: What is Different About Computer and Network Security?*, 3 J. TELECOMM. & HIGH TECH. L. 163 (2004).

93. *Id*. at 176–86.

with identity theft — the would-be identity thief can attempt to compromise an account multiple times. Identity thieves also have the advantage that their attacks need not occur in person. The opportunity to engage in repeated and remote attacks enables malicious actors to learn the very secrets that supposedly protect the system, while leaving the public and regulators in the dark.

C. Reporting Will Pit Financial Institutions Against Victims

In response to this Article's proposal, Professor Daniel Solove has argued that requiring financial institutions to report information about identity theft will create perverse incentives: institutions will become less accepting of victim's claims in an effort to make their identity theft rates appear lower.[94] In his view, the proposal will harm consumers by effectively making the victims pay for the fraudulent charges made by others.[95]

Solove's objection is a serious one. Stronger disincentives to bad faith denials of claims may have to be established to complement existing competitive pressures. One possible remedy, borrowed from the insurance industry, would allow a wronged victim to collect damages if the lender rejects a dispute of a fraudulent charge without justification.

Another remedy would be to require financial institutions to identify all situations in which the victim challenged a charge as fraudulent. If the lender suspects that the "victim" authorized the charges, the institution can report the incidents as familiar fraud to distinguish them from cases in which identity theft is clearly present. While financial institutions may still be tempted to distort their statistics and report most identity theft as familiar fraud, more extensive reporting requirements will tend to tighten the system, making it progressively more difficult to cook the books.

Solove's argument also undervalues the power of competition to combat the problem of fraudulent claim denial. If a certain institution develops a reputation for challenging good faith fraud claims, it could lose customers to other lenders that are more solicitous to victims.[96]

---

94. Telephone Conversation with Daniel Solove, Assoc. Professor of Law, George Washington Univ. Law Sch. (Feb. 6, 2007).

95. *Id.*

96. The wireless phone industry is an illustrative case study in the importance of customer satisfaction. When mobile number portability allowed customers to switch their cell phone providers without losing their telephone number, companies with the lowest levels of customer satisfaction saw a significant fall in subscribers. *See* Bruce Meyerson, *Number Portability Hurting AT&T Wireless*, CHI. SUN-TIMES, Apr. 1, 2004, at 71.

D. The Market Will Solve the Identity Theft Problem

Whether the market can successfully address identity theft largely depends on the known unknowns of the crime. Without reporting, we cannot know whether the market is successfully combating the crime. Reporting will elucidate the scope of the problem and its trends and, as explained in Part VI.D, create a more efficient market for identity theft prevention.

Some have argued that lenders are already working to minimize identity theft and do not need additional incentives.[97] In this view, the simple economics of the crime already provide an adequate incentive: because such fraud harms the lender's bottom line, a reduction in the incidence of the crime would result in greater profits. Accordingly, reporting simply adds another costly and unnecessary regulatory burden on financial institutions that are already addressing the problem through profit-driven competition. Moreover, those opposed to this proposal could point out that protection of consumers does not justify burdening financial institutions with a reporting requirement because consumers generally do not bear the costs of identity theft; instead, most costs are borne by other parties to the transaction.[98] Arguably, the cost to consumers is especially small in the context of synthetic identity theft because the person whose information was used may never learn of the crime.

However, as estimates of the prevalence and severity of identity theft suggest, it is plain that the market has thus far failed to address the problem. The rise of synthetic identity theft indicates that financial institutions are not authenticating the identities of credit applicants. Instead, it appears that financial institutions are only authenticating the SSN by comparing it to the date of birth, rather than ensuring that the number is issued to the correct person. This means that lenders are not using all the tools available to them to prevent identity theft — simply matching the name of the applicant to the SSN would in many cases make this type of fraud impossible.

The current verification practices used by financial institutions have serious public policy implications. Financial institutions oppose overly restrictive privacy legislation, arguing that more extensive privacy rights will limit the ability of businesses to use personal information and thus undermine fraud prevention efforts.[99] Their position fails

---

97. *See, e.g.*, Brad Stone, *To Fight Identity Theft, a Call for Banks to Disclose All Incidents*, N.Y. TIMES, Mar. 21, 2007, at C3, *available at* http://www.nytimes.com/2007/03/21/business/21identity.html.

98. SYNOVATE, *supra* note 7, at 6.

99. *See* Hjalma Johnson, President, Am. Bankers Ass'n, Remarks Before the ABA Community Bankers Council, Banking and the Future of Financial Privacy: A Commitment to Our Customers (Nov. 15, 1999), *available at* http://www.aba.com/NR/rdonlyres/80468413-4225-11D4-AAE6-00508B95258D/46417/HJSpeech111599.pdf; s*ee also* Am.

to recognize that lenders are not currently taking advantage of the information that is available to them and could be used to combat identity theft.

In addition, while lenders can bear the economic losses of identity theft, they can also pass off the costs of the crime to others. First, financial institutions share the costs with consumers directly through lost time, inconvenience, and out-of-pocket costs.[100] They also share the costs indirectly through higher fees.[101] Second, a largely overlooked way in which financial institutions share the costs of identity theft with third parties is by writing off their losses when computing their corporate income taxes.[102] Accordingly, the burden of identity theft is tax-subsidized: it is deducted from earned income like any ordinary business expense. If identity theft struck more directly at the bottom line, institutions would be more likely to take precautions against the crime.

VI. THE BENEFITS OF THE REPORTING APPROACH

This Article argues that the number and magnitude of the benefits associated with the reporting proposal outweigh any difficulties or disadvantages associated with its implementation. These benefits can help in the fight against identity theft.

A. Reporting Will Identify the Most Vulnerable Practices

Reporting will enable financial institutions, regulators, and the public to identify the financial practices most vulnerable to identity theft. It may be the case that some financial products, such as instant credit lines that can be obtained online in minutes, are far more likely to be the target of fraud than products that generally require more due diligence, such as mortgage loans. If the data show that different practices have different vulnerabilities, preventive measures can be tailored to the level of risk associated with different products. For instance, if data indicated that instant credit lines were vulnerable, regulators could require lenders to collect more personal information for instant credit applications or cap the amount of money that can be

---

Bankers Ass'n, Industry Issues: The Devastating Effect of Opt-In Restrictions, http://www.aba.com/Industry+Issues/GR_PR_Opt-in.htm (last visited Dec. 1, 2007) (discussing the dangers of mandatory opt-in restrictions as a privacy default).

100. *See supra* note 29 and accompanying text. Furthermore, FTC found that the average victim spent $500 of his own money and 30 hours of time dealing with the consequences of identity theft. SYNOVATE, *supra* note 7, at 6.

101. Fees for financial products have continued to rise. FED. RESERVE, ANNUAL REPORT TO THE CONGRESS ON RETAIL FEES AND SERVICES OF DEPOSITORY INSTITUTIONS 8 (2003), *available at* http://www.federalreserve.gov/boarddocs/rptcongress/2003fees.pdf. Perhaps, if identity theft rates were reduced, these fees would be lower.

102. I.R.C. § 165 (2000).

lent on a new account until the account holder has established a specified payment history.

B. Reporting Will Provide Metrics for Interventions

Reporting will help all parties decide whether existing preventive measures are appropriate, overly burdensome, or in need of enhancement. For instance, since 1997, California lenders of in-store instant credit have been required to collect at least three types of personal information from the applicant and match them with information obtained from a consumer reporting agency before authorizing a new account.[103] The purpose of this provision is to minimize the likelihood of identity theft by requiring retailers to properly identify new customers.[104] But, has this provision been effective? Are three identifiers enough, or should more be collected? Reports on the number of fraud attempts and the results of those attempts would make it possible to compare statistics across multiple states and, thus, determine whether this regulation improves security.

The data reported may also indicate that certain practices are so vulnerable to identity theft that they should be discontinued. For instance, lenders send replacement credit cards to addresses that are not current.[105] They also send unsolicited convenience checks.[106] Even unsophisticated thieves can obtain these offers from the victim's mail and use them.[107] Customer consent should be required for the prac-

---

103. CAL. CIV. CODE § 1785.14(a)(1) (West 2007).

104. *See* S. RULES COMM., 1997–1998 REGULAR SESSION, BILL ANALYSIS, AB 156 (Cal. Sept. 2, 1997), *available at* http://info.sen.ca.gov/pub/97-98/bill/asm/ab_0151-0200/ab_156_cfa_19970902_160944_sen_floor.html (author statement in support of bill).

105. *See* Lucy Lazarony, *Old Address + New Credit Card = Danger*, BANKRATE.COM, June 2, 2003, http://www.bankrate.com/brm/news/cc/20010831a.asp.

106. *See* IOWA DEP'T. OF JUSTICE, HOW TO AVOID IDENTITY THEFT § 10 (1998), *available at* http://www.state.ia.us/government/ag/consumer/brochures/avoid_identitytheft2.html.

107. 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 sent it to the new address, thus demonstrating that a thief could easily use even a torn-up offer to commit fraud. The Red Tape Chronicles, *Even Torn-Up Credit Card Applications Aren't Safe*, http://redtape.msnbc.com/2006/03/what_if_a_despe.html (Mar. 14, 2007, 07:00 CST). In another case, Chase Manhattan bank issued a Platinum MasterCard to "Clifford J. Dawg." The owner of a dog had signed up for a free e-mail account in his pet's name and later received a pre-approved credit offer for a Clifford J. Dawg. The owner found this humorous and responded to the offer, listing nine zeros for the dog's SSN, the "Pupperoni Factory" as employer, and "Pugsy Malone" as the mother's maiden name. The owner also wrote on the form: "You are sending an application to a dog! Ha ha ha." The card arrived three weeks later. *Dog Issued Credit Card, Owner Sends In Pre-Approved Application As Joke*, NBCSANDIEGO.COM, Jan. 28, 2004, http://www.nbcsandiego.com/money/2800173/detail.html; *Easy, Fast Credit Available to All Comers*, FOXNEWS.COM, Jan. 29, 2004, http://www.foxnews.com/story/0,2933,109771,00.html.

tices determined to be too susceptible to fraud or to transfer too much risk to the customer.[108]

Unfortunately, interested parties — policymakers, financial institutions, and consumers — lack the tools for conducting a meaningful cost-benefit analysis of current, proposed, or nonexistent regulatory measures. Reporting is the best method for acquiring the data needed to make smart decisions.

C. Reporting Will Focus Public Attention on the Real Problem

Identity theft is a high-stakes issue in the world of public policy. It is a popular talking point for political candidates, who have proposed many laws with serious implications for financial institutions.[109] Financial institutions, therefore, seek ways to reduce the regulatory attention focused on their industry because of identity theft.

One industry tactic is to distribute "press release" surveys created using questionable methods.[110] Javelin Research releases many such surveys, including industry-sponsored polls of victims, which assert that identity theft is declining.[111] Yet Javelin's polls do not reflect synthetic identity theft.[112] However, to the extent that policymakers find this research convincing, it may protect the study's sponsors (i.e., Visa) from unwanted regulatory measures.

Contrary to conclusions in the existing literature,[113] Javelin Research also makes the bold claim that most identity theft is committed by friends or family members of the victim.[114] This argument could be read to imply that the victim is somehow at fault for not protecting his

---

108. Similar restrictions for other types of unsolicited mailings already exist. *See, e.g.*, Consumer & Governmental Affairs Bureau, FCC, Fax Advertising: What You Need to Know, http://www.fcc.gov/cgb/consumerfacts/unwantedfaxes.html (last visited Dec. 1, 2007) (summarizing the statutory prohibition on unsolicited fax advertising).

109. *See, e.g.*, Press Release, Nat'l Conf. of State Legislatures, NCSL's Top 10 Policy Issue Forecast: Heat Is on State Legislatures (Jan. 4, 2007), http://www.ncsl.org/programs/press/pr070104.htm (noting that the public's concerns about security breaches and identity theft are resulting in states debating and enacting laws to protect privacy).

110. For an in-depth discussion of the "market" for policy research, see generally Oscar H. Gandy, Jr., *The Role of Theory in the Policy Process*, *in* TOWARD AN INFORMATION BILL OF RIGHTS AND RESPONSIBILITIES 99 (Charles M. Firestone & Jorge Reina Schement eds., 1995).

111. *See* KIM, *supra* note 41, at 1.

112. *See supra* note 41. For an in-depth explanation of this point, see Brown Study Blog, *Javelin's Bogus Analysis, supra* note 8.

113. *See* FDIC REPORT, *supra* note 15, at 10 ("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."); GORDON ET AL., *supra* note 67, at 53–54 (finding that in of all cases for which the source of stolen personal information could be determined, 50% were stolen from a business, and 15% were stolen from a friend or family member).

114. *See* KIM, *supra* note 41, at 6–12; JOHANNES, *supra* note 38, at 27–31; JAVELIN STRATEGY & RESEARCH INC., 2005 IDENTITY FRAUD SURVEY REPORT 6–8 (Mary T. Van Dyke ed., 2005) (on file with the *Harvard Journal of Law & Technology*).

personal or financial information from friends and family members.[115] Such reasoning shifts the responsibility for identity theft away from the institution and onto the consumer. If such tactics are successful, policymakers may focus less on the role of the financial institution in identity theft, and instead allocate resources to educate individuals about information security in an effort to make it more difficult for friends and family to steal victims' identities.

Moreover, the assertion that victims of identity theft are closely connected to the perpetrator relies upon shaky assumptions. Javelin's conclusion is based on the survey responses of a very small subset of the victims who knew the identity of the perpetrator, and these responses are generalized to the rest of the respondents who did not.[116] For this approach to be valid, the small subset would have to be sufficiently similar to the larger sample, which Javelin failed to demonstrate.[117] Recognizing the flaws of the Javelin study, FTC has characterized the conclusion that impostors are most often friends or relatives of victims as misleading.[118]

Better reporting will provide more reliable information to the public and will demonstrate whether regulatory measures are justified. By providing an alternative to the specious "press release" surveys, reporting may lessen the effect of these surveys on the policy debate. In this way, this Article's proposal will help focus public attention on the real causes of identity theft.

D. A More Competitive Market for Protecting Consumers Will Arise

Few would deny that identity theft is currently an easy crime to commit.[119] Most identity theft occurs offline and does not require sophisticated computer cracking skills.[120] Thieves are able to obtain credit using fabricated, entirely dissimilar names.[121] A surprising amount of identity theft is committed by street-level criminals, sometimes in the throes of methamphetamine binges.[122] Citing the facts of

---

115. *See* Statement of Chris Jay Hoofnagle, Senior Counsel, Elec. Privacy Info. Ctr., to Maryland Attorney General Identity Theft Forum (Nov. 21, 2005), *available at* http://epic.org/privacy/idtheft/mdstate11.21.05.html.

116. For instance, in Javelin's 2007 survey, only 144 of the 469 victims knew who stole their identity. KIM, *supra* note 41, at 3, 13.

117. *See* Brown Study Blog, *Javelin's Bogus Analysis*, *supra* note 8.

118. E-mail from Claudia Bourne Farrell, Office of Pub. Affairs, FTC, to Robin Sidel, Correspondent, Wall St. Journal (Oct. 20, 2005 11:16 EST), *available at* http://chrishoofnagle.com/blog/wp-content/uploads/2007/02/ftc_email_on_javelin.pdf.

119. Collins & Hoffman, *supra* note 63, at 9.

120. Press Release, Better Business Bureau, New Research Shows that Identity Theft Is More Prevalent Offline with Paper than Online (Jan. 26, 2005), *available at* http://www.bbb.org/alerts/article.asp?ID=565.

121. *See supra* Part II.A.

122. John Leland, *Stolen Lives, Meth Users, Attuned to Detail, Add Another Habit: ID Theft*, N.Y. TIMES, July 11, 2006, at A1, *available at* http://www.nytimes.com/2006/07/

recent identity theft cases, some analysts have suggested that lenders are not screening any credit applications for fraud.[123]

Consumers cannot protect themselves from becoming victims of identity theft for several reasons. First, financial institutions do not help consumers make informed decisions regarding the security of their identities. There is virtually no information available on the relative risk of fraud among financial institutions, and the little information that does exist is only marginally helpful.[124] Second, lax lending standards also contribute to identity theft; it is far from clear that lenders successfully screen applications for fraud. The reporting requirements proposed in this Article will inform consumer decisions and help address these problems. Statistics showing the relative risks of fraud for each institution will enable consumers to make meaningful distinctions in the marketplace.

Even though policy debates frequently ignore the role of the financial institution in identity theft,[125] the frequent failure of existing lending practices to detect suspicious activity[126] suggests that market-

---

11/us/11meth.html. Furthermore, in a 2004 study, the Michigan State University Identity Theft Crime and Research Lab found that 15% of the 1,037 perpetrators it surveyed were linked to drug crimes. The study reported that the use of stolen identities for the production, sale, and support of methamphetamine habits is epidemic. Collins & Hoffman, *supra* note 63, at 15.

123. *See, e.g.*, Press Release, Gartner, *supra* note 86, at 1 ("[B]anks and [financial service providers] must implement solutions that effectively screen for application fraud, so they don't wrongfully extend credit to identify thieves.").

124. *See, e.g.*, JAMES E. VAN DYKE, JAVELIN STRATEGY & RESEARCH INC., BANKING IDENTITY SAFETY SCORECARD (Mary T. Monahan ed., 2006).

125. *See* Chris Jay Hoofnagle, *Putting Identity Theft on Ice: Freezing Credit Reports to Prevent Lending to Impostors*, *in* SECURING PRIVACY IN THE INTERNET AGE (Anupam Chander et al. eds., Stanford Univ. Press, forthcoming 2007), *available at* http://ssrn.com/abstract=650162.

126. A victim's response to ITRC's 2003 survey illustrates this problem:

> [T]he 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.

ITRC, *supra* note 5, at 42. The facts of numerous cases suggest poor identity authentication practices in credit granting. *See, e.g.*, Nelski v. Pelland, 86 F. App'x 840 (6th Cir. 2004) (stating that phone company issued credit to impostor using victim's name but slightly different SSN); United States v. Peyton, 353 F.3d 1080 (9th Cir. 2003) (stating that impostors obtained six American Express cards using correct name and SSN but directed all six to be sent to the impostors' home); Aylward v. Fleet Bank, 122 F.3d 616 (8th Cir. 1997) (stating that bank issued two credit cards based on matching name and SSN but incorrect address); Farley v. Williams, No. 02-CV-0667C(SR), 2005 U.S. Dist. LEXIS 38924, at *1 (W.D.N.Y. Dec. 30, 2005) (stating that two accounts were opened with victim's name and SSN but incorrect address); Vazquez-Garcia v. Trans Union de P.R., 222 F. Supp. 2d 150, 153 (D.P.R. 2002) (stating that impostor successfully obtained credit with matching SSN but incorrect date of birth and address); Dimezza v. First USA Bank, Inc., 103 F. Supp. 2d 1296 (D.N.M. 2000) (stating that impostor obtained credit with SSN match but incorrect address). In one case, a court allowed a negligence claim against a lending institution for poor authentication procedures. Wolfe v. MBNA Am. Bank, 485 F. Supp. 2d 874 (W.D.

based incentives, in conjunction with regulatory controls, could help control the problem. Specifically, reporting would enable financial institutions to establish themselves as leaders in the fight against identity theft.

VII. CONCLUSION

Identity theft is believed to be the fastest growing white collar crime.[127] Yet the public and policymakers have limited information about the scope, forms, and severity of identity theft. The lack of information prevents stakeholders from gauging the seriousness of the crime and responding appropriately. Misperceptions about identity theft have endured because measurements of the crime have relied on public surveys of its victims; such surveys are often sponsored by financial institutions. This method is both under- and over-inclusive in measuring the incidence of identity theft.

This Article proposes an alternative solution and argues that financial institutions, the entities with the most information about identity theft, should be required to publicly report data about the crime. To make the known unknowns of identity theft known, financial institutions should report information on: (1) the number of identity theft incidents suffered or avoided; (2) the forms of identity theft attempted and the financial products targeted; and (3) the amount of loss suffered or avoided. Such reporting will considerably improve our understanding of identity theft and enable policymakers to tailor preventive measures to the severity and methods of the crime.

More importantly, such reporting will create a market for identity theft prevention. Financial institutions will then have incentives to offer the safest products. The resulting competition will make consumers' personal information safer, and allow consumers to make informed choices among institutions based on their preference for risk.

Tenn. 2007) (permitting negligence claim against defendant bank to continue under Tennessee law where a fraudulent credit application was accepted despite having a false address, phone number, and mother's maiden name). *But cf.* Huggins v. Citibank, N.A., 585 S.E.2d 275 (S.C. 2003) (denying negligence claim against defendant bank for negligent enablement of identity fraud because no duty existed between bank and plaintiff, a non-customer).

127. FTC REPORT, *supra* note 3, at 1.