CYBER-IDENTITY THEFT: A CONCEPTUAL MODEL AND IMPLICATIONS FOR PUBLIC POLICY

Angeline Grace Close
North Georgia College and State University /
University of Georgia
Terry College of Business
124 Brooks Hall
Athens, GA 30602
(706) 542-3764 (P)
(706) 542- 3738 (F)
aclose@terry.uga.edu

George M. Zinkhan
University of Georgia
Terry College of Business
124 Brooks Hall
Athens, GA 30602
(706) 542-3764 (P)
(706) 542- 3738 (F)
aclose@terry.uga.edu

R. Zachary Finney
North Georgia College and State University
Newton Oakes Center
Dahlonega, GA 30507
rzfinney@ngcsu.edu

The authors thank the five anonymous reviewers for their insights.

CYBER-IDENTITY THEFT: A CONCEPTUAL MODEL AND IMPLICATIONS FOR PUBLIC POLICY

ABSTRACT

This research sets a conceptual base for further empirical work on *cyber-identity theft*, or identity theft associated with the Internet. To do this, we introduce three classification schemes: 1) methods used by the thieves, 2) time frame of the theft, and 3) behavioral responses by victims. Together, these schemes synthesize and illustrate major problems in hopes of increasing awareness regarding the reality of cyber-identity theft. Our schemes purport to stimulate empirical work done on the increasing public policy and consumer welfare issues embedded by the Internet and its key role in identity theft.

CYBER-IDENTITY THEFT: A CONCEPTUAL MODEL AND IMPLICATIONS FOR PUBLIC POLICY

> A man was arrested in Greenwood, Ind., putting a halt to his identity-theft business. He was caught because, three times in a three-day period, he aroused suspicion by approaching a certain ATM on foot, carrying a motorcycle helmet, donning the helmet as he neared the ATM's camera, making a withdrawal (with someone else's ID), walking away, and then removing the helmet. [WISH-TV (Indianapolis), 8-5-03]

As can be seen by the news blurb above, some individuals have attempted (with varying degrees of success) to enter the identity theft "business". Yet, many identity thieves are not as inept as the helmet-donning identity thief mentioned above; identity thieves are often inconspicuous- *especially* those thieves who use the Internet in hopes of victimizing consumers. Identity thieves increasingly hide behind computers and other forms of electronic exchange. "In this era of faceless business transactions enabled by information technology (IT), identity can no longer be taken for granted as a fundamental physical characteristic. Rather, identity has become a database entity that can be disconnected from physical recognition – even bought and sold as a commodity – and as such is subject to easy theft and widespread misuse." (Thompson 2002, p. 64).

Identity theft is the most common classification of consumer complaints; approximately 42 percent of all complaints to the FTC report identity theft (www.consumer.gov/idtheft). The complaints often total the amount of *financial* losses incurred, yet, the costs of victimization are

beyond monetary repair. For instance, in order to eliminate $17,000 of fraudulent charges from one's credit history, victims typically part with over $800, 175 hours of lost productivity, and up to four years in their "normal lives" (Burnett 2003). It is not a surprise that identity theft is a growing problem, and, to some extent, this problem can be attributed to the emergence of the electronic marketplace. As Internet usage continues to increase, the use of the Internet an identity theft vehicle will increase proportionally (Saliba 2000). Identity theft is becoming more common, more costly, and more sophisticated- mainly due to the Internet. And at present, identity theft is the top *online* fraud (FBI 2003). Given this situation, re-appraisals of both research and public policy are needed.

We define cyber-identity theft as the *online or electronic acquisition of personal information with the purpose of utilizing such information for deceitful activity either on the Internet or offline*. In other words, cyber-identity theft is using electronic (i.e., web-based) means to carry out any form of identity theft. We focus on cyber-identity theft (i.e., e-identity theft); however, many issues discussed may be relevant to on-ground identity theft as well.

Research Objectives

In light of the need for further academic research on the Internet and the risk of identity theft, we set a conceptual groundwork, which combines consumer issues surrounding the Internet and identity theft. Two distinct objectives guide the current study: 1) to introduce three classification schemes for further empirical study, which synthesize conceptualizations of identity theft and the Internet. Together, these schemes provide an inventory of the main areas of

cyber-identity theft, by analyzing the following components of cyber-identity theft: a) methods, b) time-frame, and c) the behavioral responses by victims. Furthermore, we aim: 2) to recognize key issues and regulations related to public policy and consumer welfare.

CYBER-IDENTITY THEFT PROCESS

In the figure below, we show a basic model of the cyber-identity theft process. We likewise illustrate how we explicate these processes (e.g., through our various tables and figures). The cyber-identity theft process, on the simplest level, proceeds as follows: initially, the cyber thief selects the areas and the method of cyber identity theft (Table 1). Then, the identity theft actually occurs. Next, the cyber identity theft recurs, in some cases (Figure 2). Finally, the victim reacts to the cyber identity theft (Table 2). All along the way, public policy and consumer-welfare issues emerge from the cycle (as described in Table 3).

INSERT FIGURE 1 HERE

CYBER-IDENTITY THEFT SCHEMES

Regardless of the type(s) of information the thieves target, there are many methods for carrying out cyber-identity theft (Table 1).

INSERT TABLE 1 HERE

We briefly describe some of the methods of cyber-identity theft below.

a) Methods of Cyber-Identity Theft

Hacking. Hacking, or entering another's computer, is a common method of the cyber-identity thief. Saunders and Zucker (1999) note that the most common (cyber) identity theft tactic is to hack into a computerized database and take personal information. Hacking has evolved to "phishing".

Phishing. With phishing, identity thieves establish a fake web site designed to look like a company's actual site; unsuspecting customers are drawn to the site and asked to disclose personal information.

Employee Abuse. Employees, especially those employees who believe that they are treated unjustly, may provide the data necessary for cyber-identity theft. With email and databases full of consumer information, an employee or other insider can pass spreadsheets along to thieves. Employees may divulge personal information unintentionally, or intentionally. Also related to cyber-identity theft and the workplace, is the possibility of phony job-listings online in order to obtain consumer information (Sullivan 2003).

Mass Rebellion. Cyber-identity thieves may use decentralized, mass rebellion sites. These peer-to peer environments (e.g., Kazaa Media Desktop) allow individuals to share files over the Internet. Cyber-identity thieves may use such peer-to-peer networks to install virus software, which records data such as website visitation and any information that is entered to a non-secure site.

Disposal. Even disconnected computers may lead to cyber-identity theft. Careless handling or disposal of discarded computers can lead to identity theft. Furthermore, disposed

hardware and software may lead to cyber-identity theft. If a user fails to take precautions such as data deletion or physical destruction of a machine, the data are readily accessible for the next user- whoever may find it.

Pranking/Posing. Cyber-identity theft may also include seemingly "lighthearted" pranks- a less sinister form of identity theft. Such instances have occurred where the e-prankster registers (complete with photograph) a friend or colleague to an e-dating site (e.g., match.com) (Close and Zinkhan 2003). Phony e-dating profiles may be a result of an online prank, causing false expectations for interested e-daters. Posing as another on Instant Messenger (IM) is another prank where users misidentify themselves- often to obtain information not privy to the cyber-identity thief.

Spyware. Personal information is sometimes collected via spyware. Spyware is a group of programs that are (sometimes inadvertently) downloaded along with legitimate or free programs (e.g., Weatherbug, Gator). Spyware then runs in the background and functions whenever the Internet-user is online for market research purposes.

Scam Within a Scam. Our final mention of methods of cyber-identity theft involves a scam within a scam. For instance, a cyber thief may pose as an attorney or a governmental employee and mass email a database of past identity theft victims, requesting personal information for evidence to assist them in a potential court case. In this way, some theft victims may be victimized in more ways than one.

b) Time Frame of Cyber-Identity Theft

Time frame is an important construct to consider when understanding cyber-identity theft. Many may think of cyber-identity theft as a lengthy process, yet we note here that many

forms of identity theft are just one single transaction. Identity theft may have a short-term or long-term duration. That is, the security may range from a one-time theft, to a recurring theft, to an ongoing assumed impersonation (see Figure 2).

INSERT FIGURE 2 HERE

Time and the frequency of occurrence both are important constructs to consider. In an online environment, consumers may not be immediately aware that their identity has been compromised. The smaller-scale transactions (e.g., deducting five dollars) may repeat at intervals, in hopes of escaping the victim's attention. In contrast, in the off-line environment, a physical "event" (e.g., stolen wallet) may make the theft more apparent

c) Behavioral Responses to Cyber-Identity Theft

Consumer responses to cyber-identity theft may be psychological (e.g., feeling foolish, ignorant, naive) or behavioral (e.g., complaining, changing credit-card companies, altering purchase patterns). Here, we focus attention on the behavioral response – showing how consumer behavior may change, following an Internet-based identity theft (see Table 2).

INSERT TABLE 2 HERE

Online Behavioral Reponses. Victims' online behavioral changes may include: the extent of future personal information disclosure, selection/use of e-tailers, and the general nature of online shopping.

i) information disclosure online

After an Internet-related identity theft, the victim may significantly limit, or even cease the disclosure of personal information online. This behavior would be inconsistent with offline fraud victimization theory, which claims that some consumers are unable to distinguish legitimate transactions from illegitimate ones (AARP); similarly, Langendefer and Shimp (2001) find that fraud victims often cannot tell whether an offer is legitimate. When victims are not aware of cyber theft and its consequences, they may continue with the original behaviors that lead to their victimization. In a situation where the consequences of identity theft are severe (e.g., financial losses, hassles, or other setbacks), then behavioral change may be drastic, including:

ii) change in the selection/use of e-tailers;

iii) change in frequency/ extent of online transactions; or

iv) change in online shopping and purchasing behavior.

PUBLIC POLICY & CONSUMER WELFARE

Table 3 lists a group of public policy issues relating to cyber-identity theft.

INSERT TABLE 3 HERE

To date, one of the largest identity theft cases in U.S. history involves cyber-theft; a software employee affiliated with credit-reporting bureaus and accomplices e-copied over 30,000 credit records and sold them for $60 each, causing a minimum of $2.7 million in losses. “With a few keystrokes, these people were able to pick the pockets of millions of Americans.” (Delio qtd.

Comey 2002) Given the high stakes for cyber theft victims, one may question to what extent should companies be held responsible for unwarily employing a cyber-identity thief?

Another issue concerns the *types* of personal data that businesses may legally buy, sell and even post online. To what extent should the government regulate the proliferation of marketing databases and the uses of the databases? Since 1998, Congress has attempted to limit the manner in which financial institutions may use customer information (*Electronic Commerce News* 2003).

A further public policy issue concerns the *role that business should play* in helping identity theft victims recover their "good names." What role do businesses need to have in assisting cyber-identity theft victims? Critics allege that credit-reporting agencies contribute to identity theft through "liberal disclosure of credit reports" (Lee 2001). Moreover, consumer advocates allege that the poor service at credit-reporting agencies makes it exceedingly difficult for victims to clear their names. To support their argument, these critics point out that in the past, firms such as Equifax, Experian, and TransUnion have agreed to pay fines to the Federal Government due to poor customer service practices (ftc.gov).

Another set of public policy considerations arise from the *risks* associated with identity theft. Risk analysis and risk assessment programs should be addressed. How is the consumer to know the risk of giving a certain firm or individual (even employer or professor) personal information, such as a social security number? Where can the consumer turn to find a risk-assessment tool, either online or offline?

Similar considerations involve the *costs* associated with identity theft. Consumers should have access to a cost-assessment program or specialist to assist identity-theft victims in the legal process. As identity theft imposes multiple costs (e.g., social, financial, psychological), there should be a systematic way to assess and alleviate such costs. Such costs arise for both consumers and businesses. To some extent, the phenomenon of identity theft poses a threat to entire economic systems.

The roles of government need to be specified and effectively communicated to the public. For example, what is the role of the Office of Homeland Security? To what extent should the FTC be involved? What media (e.g., Internet, brochures) are best for implementing programs? How can cyber-identity theft instances be reduced in both scale and scope?

REGULATION

Regulatory matters are noteworthy for future study, as well. We discuss two responses to identity theft of note: The Identity Theft and Assumption Deterrence Act (a governmental act), and The Coalition on Online Identity Theft (a corporate-based group). First, the Federal Government has responded to this problem with *The Identity Theft and Assumption Deterrence Act (ITADA)* of 1998. *ITADA* has three major goals; specifically, the Act: 1) allows victims of identity theft to recover financial damages, 2) imposes criminal penalties of up to 15 years imprisonment and fines of up to $250,000 for those convicted of identity theft, and 3) directs the Federal Trade Commission to enforce the act (Saunders and Zucker 1999). Although the act

imposes criminal penalties of up to 15 years imprisonment and fines of up to $250,000 for those convicted, many consumer advocates believe that *ITADA* does not go far enough. Critics contend that, in drafting ITADA, lawmakers failed to realize that financial losses are often not the greatest losses incurred by a cyber-identity theft victim. Furthermore, it is questionable whether Congress has provided the FTC with the resources to enforce ITADA adequately.

A second response to the growing instances of Internet-related identity theft is the *Coalition on Online Identity Theft*. The group consists of e-tailers, online auctioneers, software companies, online security companies, and credit card providers. The coalition maintains three objectives: 1) expanding public education campaigns, promoting technology and tips for preventing and dealing with online theft, 2) documenting and sharing non-personal information about emerging online fraudulent activity to prevent future scams, and 3) working with the government to ensure effective enforcement of criminal penalties against cyber thieves (CIOL News 2003). Such is a noteworthy start of a community, which unites otherwise market competitors, against a greater societal and economic threat.

CONCLUSION

The rising incidence of cyber-identity theft is part of a broader change in the nature of human identity. A person's physical identity is now often entirely separate from many other forms of identity (Thompson 2002). Thus, consumers can harness the power of the Internet to multiply their identities on chat rooms, e-dating services, email, and other virtual spaces. And, should the user choose to do so, he or she may have a unique identity for each contact.

At the same time, organizations are trading information pertaining to individuals' purchasing habits and lifestyles. The era of CRM has lead to a greater emphasis on maintaining up-to-date, information on their target consumer. Hence, public policy makers have an arduous task ahead of them. First, authorities are attempting to regulate a moving (often international) target. The number of cyber-scams is limited only by the considerable imagination of the cyber-thieves. And, policy makers cannot count on technology to provide the means of catching cyber-crooks; as the government takes advantage of improved technologies to catch cyber thieves, the crooks use the same technology to invent improved schemes. Indeed, the "arms race" between the crooks and the regulators brings to mind the *Spy vs. Spy* cartoons in the old *Mad Magazine*: as one spy increases his deceit and artifice, so does the other. In the end, they are doomed to keep fighting, because neither spy can gain a meaningful victory.

In the end, all technology users must be mindful of the potential downside of going online. The costs to cyber identity theft victims are real; clearly, an ounce of prevention (not becoming a victim) beats a pound of cure (trying to regain one's "lost" identity). Researchers have an important role to play in suppressing cyber-identity theft in the future. It is hoped that this beginning conceptual piece will spark researchers to study identity theft and its relation to the Internet. In turn, we hope that such academic research will to lead to further attention to identity theft and to improved public policy both in the U.S. and abroad. By documenting the means employed by cyber crooks, the effects of such schemes on victims, and the public policy issues facing our society, we can begin to reclaim cyberspace as a means of enhancing and enriching (our own) human experiences.

REFERENCES

Burnett, Richard, (2003), "Identity Theft Victims Need Time, Money, Persistence to Clear Names," *Knight Ridder Tribune Business News,* August 20, 2003.

Close, Angeline G. and George M. Zinkhan (2003), "Romance and the Internet: The E-mergence of E-dating," *Advances in Consumer Research* (Vol. 30), Provo. UT: Association for Consumer Research (forthcoming).

Delio, Michelle (2002), "Cops Bust Massive ID Theft Ring," *Wired News*, November 25, http://www.wired.com/news/privacy/0,1848,56567,00.html, accessed: September 21, 2003.

Electronic Commerce News (2003), "Identity Theft Battle Moves to Congress," *Electronic Commerce News*, February 17, 2003, p. 1.

Federal Trade Commission (1999), *Prepared Statement of the FTC on Financial Identity Theft Before the Subcommittee on Telecommunications, Trade and Consumer Protection and the Subcommittee on Finance and Hazardous Materials of the Committee of Commerce*, http://www.ftc.gov/os/1999/04/identitythefttestimony.htm, accessed September 21, 2003.

Hemphill, Thomas A. (2001), "Identity Theft: A Cost of Business?" *Business and Society Review*, 106(1): 51-63.

Hinde, Stephen (2003), "Careless about privacy," *Computers and Security*, 22(4): 284-88.

Langendefer, Jeff and Terence Shimp (2001), "Consumer Vulnerability to Scams, Swindles, and Fraud: A New Theory of Visceral Persuasion," *Psychology and Marketing*, Volume 18, 7, p. 763-783.

Lee, W. A. (2001), "Court Case Helps Keep Heat on Credit Bureaus," *American Banker*, 167(211): 8.

Saliba, Clare (2000), "ID Theft Most Common Offline, Experts Say," *E-Commerce Times*, October 30, 2000, http://www.ecommercetimes.com/perl/story/4675.html, accessed September 21, 2003.

Saunders, Kurt M. and Bruce Zucker (1999), "Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act," *International Review of Law, Computers, & Technology*, 13(2), 183-192.

Sullivan, Bob (2003), "Online job listing an ID theft scam" MSNBC News, Nov. 4, 2003, http://www.msnbc.com/news/830411.asp, accessed September 24, 2003.

Thompson, Joe F. (2002), "Identity, Privacy, and Information Technology," *EDUCAUSE Review* (November-December): 64-65.

Yip, Pamela (2003), "Congress Crafts Legislation to Combat Identity Theft," *Knight* Ridder Tribune Business News, February 3, 2003.

For further information contact: Angeline Grace Close
University of Georgia
Terry College of Business
124 Brooks Hall
Athens, GA 30602
(706) 542-3764 (P)
(706) 542- 3738 (F)
aclose@terry.uga.edu

Figure 1
Cyber Identity-Theft Process

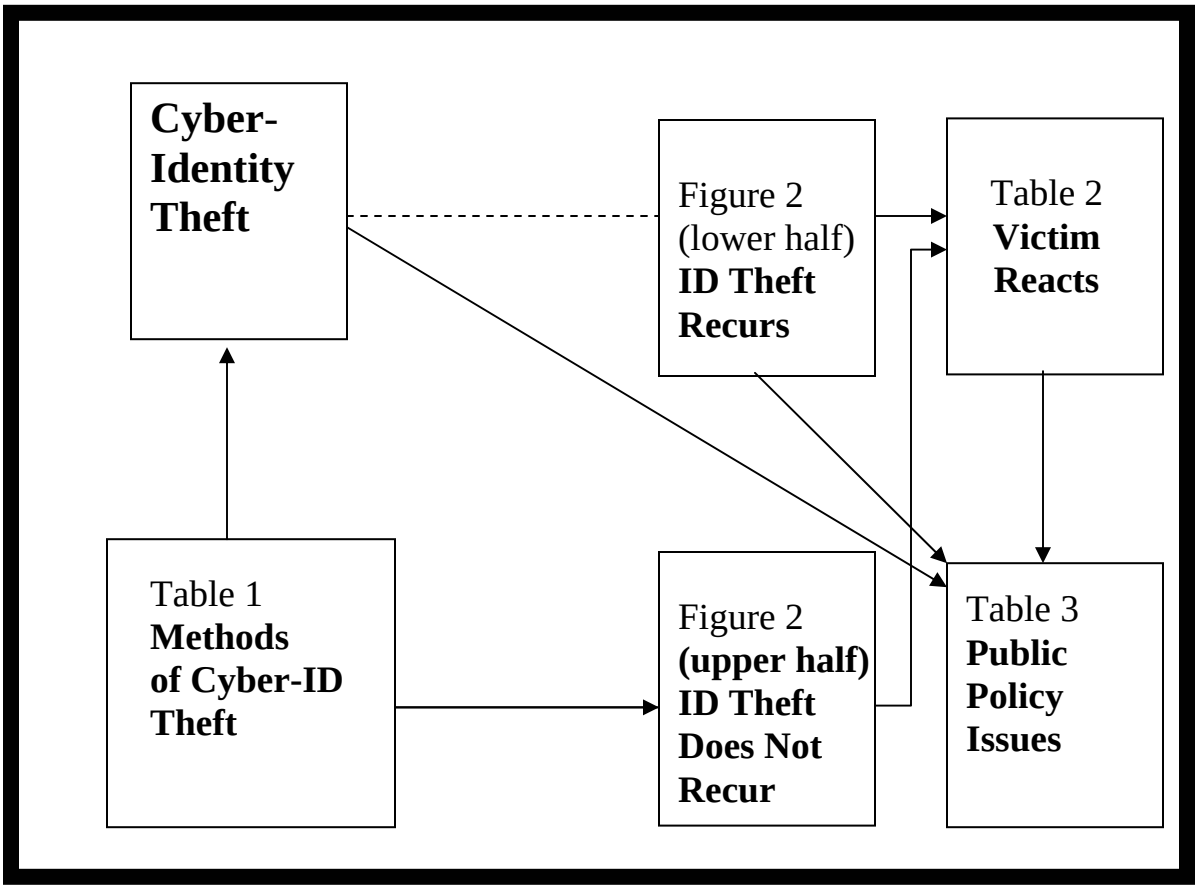

Figure 2

Time Frame of Cyber-Identity Theft and Examples

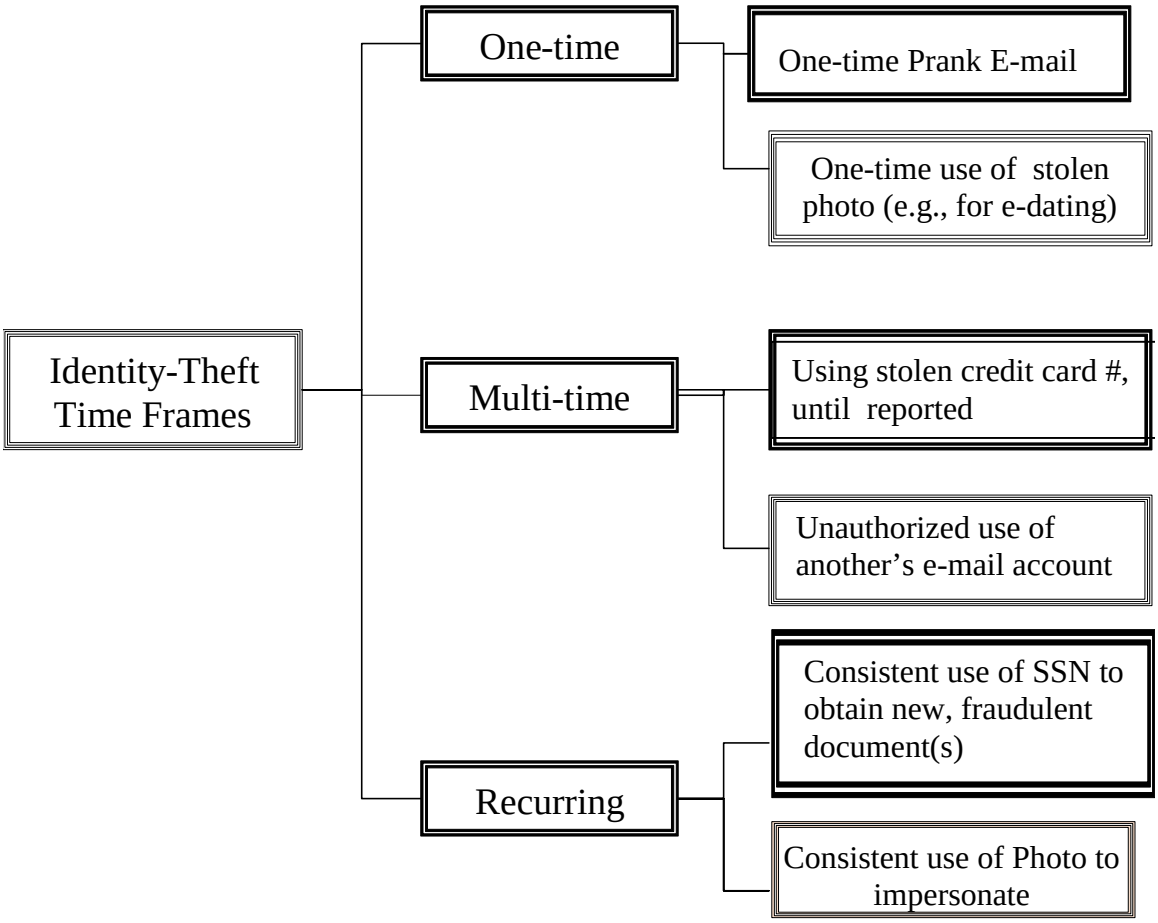

Table 1

Methods of Cyber-Identity Theft

Method	Definition	Example
Broad Scope*		
Hacking	Breaking into a computer database personal or business/organization/government	Wiring another's' funds
Employee Theft	Employees utilizing or selling their company database for fraudulent means or without permission	Pilfering office files
Dictionary Programs	Automatically search all dictionary words for a possible password	Checking all works A to Z;
Spyware	Software, often disguised, that may install itself with other legitimate or free downloads, to collect personal information	Weather-bug; Gator
Skimming	Copying information from a magnetic strip, and subsequently using the information to create a duplicate.	Credit cards
Tapping	Monitoring computer systems to extract key information.	Restaurant computers for credit card #s
Pre-approved	Taking another's per-approved credit and SSN to open an unauthorized account	Mailed credit card offers
Mass Rebellion	Peer-to-peer networks built to exchange music or media files. At present, the future of such sites is unclear, and some users are	peer-to-peer sites (e.g., Kazaa, Napster)

	being taken to court (e.g., by the music and film industry)	
Narrow Scope		
Careless-ness	Prowling for users who use their computer or Internet access carelessly	Saved Passwords, logoff may not go through
Disposal Abuse	Obtaining information from another's disposed / sold hardware or software	Dumpster-diving, leaving personal information behind on old computer via junk-yard, garage sale
Autofill Abuse	Obtaining information from computer programs that "memorize" and complete typing on another's machine	Type in a few letters until cleared
Phishing	Establishing a fake web site designed to look like a company's actual site or sending official-looking messages	"Official" request for SSN
Phony	A phony machine that copies personal information	ATM
Pre-text	Calling a prospective victim, posing in an attempt to obtain personal information	Bank ; Credit card company
Posing	Unrightfully representing another individual	Bank rep.; computer exams
Pranking	Posing as another online to play a joke or for fun	e-dating
Fraudulent job posting	Posting a job that does not exist to collect personal information	"Manager Wanted"
Shoulder	Peeking for information as another enters it on a computer screen;	Passwords; account

Surfing	physically watching passwords	numbers
Intercepting IMs	Receiving online traffic intended for another	IMs; e-mail

* Scope refers to whether the method is more likely to gather data from several consumers at once (i.e., broad) or from one consumer at a time (i.e., narrow).

Table 2

Behavioral Responses to Identity Theft

Victim's behavior may change (via):	**Online Example**	**Offline Example**
Lessened (correct) disclosure of personal information	e-mail addresses	Home or work addresses
Change in selection/use of exchange partners	e-tailers	Retailers
Change in frequency/ extent of transactions	e-commerce; e-dating	Shopping; credit card use
Change in general shopping and purchasing behavior	Security checks	Requesting to check identification for credit card purchases

Table 3

Public Policy and Consumer Welfare Issues

I. Dissemination of cyber-identity theft methods (so that potential victims can protect themselves).

II. Employee access to data and associated potential for misuse.

III. Credit-reporting bureaus:

a) Is it necessary to revise procedures so that victims can "set the record straight"?

b) How to safeguard the information that credit bureaus provide to third parties?

c) Disclosure of credit reports and privacy issues.

IV. The inherent difficult associated with proving you **did not** commit acts (e.g., make specific charges to a credit card)

V. Regulation of data exchanges.

VI. Uses of marketing databases:

a) Selling databases to third parties.

b) Telemarketing & no-call lists.

VII. Use of data by financial institutions.

VIII. Liability issues:

a) Who is responsible for the loss of information & privacy?

b) Who will pay the costs of "restoring" identify and paying associated costs (e.g., related to credit card fraud).

c) Assessment of fault.

d) To what extent do criminal statutes need to be revised?

e) Are current laws and regulations sufficient to deal with cyber identity-theft?

IX. Assisting cyber-identity theft victims.

X. Expanding public education / awareness (e.g., about theft methods, remedies).

XI. Educating the populace so that overall crime rates decline (e.g., so that less people have an interest in perpetrating identity thefts).

XII. Effective criminal enforcement

XIII. Risk analysis & risk assessment:

a) What are the costs & benefits associated with preventing identify theft?

b) What would be the costs associated with reducing identity theft to zero?

c) Who will bear these costs?

d) What aspects of identify theft pose the largest risks for society or specific industries or specific consumers?

e) Assessment of damages.

XIV. What are the specific costs for consumers (e.g., social, financial, psychological)? How can these costs be alleviated?

XV. What are the costs for business (both at the firm level and the industry level)? What are the threats to our economic system?

XVI. What are the best ways to promote safety tips and improved technologies?

XVII. What are the best media (e.g., Internet, class-room setting, one-on-one instruction, brochures) for implementing education or remedial programs?

XVIII. What are the best ways to "reform" identify thieves?