The Ongoing Critical Threats Created by Identity Fraud: An Action Plan

Gary R. Gordon, Ed.D.
Utica College

Norman A. Willox, Jr.
LexisNexis Special Services Inc.

Abstract

Much has happened since the 2003 publication of *Identity Fraud: A Critical National and Global Threat* and yet much is still the same. There is a greater awareness of the problem, as indicated by the number of conferences focused on identity theft, the amount of press on the topic, and the increase in legislative activity. However, we continue to struggle with the ramifications of the use and risks of data in an information society and its potential implications for identity fraud. The possibility that there is a correlation between data misuse and identity fraud has been exacerbated by the heavily publicized recent corporate and governmental security breaches that have involved the loss or theft of personal data. As a result, the debate on the responsible use of personal identifier information for making decisions in the areas of commerce, law enforcement, and national security has intensified. The challenges of privacy and security in this new era remain the same.

This paper follows the structure of the earlier one, maintaining the same headings for consistency purposes. In each section, there is discussion of what has occurred since 2003, what gaps remain, and what the research agenda should be to close those gaps. Examples of this research are suggested.

Size and Scope of the Identity Fraud Problem

While there has been significant attention focused on identity theft issues, little progress has been made to quantify the size and scope of the problem. Since 2003, there have been only two major studies, 2005 Identity Fraud Survey Report, and 2006 Identity Fraud Survey Report both by Javelin Strategy & Research. The 2005 report replicates the 2003 FTC's Identity Theft Survey Report and is an effort to identify trends. The results indicate that there were 9.3 million new victims in 2004. The 2006 report indicates that the number of victims has dropped to 8.9 million. This is a decrease from the 10.1 million reported in 2003. While these studies provide a baseline for longitudinal trends and insight into how identity theft occurs, they only focus on identity being compromised through theft or stolen records, not through identity fraud, also known as

synthetic identity. They provide estimates of the scope and a descriptive approach to victimization characteristics.

Little progress has been made in developing a national database of identity fraud incidents. UCR and NIBRS do not include a category to collect this information. However, in July 2004, the National Crime Victimization Survey was updated to include a section on identity theft. There is not yet enough data available for analysis, but in future Bureau of Justice Statistics reports, information on the size and scope of identity theft will be presented. In the September 16, 2004 version of the National Crime Victimization Survey, the section on identity theft collects information regarding the discovery of the use of or attempt to use credit cards or numbers without permission; the use of or attempt to use other accounts, including wireless telephone and bank accounts; and discovery of the use of or attempted use of personal information without permission to procure new accounts. The number of episodes of use or attempted use is asked, as well as the timing of the attempts, how the victim was made aware of the identity theft, the monetary amount obtained or used by the perpetrator, and the effect of the misuse on the victim, including how long it took to resolve the problems it caused. The final question in the identity theft section asks the respondent what specific problems the identity theft caused, from being turned down for a loan to having utility services terminated to being the subject of a criminal investigation.

The addition of identity theft questions in the National Crime Victimization Survey is a significant step. The information garnered from these questionnaires will be invaluable in conducting research about the size and scope of identity fraud and theft. It will also provide data that can be used in studying the characteristics of identity fraud and theft victims, as the questionnaire gathers information concerning the respondents' sex, income level, marital status, age, education, housing, race, telephone use, and the like. The required research identified below will provide analysis of this information so that conclusions can be drawn which will lead to solutions to the problem.

Required Research

Study the trends, causes, early detection, and prevention of identity fraud and theft.

Examples:

- Exploratory and descriptive studies to record and understand the size and scope of identity fraud and theft
- Examination of characteristics of individuals, organizations, and businesses victimized by identity fraud offenders
- Development of methods for reporting, tracking and classifying identity fraud

The Role of Identity Fraud in Facilitating Criminal and Terrorist Activity

Beyond the garden variety methods of identity theft identified in the above studies, the modus operandi of criminals who are engaged in identity fraud has proven to be dynamic, technologically innovative, and focused on vulnerabilities of information systems. They have exploited the outermost perimeter of secure corporate and government systems where customers, vendors, and citizens seek services. In the 2003 white paper, anecdotal evidence was presented that implied that identity fraud is a facilitator of criminal and terrorist activities. Similar information has appeared in two recent GAO reports that support this thesis. In a May 2005 report, Improvements Needed to Strengthen U.S. Passport Fraud Detection Efforts, the authors suggest that passport fraud is used to commit other crimes.

> According to State Bureau of Diplomatic Security documents, passport fraud is often committed in connection with other crimes, including narcotics trafficking, organized crime, money laundering, and alien smuggling. According to Diplomatic Security officials, concerns exist within the law enforcement and intelligence communities that passport fraud could also be used to help facilitate acts of terrorism (GAO-05-477).

However, there have not been any research studies that support this premise.

Since 2003, there has been a dramatic increase in the collection methods used by criminals to steal personal identifier information. These include key logging programs, phishing and pharming schemes, and a variety of methods to gain access to databases containing vast amounts of information. One study on key logging reports that this hacking activity has increased over 65% since 2004. VeriSign reports that in 2005 there were 6,191 keyloggers, as compared to 3,753 in 2004 and 300 in 2000. “Keyloggers, silently installed programs that record a victim's keystrokes and send them to hackers, put tens of millions of Internet users' finances, personal data and account information at risk. Largely distributed by organized cyber theft groups, they are typically packaged with phishing emails or spyware -- malicious code that then tracks victims' online activity -- often eluding traditional security defenses like anti-virus software and firewalls” (PR Newswire 2005). Hackers use keylogger programs to collect keystrokes from unsuspecting victims whose use of online chat rooms and instant messaging type programs makes them vulnerable. The hacker activates the program so that he can collect any information that the user has inputted online, including personal data used in online transactions. A significant amount of this data is transmitted internationally to countries where it is difficult for the United States to intervene. The perpetrator then uses that information to assume an identity and gain access to credit card accounts and the like.

While malware, viruses, and worms still pose problems, cybercriminals have become more sophisticated, organized, and clandestine in their activities.

> While hactivists seek maximum public exposure to advance a political cause, fraud is all the more insidious because perpetrators and victims conspire to keep it hidden. This year promises to be the worst yet…Cybercriminals are making so much money – more than the illegal drug trade last year, according to the U.S. Treasury – that they've been doing their own R&D. That research is already bearing fruit. Experts worry that direct theft of data (as opposed to phishing…) is on the rise. Identity thieves are now able to target specific attacks against specific people or companies and they can select their targets based on factors like net worth (Sparks, 2006).

For the past five years, the United States Secret Service has noted an increasing trend in such cybercrime activity. They have conducted several successful investigations, including Operation Firewall, which identified and eventually shut down several organized computer crime groups – Shadowcrew, Carderplanet, and Darkprofits. "The criminal organizations operated websites used to traffic counterfeit credit cards and false identification information and documents. These websites not only shared information on how to commit fraud, but also provided a forum by which to purchase such information and tools" (www.secretservice.gov, 2004).

Cybercriminals, like any other criminals, are eager to stay at least one step ahead of law enforcement and the technological community. Any technological innovation presents an opportunity for them. The newest cellular technologies, including iPods and MP3 files, are vulnerable to key logger and other forms of spyware. Organized crime groups are also using botnets to increase their efficiency in implementing denial of service attacks, spamming, and stealing personal information.

> Because China's PCs don't generally run licensed versions of Microsoft's Windows, they're not eligible for the security patches Microsoft makes available to its legitimate users. Hackers have already taken control of the PCs of thousands of unsuspecting Chinese and used them as a platform from which to launch spam attacks. These so-called botnets are routinely bought, sold and swapped in Internet chat rooms (Sparks, 2006).

Cybercrime commerce is booming and negatively impacting legitimate commerce and national security.

Required Research

Study the evolving threat from cyber criminals, insiders, and organized crime groups.

Examples:

- Current and emerging criminal groups that perpetrate identity fraud and theft with a focus on their modus operandi
- Value of information: societal and criminal calculus
- Review and analysis of emerging data on identity fraud and its relationship to criminal behavior
- Develop best practices for detecting, preventing, investigating, and prosecuting attacks from organized criminal groups, cyber criminals, and insiders.
- Evaluate technology as a problem and a solution

Managing Identity Fraud: Laws and Regulations

Throughout the 9/11 Commission hearings, conducted in 2003 and 2004, the country watched with stunned attention as critic after critic identified one government intelligence breakdown after another that not only led up to the events of September 11, 2001, but continue to tear at our terrorism protections. When it released its report in July 2004, the 9/11 Commission identified identity authentication as one of those failures. There, it specifically called for identity authentication or "screening" systems, observing, "At many entry points to vulnerable facilities, including gates for boarding aircraft, sources of identification are the last opportunity to ensure that people are who they say they are and to check whether they are terrorists" (9/11 Commission Report, p.390).

Following the recommendations of the 9/11 Commission, Congress passed the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, which the President enacted into law on December 17, 2004. Several of the provisions of IRTPA deal specifically with the identity authentication weaknesses identified in the 9/11 Commission Report. For example, the law requires the development of standards for the use of biometric identifiers in airport access control systems (Section 4011); the development of a plan to accelerate implementation of an automated biometric entry and exit data system (Section 7208); the development of a plan to require a passport or other documents deemed to be sufficient for U.S. citizens and others previously waived from producing identification documents when traveling into the United States (Section 7209); and the establishment of minimum standards for the creation and use of the typical identity "breeder documents," such as birth certificates (Section 7211), driver's licenses and personal identification cards (Section 7212), and Social Security cards and numbers (Section 7213).

In May, 2005, Congress furthered the cause of mandating identity authentication systems by passing the Real ID Act of 2005, as part of the Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005 (P.L. 109-13). Real ID mandates the establishment of minimum driver's license certification requirements and imposes on all federal

agencies a requirement that within three years they may not accept, for any official purpose, a state-issued driver's license or identification card unless the state meets the minimum requirements.

In August 2004, the President, recognizing the need for standardization of identification credentials to promote security and prevent identity fraud, issued Homeland Security Presidential Directive (HSPD) 12, "Policy for a Common Identification Standard for Federal Employees and Contractors." Pursuant to this Directive, in February 2005, the Department of Commerce's National Institute of Standards and Technology (NIST) promulgated Federal Information Processing Standards Publication (FIPS) Pub 201, Personal Identity Verification (PIV) of Federal Employees and Contractors. The PIV specifies the architecture and technical requirements for a common identification standard for federal employees and contractors, with the goal of achieving "security assurances for multiple applications by efficiently verifying the claimed identity of individuals seeking physical access to federally controlled government facilities and electronic access to government information systems."

Notwithstanding the efforts since 2003 to develop more effective identity management systems which will protect against identity fraud and terrorism, there is still no program designed to determine that someone is who they say they are before boarding a commercial airplane. Similarly, drivers' licenses are still relied upon as the principal means of identity proofing, despite the existence of many of the same deficiencies that prompted the passing of IRTPA and the Real ID Act. Uniformity in government credentialing is still lacking as well.

Fraudsters have complicated these identity management efforts by taking aim on the best identity verification solutions. Beginning early last year, it became apparent that databases of many companies and government agencies were being victimized through theft, connivance, and hacking, exposing the personal information of hundreds of thousands of Americans. Despite the best law enforcement efforts of the United States Secret Service, the Federal Bureau of Investigation and others, many of the responsible criminals remain largely undetected and undeterred. Meanwhile, Congress, the Federal Trade Commission and other regulatory agencies are examining how best to shore up government and corporate security processes to mitigate these threats, while not unduly restricting the information solutions that help prevent identity fraud.

Required Research

Assess the impact of policy decisions, legislation, and regulatory actions.

Examples:

- The legal and technical challenges of sharing personal identifier information within government, within industry, and among government and industry

- Determine the impact of policy decisions such as limiting the use of SSNs and biometric data
- Analyze the evolving legislation and the issues that remain to be addressed

Managing Identity Fraud: Information Policy and Technology

It is evident that focusing solely on identity fraud and theft is insufficient, because the phenomenon is part of a much broader and complex discussion. The identity fraud problem quickly morphs into several areas that impact how organizations and individuals conduct business or accomplish their mission. Although collecting and matching personal identifying data presents a risk, it is key to providing customer service, maintaining a good reputation, ensuring trusted transactions, protecting against fraudulent applications, preventing terrorism, and locating sexual predators. Because personal identifier information is required to validate or authenticate identity, it is valuable and absolutely necessary. Its market value makes it increasingly vulnerable to crime. It can be stolen and used for immediate financial gain (creating an account and charging purchases) or as part of a batch of identities available for sale through carding websites. The challenge is to develop trusted and secure information-sharing environments that maximize the societal benefits of using this type of information and minimize the risks associated with it.

Corporations and governments that hold personal identifier information must:

- Evaluate and improve their information security practices to protect sensitive information;
- Prevent the potential loss of this data;
- Develop policies for use of information;
- Consider the privacy implications for the use and abuse of this information;
- Review and assess their identity authentication systems and background screening methods;
- Determine how information is being used to harm individuals and businesses and implement solutions to mitigate the harm;
- Find solutions to the impediments and risks of information sharing;
- Determine how enabling technologies can facilitate information sharing and enhance privacy.

Consumers are faced with questions regarding:

- How they can prevent themselves from becoming an identity fraud victim;
- How to respond to breach notices;
- What to do if someone assumes their identity;
- How they can best manage and control their identity.

Required Research

Study the use of data, its protection, and the role of enabling technologies to facilitate privacy and information sharing.

Examples:

- Impact of data breaches on the rate of identity theft
- Public perception studies to determine attitudes toward trust, information use, and policies
- Evaluation of privacy technologies that purport to enable enhanced privacy and facilitate information sharing
- Securing sensitive information: practices, methods, and policies

Identity Management Systems

Identity management systems need strong identity authentication processes. Determining that a person who is claiming an identity is really the person whose identity is presented is a critical stage for commerce and security, both domestically and globally. The personal information an agency, institution, or corporation holds is an asset that must be protected in order to establish and maintain trust between the organization and its clients or customers. The risks and consequences of a security breach include impairment of reputation, financial losses, loss of customer confidence, failure to meet regulatory standards, and added costs. Strong identity management systems are necessary to assist in regulatory compliance, prevent fraud, improve security, promote customer confidence, and to enter into a trusted relationship transaction.

While efforts have been made to use risk-based methods to improve the identity authentication process, they have not been completely successful. Government programs such as CAPPS II have been cancelled because policy concerns over mission creep, audit, and redress have not been addressed to the satisfaction of congressional committees. The rash of disclosures about security breaches in 2005 made a big splash in the media. In reality, only a small percentage of the breached data caused any harm. This may be because in many cases the data was lost, not stolen. Attempts to use stolen data are often thwarted by fraud prevention and mitigation strategies that many institutions have in place. However, the risk of stolen data being misused is still there. "Society's growing reliance on information technologies exacerbates both the threat posed by personal information in the wrong hands and the dangers of poorly focused or excessive regulation intended to guard against that threat" (Cate, 2005). Identity management systems that strike a balance must be developed and implemented. Best practice standards and technological systems must be put in place to secure identifying information and protect against security breaches for every organization – private or public – that processes, stores, and uses personal data.

Required Research

Study how to improve identity authentication systems and protect identity information to reduce fraud and improper payments, and protect national security.

Examples:

- The evaluation of risk-based technology solutions
- The effectiveness of identity authentication systems
- Improving authentication methods of customers and citizens using business and government web-based systems

Recommendations

In the original white paper, seven recommendations were made to establish a national strategy, a research agenda, and develop policies to combat the growing threat of identity fraud. While some progress has been made on these recommendations, much remains to be accomplished.

The 2003 recommendations were:

1. Gain a commitment from the highest levels of federal government to lead and fund a national strategy to combat the identity fraud problem.
2. Establish a central information database of identity fraud incidents.
3. Establish a national identity fraud research agenda.
4. Establish more sophisticated domestic and global information-sharing networks.
5. Conduct a study of existing domestic and global policies, laws, and regulations to determine best practices for combating identity fraud.
6. Enhance the protection of individual privacy and information ownership.
7. Improve information-sharing systems that enhance identity authentication solutions while protecting privacy.

N.B. A full discussion of these recommendations can be found in the 2003 white paper at www.utica.edu/academic/institutes/ecii/jecm/articles.cfm?action=issue&id=15.

The following recommendations are an extension of the ones above. However, instead of calling for action, they articulate an action plan.

1. Establish a research center that fosters a partnership among the private and public sectors and academe.
2. Convene a symposium of subject matter experts to formulate a multi- year research agenda.
3. Develop and implement a comprehensive research plan including strategies to fund it.
4. Draw on the research to formulate policies for combating identity fraud, improving information sharing, strengthening security, and enhancing privacy.
5. Utilize the research to develop technological and best practice solutions that will improve risk management, facilitate commerce, and augment security.

1. Establish a research center that fosters a partnership among the private and public sectors and academe.

The Center for Identity Management and Information Protection (CIMIP) has been formed by Utica College to address the issues raised in this white paper. It is comprised of corporate, government, and academic partners who are committed to finding solutions through a strong applied research agenda. CIMIP will provide thought leadership through studies of new identity fraud prevention strategies, improved information-sharing methods, innovative information use, and enhanced technological solutions. One purpose of these studies will be to drive policy, regulatory, and legislative decisions.

CIMIP will be led by Utica College faculty and will partner with thought leaders in the corporate and government space, as well as other leading academic partners.

Mission

The Center for Identity Management and Information Protection will facilitate a national research agenda on identity management, information-sharing policy, and data protection. The Center is committed to providing thought leadership by conducting studies and conferences that will promote new prevention strategies, improved information sharing, innovative information use, enhanced technological solutions, and drive policy, regulatory, and legislative decisions.

Goals

- Study the trends, causes, early detection, and prevention of identity fraud and theft.
- Understand the evolving threat from cyber criminals, insiders, and organized crime groups.
- Assess the impact of policy decisions, legislation, and regulatory actions.
- Improve identity authentication systems to reduce fraud and improper payments and protect national security.
- Study the use of information, its protection, and the role of enabling technologies to facilitate privacy and information sharing.

The establishment of the Center will provide the leadership addressed in the 2003 recommendation #1. The research and subsequent policies and solutions derived from the research output will address recommendations #2-7 in the earlier white paper.

2. Convene a symposium of subject matter experts to formulate a multi-year research agenda.

In 2006, the Center for Identity Management and Information Protection will convene a workshop to assist in the formulation of a research agenda. In addition to the CIMIP partners, subject matter experts from industry, government, law enforcement, academe, and think tanks will be invited. The proceedings will be published and used as a roadmap for research for the next three years. It is hoped that through such an exercise, a focused national research agenda can be developed, thus addressing and expanding on the 2003 recommendation to establish a national identity fraud research agenda.

3. Develop and implement a comprehensive research plan including strategies to fund it.

Based on the proceedings of the workshop and the guidance of the CIMIP Research Steering Committee, which is comprised of its partners, a comprehensive multi-year research agenda will be articulated. A strategy for funding the plan will be included. The initial seed money for CIMIP will come from forward-thinking corporate partners. However, in order to complete the ongoing research necessary to address and solve this problem, additional funding must come from other constituents, such as the federal government and private foundations.

4. Draw on the research to formulate policies for combating identity fraud, improving information sharing, strengthening security, and enhancing privacy.

It is anticipated that thoughtful and well-designed research projects will provide a process for the development of public policies to address these challenging problems. If policies are based on strong research foundations, stakeholders will be more willing to accept and implement them. In many cases, the efforts to resolve problems have been bogged down by unproven claims that tend to support specific ideological agendas. These myths need to be challenged; the only way to achieve that is through a research agenda that sheds light on these issues.

5. Utilize the research to develop technological and best practice solutions that will improve risk management, facilitate commerce, and augment security.

As with the formulation of policy above, it is anticipated that the applied research projects will identify best practices for industry and government. The results of assessing policies and programs will offer guidance to organizations as they strive to establish best practices for themselves and their industries.

Concluding Remarks

The issues identified in this paper are complex, challenging, and have far reaching impacts on how commerce is conducted, how security decisions are made, and how citizens interact with their government and society. The action plan proposed is the next logical step to addressing many of these issues. It is based on a well-articulated and designed research agenda that, if successful, will drive policy development and stimulate wide-ranging solutions.

Now is the time to carry out the 2003 recommendations and move forward. The action plan outlined here provides the vehicle for doing so. The debate and discussion must end. All stakeholders are invited to respond to this call for action and to embrace the plan. Without their agreement and commitment to moving forward, this epidemic will continue to grow exponentially and will impact each stakeholder and every aspect of our society.

About the Authors

Gary R. Gordon, Ed.D. is a professor of Economic Crime Management at Utica College. He developed the first major in Economic Crime Investigation in 1988, at Utica College. In 1999 he developed the first master's degree in Economic Crime Management. He co-founded the Economic Crime Institute of Utica College in 1988 and serves as its Executive Director. He is also the Executive Director of the Center for Identity Management and Information Protection at Utica College, which was announced in June 2006. Dr. Gordon holds a doctorate in Counseling Psychology from Boston University, a master's degree in Criminal Justice from the University of New Haven, and a bachelor's degree in Psychology from Clark University.

Norman A. Willox, Jr. is the CEO of LexisNexis Special Services, Inc. (LNSSI). Mr. Willox is the Chairman of the National Fraud Center, where he was CEO for more than ten years. He serves as a board member for the Economic Crime Institute of Utica College and worked with Dr. Gordon to create the Center for Identity Management and Information Protection. He is also a member of the board of the International Fraud Symposium, a trustee for the National Coalition for the Prevention of Economic Crime, and a founding member of the Internet Fraud Council. Mr. Willox has formal law enforcement and professional training credits and received his bachelor's degree in Public Administration from West Chester University.

References

Cate, Fred (2005). Information Security Breaches and the Threat to Consumers. The Center for Information Policy Leadership, Hunton & Williams LLP.

FIPS PUB 201 (2005, February 25). *Personal Identity Verification (PIV) of Federal Employees and Contractors, Computer Security Division*, Information Technology Laboratory, National Institute of Standards and Technology. http://www.csrc.nist.gov/publications/ fips/fips201/FIPS-201-022505.pdf

GAO-03-477 (2005, May). *Improvements Needed to Strengthen U. S. Passport Fraud Detection Efforts, Report to Committee on Homeland Security and Governmental Affairs*, U. S. Senate. http://www.gao.gov/new.items/d05477.pdf, retrieved October 5, 2005.

Gordon, G., Willox, N., Rebovich, D., Regan, T., & Gordon, J. (2004). Identity Fraud: A Critical National and Global Threat. *Journal of Economic Crime Management*, 2(1), 1- 48.

iDefense Tracks Dramatic Growth in Password-Stealing Keyloggers (2005, November 15). *PR Newswire.* http://sev.prnewswire.com/computer-electronics/20051115/SFTU05515112005-1.html, retrieved January 4, 2006.

Javelin Strategy and Research and Better Business Bureau (2005). *2005 Identity Fraud Survey Report.*

National Commission on Terrorist Attacks (2004). T*he 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States.* New York: W. W. Norton and Co.

National Crime Victimization Survey. Form NCVs-1, 9/16/2004. http://www.ojp.usdoj.gov/bjs/pub/pdf/ncvs104.pdf, retrieved January 5, 2006.

New Research Shows Identity Fraud Growth Is Contained and Consumers Have More Control Than They Think (2006, January 31). BBB Online. http://www.bbbonline.org/idtheft/safetyquiz.asp, retrieved February 1, 2006.

Sparks, John. Is That a Bull's-Eye on Your Wallet? (2006, January 9). *Newsweek International Edition*. http://msnbc.msn.com//id/10682795/site/newsweek, retrieved January 5, 2006.

U. S. Secret Service's Operation Firewall Nets 28 Arrests (2004, October 28). U.S. Secret Service Press Release. www.secretservicce.gov/press/pub2304.pdf, retrieved January 5, 2006.