TESTIMONY OF BESTOR WARD

Member of the

NATIONAL ASSOCIATION FOR INFORMATION DESTRUCTION, INC. ("NAID")

Before the

COMMITTEE ON FINANCIAL SERVICES

UNITED STATES HOUSE OF REPRESENTATIVES

Hearing on

ASSESSING DATA SECURITY:

PREVENTING BREACHES AND PROTECTING SENSITIVE INFORMATION

MAY 4, 2005

I. Introduction

Mr. Chairman and members of the Committee, I am Bestor Ward, a member of the National Association for Information Destruction, Inc. ("NAID"). I appreciate the opportunity to appear before you today to discuss the important role that proper information destruction plays in the fight against identity theft. NAID commends the Committee for addressing this critical issue.

I am President of Safe Archives – Safe Shredding, a business that provides secure records management, media storage, and information destruction services in Mobile, Alabama and the surrounding area. I am a member of NAID's Governmental Relations Committee. I also serve on the boards of the J.L. Bedsole Foundation and AmSouth Bank N.A. Through these professional roles, I have gained first-hand experience about identity theft. As an AmSouth Bank director, I receive regular updates on the incidence of identity theft affecting the bank. The J.L. Bedsole Foundation has been the victim of identity theft; on two separate occasions the foundation's credit card was used by an identity thief who made expensive charges on the card. As President of Safe Archives – Safe Shredding, I run a business dedicated to storing and destroying confidential records securely, so that they do not fall into the wrong hands.

NAID is the international, non-profit trade association of the information destruction industry. NAID and its individual members are expert in, and committed to, the proper destruction of paper records and other media containing sensitive financial or personal information that could be misused by identity thieves. NAID's mission is to champion the responsible destruction of confidential information and materials by promoting the highest standards and ethics in the industry. NAID members are bound to a strict code of ethical practices. NAID has a Complaint Resolution Council that is dedicated to reviewing ethical

complaints and recommending appropriate actions (up to and including fines and expulsion) to the NAID Board of Directors. In addition, NAID offers an annual operations certification program to its members, which establishes standards for employee hiring and screening, operations, the destruction process, and insurance, as well as other security factors.

My testimony today covers four main points. First, I will discuss the serious problem of identity theft, which is caused in part by improperly discarding sensitive consumer information. Second, I will address the current legislation that governs information privacy, including the Fair and Accurate Credit Transactions Act, the Gramm-Leach-Bliley Act, and the Health Insurance Portability and Accountability Act. Third, I will argue that, while these laws represent positive steps towards preventing unauthorized access to personal information, they leave significant gaps in coverage. Finally, I will discuss NAID's recommendations for new, uniform legislation to fill these gaps in order to prevent identity theft.

II. Improper Information Destruction and Identity Theft

As this Committee recognizes, identity theft is a serious crime that imposes enormous costs on society. Tens of millions of Americans have been victims of identity theft, costing consumers and businesses tens of billions of dollars.[1] In 2004 alone, 246,570 identity theft complaints were reported to the FTC.[2]

In addition to tangible economic losses, identity theft victims face lost job opportunities, loan denials, and huge intangible costs as they devote months and years to rectifying their

---

1 Synovate/FTC, Identity Theft Survey Report 6-7 (Sept. 2003), *at* http://www.ftc.gov/os/2003/09/synovatereport.pdf; *see also*, Report: Overview of the Identity Theft Program (Oct. 1998 – Sept. 2003) (Sept. 2003), *at* http://www.ftc.gov/os/2003/09/timelinereport.pdf.

2 FTC, National and State Trends in Fraud & Identity Theft (January – December 2004) 4 (February 1, 2005), *at* http://www.consumer.gov/sentinel/pubs/Top10Fraud2004.pdf.

damaged credit records. Identity theft also poses a serious threat to public safety. Terrorists and other criminals, for example, may open bank accounts under false names, launder money using false identities, and use fraudulently obtained drivers licenses to avoid detection. While making identity theft more difficult will not prevent the determined terrorist or criminal from assuming a false identity, the protection of sensitive information can make it more difficult for them to do so. Numerous identity theft crimes are committed by so-called "dumpster divers" who uncover and misuse sensitive paper and electronic documents after they have been discarded. Many hearings to date have focused on controlling or limiting the sale or transfer of personal information. Yet, such controls are undermined when the ultimate disposal of sensitive consumer information is not regulated. It simply does not make sense to implement information-transfer controls while ignoring the fact that this same information is often being placed in the trash for anyone to take.

Identity theft is a crime of opportunity, and it is vital that we take steps to reduce criminal opportunities. One of the most efficient and effective ways to fight identity theft is to prevent it by ensuring secure records management and proper disposal of confidential information at the point when documents are discarded in the normal course of business. It makes far greater sense to enact strong laws that prevent so-called "dumpster divers" and other criminals from accessing information, than waiting until after massive losses have occurred and attempting (often unsuccessfully) to find and prosecute the perpetrators after the fact. Relying on after-the-fact prosecution to fight identity theft is particularly ineffective, considering that approximately 61% of victims who reported identity theft to the FTC in 2004 did not notify any police department.[3]

---

[3] FTC, National and State Trends in Fraud & Identity Theft (January – December 2004) 11 (February 1, 2005), *at* http://www.consumer.gov/sentinel/pubs/Top10Fraud2004.pdf.

III. Current Legislation Governing Information Privacy and Identity Theft

NAID commends Congress for combating identity theft by enacting the Fair and Accurate Credit Transactions Act ("FACT Act"), the Gramm-Leach-Bliley Act ("GLBA"), and the Health Insurance Portability and Accountability Act ("HIPAA"). However, NAID recognizes that the existing federal and state consumer fraud legislation leaves significant gaps in coverage. NAID thanks this Committee for its attention to this serious matter, and encourages the Committee to take further steps to fill these gaps. In particular, NAID supports strong, uniform information disposal legislation that broadly covers all businesses that possess documents containing consumer information subject to misuse.

A. The FACT Act and Disposal Rules

Pursuant to the FACT Act, the Federal Trade Commission ("FTC") has adopted a rule entitled, "Disposal of Consumer Report Information and Records"[4] ("FTC Disposal Rule"), which will take effect on June 1, 2005.[5] Under that rule, businesses are required to properly dispose of and to destroy "consumer information," which is defined as "any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report. Consumer information also means a compilation of such records."[6] In turn, the FACT Act defines "consumer report" as any "communication of any information by a

---

4 16 C.F.R. Part 682.

5 The Securities and Exchange Commission, the Federal Deposit Insurance Corporation, the Comptroller of the Currency, the Federal Reserve System, the Office of Thrift Supervision, and the National Credit Union Administration also promulgated rules pursuant to the FACT Act. 69 FR 71322 to be codified at 17 C.F.R. Part 248; 69 FR 77610 to be codified at 12 C.F.R. Parts 334, 364; 69 FR 77610 to be codified at 12 C.F.R. Parts 30, 41; 69 FR 77610 to be codified at 12 C.F.R. Parts 208, 211, 222, 225; 69 FR 77610 to be codified at 12 C.F.R. Parts 568, 570, 571; 69 FR 69269 to be codified at 12 C.F.R. Parts 717, 748.

6 16 C.F.R. § 682.1(b).

consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living," which is intended to assist in "establishing the consumer's eligibility for — (A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes;" or other authorized purposes.[7]

The FTC Disposal Rule specifically requires any person or company that possesses or maintains "consumer report" information to "tak[e] reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal."[8] The rule provides examples of how to comply with this standard, including:

- Implementing and monitoring compliance with policies and procedures that require shredding or other forms of destruction of documents and electronic media containing consumer information; and
- Contracting with a third party to properly dispose of consumer information and monitoring their performance.

By June 1, 2005, entities over which the FTC has authority[9] must adopt and implement their own document destruction policies or contract with a document shredding company or other data destruction company to do so. Penalties for violating the rule include actual damages;

---

7 15 U.S.C. § 1681a(d)(1). This definition is also subject to some exclusions. 15 U.S.C. § 1681a(d)(2).

8 16 C.F.R. § 682.3(a).

9 The FTC has authority to enforce compliance under the Federal Trade Commission Act. The FTC's jurisdiction extends over entities except certain banks, savings and loan institutions, federal credit unions, common carriers, air carriers, insurance companies, and others subject to the Packers and Stockyards Act. 15 U.S.C. §§ 1681s, 1681w; 15 U.S.C. § 1012.

statutory damages up to $1,000; punitive damages; attorneys' fees; and civil penalties up to $2,500 per violation.

Although the FTC's Disposal Rule holds great promise in combating identity theft, its effectiveness is limited by the fact that it reaches only "consumer report" information. In the end, however, individuals could just as easily become victims of identity theft through compromise of their personal information from sources other than consumer reports, such as discarded credit card records or computer tapes placed in the trash. Enormous cost, inconvenience, and a sense of violation can be avoided through the simple expedient: proper disposal of all documents containing sensitive consumer information.

B. The Gramm-Leach-Bliley Act and FTC Safeguards Rules

The FTC's Disposal Rule supplements the privacy provisions set forth in the Gramm-Leach-Bliley Act, and its associated agency rules. The Gramm-Leach-Bliley Act governs financial institutions, and protects the privacy of non-public consumer information. The FTC promulgated "Standards for Safeguarding Customer Information" ("FTC Safeguards Rule") pursuant to the Gramm-Leach-Bliley Act. Under the FTC Safeguard Rule, covered entities are required to, "develop, implement, and maintain a comprehensive information security program" that contains appropriate "administrative, technical, and physical safeguards."[10] Such safeguards must be reasonably designed to: "(1) Insure the security and confidentiality of customer information; (2) Protect against any anticipated threats or hazards to the security or integrity of such information; and (3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer."[11]

---

10 16 C.F.R. § 314.3(a).

11 16 C.F.R. § 314.3(b).

Notably, if a financial institution decides to retain a third party to safeguard its customer information, the FTC Safeguards Rule requires that it "[o]versee service providers, by: (1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and (2) Requiring [] service providers by contract to implement and maintain such safeguards."[12] Accordingly, a financial institution must either take internal steps to safeguard customer information or contract with a "capable" third party to do so.

The major limitation of the FTC Safeguards Rule is that it applies only to financial institutions. NAID agrees with the position of FTC Chairman Deborah Platt Majoras that Congress should extend this rule to apply more broadly, beyond financial institutions.[13] There is no reason to limit these requirements to financial institutions. Rather, all record owners should be required properly to dispose of sensitive customer information or, after conducting due diligence, to contract with a capable record disposal company to do so and to monitor the disposal company's performance.

NAID supports various due diligence efforts, including record owners reviewing and evaluating the disposal company's information security policies or procedures, or taking other appropriate measures to determine the competency and integrity of the potential disposal

---

[12] 16 C.F.R. § 314.4(d). Similarly, under the U.S. Department of Health and Human Services standards for HIPAA, a covered entity that permits a business associate to maintain its electronic protected health information must enter a written contract or other written arrangement that documents satisfactory assurances that the business associate will appropriately safeguard the information. 45 C.F.R. § 164.308(b)(1), (4). In particular, such a contract must provide that the business associate will "[i]mplement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information" in its possession. 45 C.F.R. § 164.314(a)(2)(i)(A).

[13] "Congress Likely to Pass Firm Legislation Targeting Identity Theft, Sen. Specter Says," 84 BNA Banking Report 712 (April 18, 2005).

company. Another worthwhile due diligence effort suggested by the FTC involves the certification of disposal companies by a recognized trade association.[14]

C. HIPAA

HIPAA governs the use and disclosure of individually identifiable health information.[15] Under the U.S. Department of Health and Human Services standards, health plans, health care clearinghouses, and certain health care providers are required to "[i]mplement policies and procedures to prevent, detect, contain, and correct security violations."[16] Accordingly, HIPAA adds an important information security mandate by requiring covered businesses to take precautions to protect the privacy of patient information that could be used to commit identity theft. However, as with FCRA and GLBA, HIPAA's reach is limited, leaving many documents with sensitive personal information unprotected.

IV. The Need for Additional Legislation

While the FACT Act, the GLBA, and HIPAA represent important steps towards preventing identity theft, they are too limited in scope. Specifically, the FACT Act and its associated rules only cover "consumer report" information. Many other documents contain information that can be used to facilitate identity theft. It makes little sense to impose strict requirements on the disposal of "consumer report" information, but not other, equally sensitive personal information derived from other sources. Requirements under Gramm-Leach-Bliley and HIPAA, and their associated rules, are also too limited in scope because they apply only to financial institutions and health care businesses, respectively. Accordingly, despite the recent

---

14 16 C.F.R. § 682.3(b)(3).

15 42 U.S.C. § 1320d-6.

16 45 C.F.R. §§ 160.103(3), 164.308.

legislative and regulatory steps taken to fight identity theft, the resulting patchwork of legal authority leaves significant gaps in coverage.

NAID proposes that Congress consider expanding on the current legal requirements by addressing the complete set of businesses and information affected by identity theft. NAID specifically sets forth three proposals for such broad-based legislation.

First, global anti-identity theft legislation should apply more broadly to all records that contain sensitive consumer information, including credit card and bank information, Social Security Numbers, telephone numbers, and addresses maintained by anyone in business.

Second, written privacy policy disclosures provided to consumers should include a statement that details the company's responsibility to destroy all discarded personal information. Consumers should also be made aware that they can request a full disclosure on how any company accepting personal information destroys it when it is discarded.

Third, senior company officers should be responsible for implementing and overseeing their business' disposal policies. Good models for this approach can be found in the Sarbanes-Oxley Act, and in the Interagency Guidelines Establishing Standards for Safeguarding Customer Information, which were promulgated by the Federal Deposit Insurance Corporation ("FDIC"), the Comptroller of the Currency, the Federal Reserve System, the Office of Thrift Supervision, and the National Credit Union Administration pursuant to Gramm-Leach-Bliley ("GLBA Safeguards Rules"). The GLBA Safeguards Rules assign responsibilities to "[t]he board of directors or an appropriate committee of the board."[17] Specifically, these individuals shall:

---

[17] 12 C.F.R. § 30, App. B § III(A); 12 C.F.R. § 225, App. F § III(A); 12 C.F.R. § 364, App. B § III(A); 12 C.F.R. § 570, App. B § III(A); 12 C.F.R. § 748, App. A § III(A). The FDIC, the Comptroller of the Currency, and the Federal Reserve System define board of directors as the

"(1) Approve the [entity's] written information security program; and (2) Oversee the development, implementation, and maintenance of the [entity's] information security program, including assigning specific responsibility for its implementation and reviewing reports from management." NAID recommends that Congress apply these models for corporate responsibility by requiring appropriate senior officials to implement and supervise disposal policies that meet the requisite legal standards. Compared to the high costs that victims and the law enforcement community incur after identity theft has been committed, it is far more efficient to require proper methods of disposal to prevent the misuse of sensitive consumer information.

V. Conclusion

I will close with an anecdote. Shortly after Georgia enacted information destruction legislation in May 2003, NAID received a call from an employee of a well-known national corporation. The caller asked for a list of Georgia companies that it could retain to shred documents covered by the state's new disposal requirements. The caller was located in the company's corporate headquarters outside of Georgia, and our NAID representative offered to send a broader list of NAID member-companies that operate in other states where the company conducts business. The caller's response was, "No thanks, the other states don't have shredding laws." This response highlights the need for strong, uniform federal legislation that closes the gaps between existing laws by requiring all businesses to properly dispose of sensitive financial and personal information that is subject to misuse.

"managing official in charge of the branch or agency." 12 C.F.R. § 30, App. B § I(C)(2)(a); 12 C.F.R. § 225, App. F § I(C)(2)(a); 12 C.F.R. § 364, App. B § I(C)(2)(a).

Mr. Chairman, we commend the Committee's interest in strengthening protections against identity theft. Thank you for inviting me to discuss this topic. I look forward to answering your questions.

Biography: Bestor Ward

Bestor Ward, president of Ward Properties, Inc., graduated from Auburn University in 1980 with a degree in marketing. Ward worked for a local bank before entering into the commercial real estate industry working for White-Spunner Commercial Development. In 1989 he joined the family-owned business, Bedsole Investment Company, Inc. which has been in continuous business in Mobile since 1928. Later he acquired the majority of the company stock and changed the name to Ward Properties, Inc. Safe Archives – Safe Shredding is a wholly owned subsidiary of Ward Properties, Inc. Ward and the Safe Archives - Safe Shredding team have become the leader in secure, quality service for records management, media storage and information destruction in the Greater Mobile Metropolitan area.

Since forming Safe Archives – Safe Shredding, Ward has become passionate about the records management industry and has become a champion of the business by educating himself and his team about business safety and security on records management issues. After receiving the counsel of numerous top industry consultants and attending industry training, Ward has become a subject-matter expert. Recently, the National Association of Information Destruction (NAID), the group known for setting the standards for the information destruction, appointed Ward to their national Governmental Affairs Committee.

Ward has extensive Civic and Business affiliations throughout Mobile and the State of Alabama and he has served on the board of many organizations including The Mobile Area Chamber of Commerce, The Rotary Club of Mobile and The J.L. Bedsole Foundation and AmSouth Bank N.A.

Safe Archives- Safe Shredding parent company, Ward Properties, Inc., has been doing business along the northern Gulf Coast since 1928 and has an extensive history of community involvement and support.

Updated 04/21/2005

United States House of Representatives
Committee on Financial Services

"Truth in Testimony" Disclosure Form

Clause 2(g) of rule XI of the Rules of the House of Representatives and the Rules of the Committee on Financial Services require the disclosure of the following information. A copy of this form should be attached to your written testimony.

1. Name:	2. Organization or organizations you are representing:
T. Bestor Ward, III	Gulf Coast Records Management, LLC AND National Association for Information Destruction (NAID)
3. Business Address and telephone number:	
PO Box 81366 Mobile, AL 36689 (251) 342-0400	450 St. Louis Street Mobile, AL 36602
4. Have you received any Federal grants or contracts (including any subgrants and subcontracts) since October 1, 2004 related to the subject on which you have been invited to testify?	**5. Have any of the organizations you are representing received any Federal grants or contracts (including any subgrants and subcontracts) since October 1, 2004 related to the subject on which you have been invited to testify?**
☐ Yes ☒ No	☐ Yes ☒ No
6. If you answered "yes" to either item 4 or 5, please list the source and amount of each grant or contract, and indicate whether the recipient of such grant was you or the organization(s) you are representing. You may list additional grants or contracts on additional sheets.	
7. Signature:	

Please attach a copy of this form to your written testimony.