STATEMENT OF

GILBERT T. SCHWARTZ

ON BEHALF OF THE

AMERICAN COUNCIL OF LIFE INSURERS

HEARING ON EXAMINING THE FINANCIAL SERVICES INDUSTRY'S RESPONSIBILITIES AND ROLE IN PREVENTING IDENTITY THEFT AND PROTECTING SENSITIVE FINANCIAL INFORMATION

BEFORE THE

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

UNITED STATES SENATE

SEPTEMBER 22, 2005

INTRODUCTION

Chairman Shelby, Ranking Member Sarbanes and Members of the Committee, I am Gilbert Schwartz, partner in the Washington D.C. law firm of Schwartz & Ballen LLP. I am appearing before the Committee today on behalf of the American Council of Life Insurers ("ACLI") to discuss the life insurance industry's responsibilities and role in preventing identity theft and protecting sensitive financial information.

ACLI is the principal trade association for the nation's life insurance industry. ACLI's 356 member companies account for 80 percent of the life insurance industry's total assets in the United States. ACLI member companies offer life insurance, annuities, pensions, long-term care insurance, disability income insurance, reinsurance and other retirement and financial protection products.

This hearing represents another chapter in this Committee's long-standing commitment to the protection of consumer information and to the prevention of identity theft, as evidenced by the Committee's central role in the enactment of the Gramm-Leach-Bliley Act (the "GLB Act") and the Fair and Accurate Credit Transactions Act of 2003 (the "FACT Act"). ACLI appreciates the opportunity to discuss with the Committee the important role that life insurers play in protecting sensitive financial information of our policyholders and in preventing identity theft.

BACKGROUND

The issue of preserving the confidentiality and security of customer information is a critically important matter for our country. It is significant not only to the nation's economic well-being, but also to insurers and other financial institutions that use this information to provide vital services to our country's consumers. Due to the inherent nature of the life insurance business, ACLI member companies obtain and maintain sensitive personal information about their policyholders and insureds. The life insurance industry has long recognized the importance of maintaining and protecting the confidentiality and security of this information and ensuring that it is not otherwise compromised.

Life insurers have long been committed to establishing and maintaining processes that protect sensitive customer information and to preventing misuse of such information. Insurers expend considerable resources to achieve these objectives. They recognize that policyholders expect insurers to protect their confidential personal information. Life insurers' recognition of the need to protect customer information predates enactment of the GLB Act. Indeed, ACLI and its members were, and continue to be, strong supporters of Title V's privacy provisions.

THE GRAMM-LEACH-BLILEY ACT

Title V of the GLB Act sets forth the Congressional policy that every financial institution has an affirmative and continuing obligation to protect the security and confidentiality of personal information of its customers. The institution's primary supervisor is required to establish appropriate safeguards relating to administrative, technical and physical safeguards to ensure the security and confidentiality of such information, to protect against anticipated threats or hazards to the security or integrity of the information and to protect against unauthorized access to, or use of, such records that could result in substantial harm or inconvenience to customers.

The Federal agencies with supervisory authority over financial institutions have adopted comprehensive guidance or rules implementing the GLB Act's data security provisions.[1] In addition, thirty-four States have adopted comprehensive regulations or statutes which establish standards for safeguarding customer information by insurers. The State requirements generally track the National Association of Insurance Commissioners' Standards for Safeguarding Customer Information Model Regulation and are consistent with the Federal guidance.

Under State law and regulation, life insurers are required to implement a comprehensive written security program that includes administrative, technical and physical safeguards for the protection of customer information. The program must be

[1] *See* 66 *Fed. Reg.*8615 (February 1, 2001) (Office of the Comptroller of the Currency, Federal Reserve Board, Federal Deposit Insurance Corporation and Office of Thrift Supervision); 66 *Fed. Reg.* 8152

appropriate to the size and complexity of the insurer and to the nature and scope of its activities. The program must also be designed to ensure the security and confidentiality of customer information, protect against any anticipated threats or hazards to the security or integrity of customer information, and protect against unauthorized access to, or use of, customer information that could result in substantial harm or inconvenience to customers. Insurers also require that companies from which they receive operational services maintain rigorous information security programs that meet the requirements of the GLB Act.

IDENTITY THEFT AND THE FACT ACT

Consumers are very concerned with the issue of identity theft. The Federal Trade Commission has reported that the number of identity theft complaints rose to almost 250,000 in 2004, an increase of 15% from 2003. Identity theft accounted for 39% of the total number of consumer complaints, topping the list of consumer frauds reported by the Federal Trade Commission by an overwhelming margin.[2]

Congress enacted the FACT Act, in part, to respond to the growing crime of identity theft. It directs Federal regulators to develop guidance to identify and prevent identity theft. The Federal agencies have proposed and adopted several regulations and provided guidance to deter identity theft. We anticipate that additional guidance

---

(January 30, 2001) (National Credit Union Administration); and 67 *Fed. Reg*. 36484 (May 23, 2002) (Federal Trade Commission).

[2] "National and State Trends in Fraud & Identity Theft, January-December 2004," Federal Trade Commission, February 1, 2005.

will be forthcoming to educate consumers and the financial industry as to how to reduce the incidence of identify theft.

BREACH OF SECURITY NOTICES

As a result of growing concerns with the possibility of identity theft resulting from security breaches of information systems, twenty States have enacted legislation requiring companies to notify consumers in the event their sensitive personal information is affected by a security breach of their information systems. Additional States are considering legislation as well. These statutes typically require disclosure of a breach of security of the computer system to the person whose unencrypted sensitive information was or is reasonably believed to have been compromised. Generally, notice is not required if after reasonable investigation it is determined that there is no reasonable likelihood of harm to customers.

Some States have adopted requirements that differ in certain key respects. The need to track these differences and factor them into a notification program will inevitably make it more difficult for institutions to send notices to consumers promptly. The complexity resulting from differing State requirements will likely mean that consumers may experience delays in receiving timely notices. Moreover, State laws may also result in overlapping enforcement mechanisms, which increases the likelihood of uneven enforcement policies from State to State.

FEDERAL BANKING AGENCY GUIDANCE

In March, 2005, the Federal banking agencies amended their interagency guidance on information security safeguards to require banking organizations to adopt response programs in the event of unauthorized access to customer information.[3] Under the agency guidance, depository institutions are required to develop and implement risk-based response programs to address incidents of unauthorized access to customer information in customer information systems. The guidance requires that if, after conducting a reasonable investigation, a depository institution determines that misuse of sensitive customer information has occurred or is reasonably possible, it should notify the customer as soon as possible. Customer notice may be delayed if law enforcement authorities request a delay so as not to interfere with their criminal investigation.

The notification requirement focuses on sensitive customer information because this type of information is most likely to be misused by identity thieves. Sensitive customer information is regarded as the customer's name, address or telephone number in conjunction with a Social Security number, driver's license number, credit or debit card account number or password or PIN that would allow someone to access the customer's account.

[3] 70 *Fed. Reg.* 15736 (March 29, 2005)

POSSIBLE FEDERAL LEGISLATION

Uniform Nationwide Protections

ACLI supports Federal legislation that provides uniform national standards for notification to individuals whose personal information has been subject to a security breach. ACLI member companies believe it critical that the substantive requirements of Federal security breach notification legislation preempt State or local laws or regulations addressing any aspect of this subject matter.

When a security breach occurs, it is important that the institution that maintained the sensitive information move quickly to investigate the nature of the breach, determine the likelihood that information may have been misused and notify customers. The proliferation of State laws that impose similar but varying requirements could result in a delay in notifying consumers while separate notices are developed for consumers who are located in States with non-uniform standards. Varying State requirements, therefore, could have an adverse effect on consumers and increase the likelihood that consumers will be victimized by identity thieves. Accordingly, ACLI urges Congress to establish uniform preemptive guidelines that will apply nationwide. Such an approach will be beneficial to consumers because it will ensure that consumers receive the same information in a timely fashion regardless of where they reside.

Sensitive Consumer Information

ACLI believes that the Federal banking agencies and the States are correct in focusing attention on notice to consumers in connection with breaches of security of unencrypted or unsecured sensitive consumer information, such as a person's name and address when combined with such information as account number or Social Security number. While databases may contain other personal information about their customers, much of the information is of little or no value to identity thieves. Accordingly, ACLI recommends that security breach legislation apply only to sensitive consumer information obtained by an unauthorized person if the information is not encrypted or secured by a method that renders the information unreadable or unusable.

ACLI also believes that it is important that Federal security breach notification legislation apply to all businesses that maintain sensitive consumer information. Consumers should be protected regardless of the nature of the business that maintains their sensitive information.

Likelihood of Harm

ACLI member companies support legislation that avoids needlessly alarming consumers and undermining the significance of notification of a security breach by requiring notification only when the security and confidentiality of personal information is truly at risk. If the primary purpose of security breach legislation is to alert consumers to the possibility that their sensitive personal information may be

subject to identity theft, it makes good sense to require companies to inform consumers only when there is a significant likelihood of identity theft. If there is little chance of identity theft or substantial harm, why needlessly alarm consumers when personal information is not at risk.

Enforcement and Rulemaking

It is also very important that there be uniform enforcement of notification standards. For this reason, ACLI strongly supports enforcement of insurers' compliance with security breach legislation exclusively by the Department of the Treasury. The Treasury Department has extensive experience with the insurance industry in connection with the implementation and enforcement of laws such as the U.S. Patriot Act, the Terrorism Risk Insurance Act and the Bank Secrecy Act, as well as regulations promulgated by the Office of Foreign Asset Controls. As a result of this experience, ACLI believes that the Treasury is well positioned to implement and enforce the insurance industry's compliance with security breach notification legislation.

In the event it is not possible to provide for enforcement jurisdiction by the Treasury Department, ACLI recommends adoption of the enforcement structure set out in the GLB Act. Under this approach, an insurer's compliance with Federal breach of security notification legislation would be enforced exclusively by the insurance authority of the insurer's state of domicile. If this approach is used,

ACLI also requests that the legislation state that it is the intent of the Congress that State insurance authorities enforce the legislation in a uniform manner.

If Federal security breach notification legislation provides for promulgation of implementing regulations, ACLI believes that the legislation should provide for the promulgation of uniform standards jointly by the relevant Federal agencies. Such an approach ensures that guidance will be applied uniformly across all industries and that the special needs of each sector of the economy will be taken into account and carefully considered. Adoption of joint standards has the added benefit of avoiding potential confusion among consumers because it provides certainty as to what consumers can expect to receive from companies that possess their sensitive information.

CONCLUSION

The issues you have before you today are indeed complex. They should be carefully studied and considered, as you are doing. ACLI anticipates that legislation you adopt will provide meaningful protection to consumers who might otherwise become victims of identity theft.

Thank you for your attention.