**WRITTEN TESTIMONY OF EUGENE FOLEY**
**PRESIDENT AND CEO OF HARVARD UNIVERSITY EMPLOYEES CREDIT UNION**

**ON**

**"ASSESSING DATA SECURITY: PREVENTING BREACHES AND PROTECTING SENSITIVE INFORMATION"**
**BEFORE THE HOUSE COMMITTEE ON FINANCIAL SERVICES**
**MAY 4, 2005**

**WRITTEN TESTIMONY OF EUGENE FOLEY**
**PRESIDENT AND CEO OF HARVARD UNIVERSITY EMPLOYEES CREDIT UNION**
**ON**
**"ASSESSING DATA SECURITY: PREVENTING BREACHES AND PROTECTING SENSITIVE INFORMATION"**
**BEFORE THE HOUSE COMMITTEE ON FINANCIAL SERVICES**
**MAY 4, 2005**

Mr. Chairman, members of the committee; my name is Eugene Foley and I am the President and CEO of Harvard University Employees Credit Union, located in Cambridge, Massachusetts. I am here today to express concern about the implications and escalating problem that theft of sensitive information resulting from data security breaches is having on American consumers, credit union members, and the institutions that issue credit cards and debit cards, most especially credit unions and small banks. Collectively, about 4,600 credit unions in this country have issued and support over 12.5 million card accounts for our members.

I have experience with this issue not only as the CEO of a credit union that had about 700 of our 10,000 card accounts compromised in one incident last year, but also as a recent victim of identity theft myself. While I was sitting in my office, with my own debit card securely in my wallet, my checking account was cleaned out by a series of card purchases made 3,000 miles away. In a matter of minutes, over $2,000 was stolen from my account. Given my position, I am particularly responsive in protecting my own sensitive information, but this caution is meaningless when entities that have captured and retained the data contained on the card stripe are careless or not compliant with security standards.

The frequency of major card data compromises is increasing at an alarming rate. Within the past two weeks alone, we have read of three major breaches which have compromised the accounts of millions of American consumers. The first major security breach to have an impact on credit unions came to light last year as result of hackers stealing a large amount of consumer information from the retailer, BJ's Wholesale Club. This case exemplifies a merchant in direct violation of card association rules and regulations. While card issuers fastidiously comply with protecting sensitive account data, the resources they expend in this effort are squandered if merchants are not held to the same standard.

A recent article in the *Wall Street Journal* cited a $5.7 million lawsuit filed last month against BJ's Wholesale Club by CUNA Mutual Insurance Corporation on behalf of 163 credit union bond holders. Millions of dollars were lost by credit unions in the security breach at BJ's alone. These costs include not only the amounts lost to fraud, but also the

costs for reissuing and blocking cards, for notifying card holders and monitoring accounts. There are card association rules in place regulating how the consumer

information which is imbedded on the magnetic stripe on the back of each card should be handled, but these rules have proven to be both insufficient and laxly enforced. Absent card association enforcement or legislative redress, credit unions have had to resort to litigation in order to find remedy for these losses.

The surest way to limit the potential damage when a merchant's files are hacked and a large base of credit card information is stolen is to cancel the existing cards and reissue new cards with new account numbers. As small banks and credit unions hold a close relationship with their card holders, this is most often the action they take. This is a very costly and time consuming undertaking. Unfortunately protecting the consumer also carries another very substantial penalty by causing the consumer to question the safety and security of the card issuer rather than the merchant who has inadequately safeguarded their personal information. The card issuer is unfairly exposed to the majority of this "reputation risk" in addition to actual monetary costs.

Even after a breach has been identified by the merchant, issuing institutions can not count on getting accurate and timely notification to pass along to the consumer. Most times, the issuer is relying on reports in the media to determine the nature of the breach. Without accurate information, it is impossible to appropriately inform our members how their information was stolen and they are often left with the impression that the credit union is at fault.

The California General Assembly undertook steps to provide this type of protection in a law that became effective on July 1, 2003. While we have had the benefit of seeing that law in action for nearly two years and their experience offers us some guidance, there is room for improvement.

It is our hope that the committee will put its authority and energy behind initiatives that will require the major credit card companies to notify financial institutions immediately in an electronic format that is usable for the effected issuer. That information should include: when a breach occurred, which merchant is responsible for that breach and which accounts are affected. It should also detail what type of personal information was compromised.

Specifically, any new statute would benefit from explicit definitions. For example, clarity with regard to which businesses would be covered, along with what constitutes personal information, are areas where the California statute has been questioned. Of particular concern is an exclusion that the California law provides for encrypted data. Unfortunately advances in hacking seem to match advances in encryption technology and those that can breach credit card files are quite likely to be able to gain access to decryption technology.

In addition, to ensure that all consumers have the utmost protection from this insidious threat, we believe that all credit card issuers should be required to at least inform consumers when their credit card has become compromised and their personal financial information has been stolen. Those consumers should then have the right to determine if they wish to have their cards cancelled and reissued, in a timely fashion, at no cost.

Mr. Chairman and members of the committee, I thank you for affording me the opportunity to share my thoughts on this subject with you.