STATEMENT OF SENATOR JON KYL
CHAIRMAN
SUBCOMMITTEE ON TERRORISM, TECHNOLOGY, AND HOMELAND SECURITY
SENATE JUDICIARY COMMITTEE
4 NOVEMBER 2003

Introduction

The theft by a computer hacker of a person's Social Security number, driver's license, or financial information can be devastating. A criminal can use this information to cause great financial harm.

S. 1350

Senator Feinstein's bill, S. 1350, the "Notification of Risk to Personal Data Act," addresses the duty of a business maintaining a computerized database with customers' sensitive personal information to inform customers of a hacking incident that compromises personal financial data.

Under the bill, notice would be triggered if the hacker obtained access to a customer's (1) Social Security number, (2) driver license number, or (3) bank account, debit, or credit card number.

Notice would be provided to individuals (1) in writing, (2) through e-mail, or (3) by substitute notice. Substitute notice can be used to prevent undue burdens on agencies or companies. Substitute notice includes notice by e-mail, the posting of notice on the company, or agency website or the notification of major media. Substitute notice is triggered if any of the following factors exist:

> (i) the business demonstrates that the cost of providing direct notice would exceed $250,000;
>
> (ii) the business of subject persons to be notified exceeds 500,000; or
>
> (iii) the business does not have sufficient contact information to notify people whose information is at risk.

Finally, under the bill, the Federal Trade Commission is empowered to fine entities $5,000 per violation or up to $25,000 per day while the violation persists. State Attorneys General can enforce the statute. Inconsistent state laws are preempted, but California's legislation is grandfathered-in.

Witnesses

Today, the Technology subcommittee will hear from three expert witnesses:

- The first witness is from my home state of Arizona. David McIntyre is the President and CEO of TriWest Healthcare Alliance. Mr. McIntyre has a distinguished career in both health care policy and operations. Earlier this year, he guided TriWest in its successful bid for the Defense Department's new West Region, serving military members, retirees, and their families in 21 Western states — including our ranking Member's state of California — a total of 2.6 million beneficiaries in all.

  Mr. McIntyre will testify about the December 2002 break-in at its Phoenix, Arizona offices. Thieves broke into a management suite and stole laptop computers and computer hard drives containing the names, address, telephone numbers, birth dates, and Social Security numbers of 562,000 military service members, dependents, and retirees. The thieves also stole medical claims records for people on active duty in the Persian Gulf. The potential harm to a group this large, particularly to those who wear the uniform of this country, was staggering. Yet, to date, not a single individual has suffered identity theft as a result of the crime against TriWest.

  Mr. McIntyre, we look forward to your description of those events and how your company responded to such a major information theft.

- Mark MacCarthy, the Senior Vice President of Public Policy for Visa will testify about the steps that VISA takes to avoid database security breaches and how VISA notifies its customers of any security breech. He will also comment on S.1350.

- Evan Hendricks, Editor, Privacy Times, will testify about the rise of database security breaches, the types of information stolen from databases, the failure to notify consumers of such breaches, and the value of notification.

Closing

In closing, I would like to note that the record will be kept open for one week for questions and for additional statements.

I would like to thank Senator Feinstein for her hard work in putting together this hearing. On this issue and every issue before the subcommittee she has worked diligently and has been a great pleasure to work with.

#