TECHNOLOGY POLICY INSTITUTE

Studying the Global Information Economy

"Slow Down on Data Security Legislation."

Thomas M. Lenard and Paul H. Rubin

August 2005

1747 PENNSYLVANIA AVENUE NW ▫ SUITE 850 ▫ WASHINGTON, D.C. 20006
PHONE: 202.828.4405 ▫ E-MAIL: info@techpolicyinstitute.org ▫ WEBSITE: www.techpolicyinstitute.org

THE PROGRESS & FREEDOM FOUNDATION

Progress Snapshot

Release 1.9 August 2005

This article appeared in the San Jose Mercury News on August 19th, 2005.

Slow Down on Data Security Legislation

By Thomas M. Lenard and Paul H. Rubin*

A series of high-profile data-security breaches exposing millions of credit card accounts to fraud has convinced the public that we are facing an epidemic of identity theft. Understandably, politicians are responding by introducing data-security bills at a rapid clip and legislation may well be enacted before the end of the year. As Sen. Arlen Specter, R-Pa., co-sponsor of one of the major bills said, "We're not dealing with a highly controversial subject where there will be significant differences of opinion."

Perhaps the subject should be more controversial, because it is not well-understood.

For one thing, the perception that identity theft is a growing problem is not supported by the data. A study commissioned by the Federal Trade Commission and a similar follow-up study show that identity theft actually declined between 2003 and 2004, though not by a statistically significant amount. Another study found that over a relatively long period -- 1992 to 2004 -- the cost of credit card fraud to card issuers has declined from 15.7 cents to 4.7 cents per $100 in credit card sales.

Indeed, the credit card companies are developing increasingly sophisticated technologies for reducing their losses, which also reduces the losses to individuals. This is because more than 90 percent of the $55 billion in annual costs due to identity theft are incurred by businesses, according to the FTC.

While the market seems to be addressing the data-security problem, the proposed regulatory solutions are of dubious merit on cost-benefit grounds. A major part of virtually all the legislative proposals is a requirement that consumers be notified when a security breach occurs that might compromise their personal data. But our analysis, based on the FTC's data, shows that the expected benefits to consumers of a notification requirement are extremely small -- less than $10 per individual whose data have been compromised. This is for several reasons. First, only a very small percentage of individuals compromised by security breaches -- perhaps 2 percent, according to a Visa estimate -- actually become victims of a fraud. Second, two-thirds of these are victims of fraudulent charges on their existing credit accounts, for which they have very

* Thomas M. Lenard is vice president for research at the **Progress & Freedom** Foundation. Paul H. Rubin is a professor of economics and law at Emory University and an adjunct fellow at PFF. Both authors have held senior positions at the Federal Trade Commission and other government agencies.

limited liability -- a maximum of $50 and usually nothing -- rather than victims of true identity theft. And, finally, even a well-designed program will eliminate only 10-20 percent of the expected costs.

The major regulatory costs to be concerned about are not the direct costs of notification. Rather, they are the costs incurred when individuals and firms overreact and take actions that are harmful either to themselves or to the free flow of information.

Individuals, for example, may be induced to place fraud alerts on their accounts or close them entirely, actions likely to be far more costly than being an identity-theft victim. A continual stream of warnings may also induce individuals to shift their credit transactions offline, which would actually increase their exposure to identity theft. In fact, a recent study concludes that "the single most-effective approach to protect against both external and domestic identity theft is to turn off all paper bills and statements."

Firms, for their part, may overreact by cutting back the information they make available and this already seems to be happening. We know that the information provided by firms in the information market is of great value to consumers and the economy. It is the reason, for example, why any individual with a decent credit rating can get a loan approved instantaneously. It also facilitates competition generally, making it easier for new firms to enter markets that require customer data.

This is an area where the United States has a significant advantage over other countries that have more restrictive data and privacy laws. In those countries, the consumer credit market does not work so smoothly. Moreover, fraudulent credit card charges are lower relative to credit card use in the United States than in other countries that have more restrictive laws -- for example, the United Kingdom.

In sum, new data-security legislation may entail large costs for virtually no benefits. We should approach it with a great deal of caution.