



Senator Feinstein Asks Credit Card Companies to Describe Steps to Notify Individuals, Protect them from Identity Theft in Wake of Massive Data Breach
June 17, 2005

Washington, DC – In the wake of a database breach potentially affecting 40 million Americans, U.S. Senator Dianne Feinstein (D-Calif.) today called on the four major credit card companies to describe the steps they are taking to notify individuals of their risk and what additional steps they are taking to protect their customers from identity theft.

Senator Feinstein is the author of three bills currently pending before the Senate including legislation:

- **Creating a national standard on notification**, requiring a business or government entity to notify an individual when there is a hacking incident that compromises personal data.
- **Setting a national standard for protecting personal information** such as Social Security numbers, driver's licenses, and medical and financial data. It requires companies to let consumers "opt in" for their most sensitive information, and "opt-out" for less-sensitive personal information.
- **Prohibiting the sale or display of Social Security numbers to the general public** (without their consent) and to require Social Security numbers to be taken off of public records published on the Internet.

In letters to the CEOs of Visa, MasterCard, American Express, and Discover, Senator Feinstein wrote:

"This weekend's announcement that 40 million credit card accounts have been compromised, including accounts from your company, causes me great concern. It is just the latest in a wave of incidents exposing nearly 58 million Americans to identity theft. I continue to be astonished by the proliferation of data breaches, each one worse than the last.

This incident is a clear sign that industry's efforts to self-regulate when it comes to protecting consumers sensitive personal data are failing. The fact that hackers could have accessed data on up to 40 million accounts because of a processor's failure to follow your own established rules makes me question the effectiveness and ability of self-regulation by your industry.

I would like to know what steps MasterCard International is taking to notify individuals affected by this breach?

In light of this latest breach, I believe that notification is vital to affording individuals the ability to protect their identity and their credit.

As you may know, I have introduced legislation which would set a national notification standard in the event of a data breach. The “Notification of Risk to Personal Data Act” (S. 751) would establish a national notification standard requiring the federal government and businesses to notify individuals when there has been a security breach which has compromised their sensitive personal data, such as Social Security numbers, driver’s license or state identification card numbers, or, financial account information.

In addition to knowing what steps you are taking to notify affected individuals, I would also like to know what additional efforts MasterCard International is taking to protect consumers against identity theft – aside from the current practice of not charging consumers for any unauthorized charges? For instance, a prudent step might be closing all compromised credit card accounts and issuing new cards with new account numbers.

I look forward to your speedy response.”

###