PROTECT YOURSELF.

In today's world, despite consumers realizing the need to become more vigilant in scrutinizing emails received from retailers or banks, an email that is not caught by a spam filter can cause a false sense of security, leading a person to believe it's from a legitimate source. These emails then request more personal information or prompt the consumers to update their account, on a site set up by the hackers. Once they have passwords to bank accounts or retailers, they can clean out accounts or make fraudulent purchases. This practice is known as "spear-phishing."

Unfortunately, these types of cyber-attacks can happen at any time, but there is a two step process available to you that will help safeguard your name and credit history:

1 Register your credit cards online with Card Patrol provided by Assist America.

We will continuously monitor underground web and chat sites that specialize in selling and trading identity information. If your data appears, you will be immediately notified and assisted in taking steps to help prevent fraudulent use of your information in the future. This service, called Card Patrol, uses state-of-the art encryption and security to safeguard your data. Register now through **http://www.assistamerica.com/Identity-Protection/Login.aspx**

2 Register your credit cards by phone with Lost and Stolen Assistance.

By calling Identify Theft Protection's 24/7 toll-free number, a member can store information from credit cards, banks and important documents in one safe, centralized location. If any of the registered items become lost or stolen, retrieving the information is fast and simple and the resolution process of canceling and replacing the cards and documents can begin immediately simply by calling Assist America's Identity Protection number: **1-877-409-9597 or if calling from overseas: 1-614-823-5227**.

You can also take some steps on your own to make sure any future database breaches won't affect you.

- **Get out of marketing databases**.
Go to www.privacyrights.org to see which data brokers are selling your name and explore each broker's opt out policy.
- **Unsubscribe from any commercial lists you're on**.
All commercial lists are required to give you an "unsubscribe" option link which is usually found at the bottom of their emails.
- **Stop most direct mail**.
Go to www.dmachoice.org and sign up to opt out of various offers for a 5 year time period.
- **Stop your bank from sharing your name**.
You must provide your bank with notification, in writing, that
you do not give them permission to sell your name to any of its affiliates.
- **Stop phone calls from telemarketers**.
Sign up with the National Do Not Call registry at www.donotcall.gov.
- **Opt out of credit card offers**.
You can stop receiving them by signing up at www.optoutprescreen.com. This free service is run by the consumer credit reporting industry.

**To find the full list of the companies affected go to www.DataBreaches.net.*

assist america®