

## Epsilon Security Breach Could Affect Millions

Check your email carefully. If you receive messages claiming to be from your bank or another company you do business with, they may not be!

Dallas-based online marketing firm Epsilon, a subsidiary of Alliance Data Systems Corp., announced on April 1st that a security breach exposed the names and email addresses of potentially millions of customers of U.S. banks, retailers and other companies. Some of the companies affected include Capital One Financial Corp, Barclays Bank, U.S. Bancorp, Citigroup Inc., JP Morgan Chase, Disney Co., Best Buy, Hilton Worldwide, Ethan Allen Interiors, Home Shopping Network, Marriott International, TiVo Inc., Walgreens and Kroger Co.

While no financial information was compromised, the concern is that scam artists could use the exposed information to target unsuspecting consumers via “phishing” emails. Phishing emails claim to be from a business or retailer you do business with and may look legitimate, however, the emails are used to get you to reveal personal information, such as account numbers, passwords, Social Security number and other sensitive data.



For more information about fraud and identity theft and how to protect yourself, call the Office of Consumer Affairs and Business Regulation’s Consumer Hotline at 617-973-8787 or 888-283-3757 (toll free in MA) or visit our website at [IdentityTheft.com](http://IdentityTheft.com). Also see the Federal Trade Commission’s website for more information on Identity Theft.

## Tips to Ensure You Don't Reveal Personal Information

1. Don't give your User ID or password in email.
2. Don't respond to emails that require you to enter personal information directly into the email via a link or ask you to send personal information.
3. Don't respond to emails threatening to close your account if you do not take the immediate action of providing personal information.
4. Don't use your email address as a login ID or password.

A word of advice to consumers - NEVER give out your personal account information to anyone unless you initiate the contact.

This includes bank account numbers, credit and debit card numbers, passwords, birth date, Social Security Number or other personally identifying information.