



IDENTITY THEFT ASSISTANCE CENTER

Contact: Kate Ennis
(301) 580-6726

kate@enniscommunications.com

For Immediate Release

DATA BREACH PLANS A NECESSITY FOR EVERY COMPANY HANDLING SENSITIVE CONSUMER INFORMATION

*Although incidence of identity theft is rare, companies must prepare
To protect consumers and maintain confidence*

WASHINGTON, DC, December XX, 2006— Every company that handles sensitive consumer data must have a plan to deal with potential data breaches in order to protect consumers against identity theft and to maintain consumer confidence, according to participants at a recent forum, “Data Breaches: Preparation, Communication and Response,” sponsored by the Identity Theft Assistance Center (ITAC).

“There’s increasing awareness of the different types of risks associated with data breaches including loss of consumer confidence, litigation, and regulation,” said Anne Wallace, executive director of ITAC. “Companies are responding by making major investments to protect data, but we all recognize the bad guys are equally committed to thwarting those protections.”

“Every company has an obligation to look at the way they do business in this regard, from securing data within the organization, to dealing with third parties, such as business partners and vendors,” said Robert Shiflet, senior vice president, Card Services Operations, Bank of America Corp.

The forum featured speakers from government, industry, academia, research organizations, law and public relations to identify trends and to share “best practices” on how to prepare and respond to data breaches. Among the findings were:

- Very few cases of identity theft result from data breaches. As can be expected, deliberate breaches, such as the hacking of a company’s information systems, result in more cases of identity theft than unintentional breaches, such as data stored on a stolen lap top.

- The potential for identity theft depends on the properties of the data that is been breached, e.g., account numbers alone are insufficient to commit identity theft.
- Companies are implementing policies to segregate data to prevent thieves from acquiring sufficient data to perpetrate identity theft.
- There is debate about the best methods to notify consumers in the event of a breach since not all breaches carry the same level of risk. But there is consensus that companies must communicate quickly and candidly with consumers about the circumstances of the breach.
- Companies should have policies and procedures in place regarding data breaches. The internal response team should represent multiple disciplines within the company, including information technology, security, legal and public relations.
- At least 33 states have enacted laws regarding data breaches with varying requirements and definitions. This legal patchwork makes compliance costly and inefficient.

About ITAC

The Identity Theft Assistance Center (ITAC) (www.identitytheftassistance.org) is a cooperative initiative founded by the financial services industry that now welcomes companies in other industries targeted by identity thieves. Since it was established in August 2004, ITAC has helped thousands of consumers restore their financial identities. ITAC shares information with the Federal Trade Commission's Consumer Sentinel database, which can be accessed by more than 1,000 law enforcement agencies nationwide. Part of the ongoing industry focus on combating fraud and identity theft, ITAC is run by the Identity Theft Assistance Corporation, a not-for-profit membership corporation sponsored by The Financial Services Roundtable and BITS.

###