Charles G. Cooper
Commissioner

TEXAS DEPARTMENT OF BANKING

2601 North Lamar Blvd., Austin, Texas 78705
512-475-1300 /877-276-5554
www.dob.texas.gov

INDUSTRY NOTICE 2012-1
Date: January 13, 2012

Supervisory Memorandum 1029: Standards for the Risk Management of Corporate Account Takeovers

The Department of Banking has issued **Supervisory Memorandum 1029** which establishes minimum standards for the Risk Management of Corporate Account Takeovers. The new policy requires banks to implement appropriate practices in the risk management of corporate account takeovers. Examiners will begin reviewing bank implementation efforts in March 2012.

Corporate Account Takeover is a form of corporate identity theft where cyber thieves gain control of a business' bank account by stealing user passwords and other valid credentials. This type of theft has resulted in significant financial harm to Texas banks and their corporate customers. As a result, the Department, in cooperation with the United States Secret Service, formed the Texas Bankers Electronic Crimes Task Force (Task Force) to develop recommended best practices to reduce the risks of electronic crimes such as corporate account takeover. The ***Best Practices for Reducing the Risks of Corporate Account Takeovers*** and other valuable resources are available on the **Texas Bankers Electronic Crimes Task Force** page on the Department's website.

A teleconference on the Practices for Reducing the Risks of Corporate Account Takeover, co-sponsored by Independent Bankers Association of Texas and Texas Bankers Association, and moderated by SWACHA, will be held on January 25, 2012 at 3:00 pm. Registration is necessary to participate in the teleconference.

To view this new policy, go to the **New Actions table** found on the Law & Guidance Manual page of the Department's website. Questions or comments regarding this Supervisory Memorandum should be directed to the **Chief IT Security Examiner** or by **email**.