December 7, 2012

MEDIA RELEASE

Conference of State Bank Supervisors

United States Secret Service

Financial Services-Information Sharing and Analysis Center

State and Federal Authorities Combat Corporate Account Takeover

Washington, DC—State and federal authorities have announced efforts to assist financial institutions in adopting best practices to reduce the risks of corporate account takeover. Corporate account takeover is a form of identity theft where cyber thieves gain control of a business' bank account, often by stealing user passwords and other valid credentials. Once this information is obtained, thieves can then initiate fraudulent wire and ACH transactions.

Recognizing the significant impact of these thefts, the Conference of State Bank Supervisors (CSBS), the United States Secret Service, and the Financial Services-Information Sharing and Analysis Center (FS-ISAC) have adopted best practices for a strong risk-management program to reduce the risks of this type of electronic theft. The practices were developed by the banking industry through a task force formed by the Texas Banking Commissioner and the Secret Service. The task force was composed of operational executives from a diverse group of banks in terms of size, complexity, and market environment so the practices would be useful for all financial institutions. State financial regulators will issue these best practices in their state throughout the coming year.

"Over the last few years, this type of electronic theft has caused significant financial harm to businesses and has impacted communities and financial institutions," said John W. Ryan, President and CEO of CSBS. "These thefts have occurred through banks of all sizes and locations across the nation. But because the financial losses of many of these crimes are often settled between the bank and its corporate customer, there is limited awareness of the extent of these crimes. It is our hope these best practices will do much to make bankers aware of the risks of corporate account takeover and the actions they can take to prevent such theft."

"Cybercriminals pose a legitimate threat to the financial security of both corporations and individuals," said Hugh Dunleavy, Deputy Assistant Director of the Secret Service's Office of Investigations. "Working with partners such as state financial regulators and FS-ISAC, the Secret Service is able to expand the collective understanding of cybercrime and augment prevention, advanced detection, and prosecution efforts of these types of crimes."

"Education and outreach is critical to our efforts to prevent corporate account takeovers," said William Nelson, President and CEO of FS-ISAC. "Together with CSBS and the Secret Service, FS-ISAC will conduct a series of webinars for banks to inform bankers about corporate account takeovers and explain the joint best practices. These webinars will do much to spread the word on corporate account takeovers and mitigate the risks such thefts cause."

More information on corporate account takeovers, including the best practices document, is available at www.csbs.org/ec/cato.

# # #

Media Contacts:
Catherine Woody, CSBS Senior Director of Communications, cwoody@csbs.org or 202.728.5733
U.S. Secret Service Office of Government and Public Affairs, 202-406-5708
Michael Ciota, FS-ISAC at mciota@fsisac.us