Reducing the Risks of Corporate Account Takeover

U.S. Department of Homeland Security
United States Secret Service

PRESS RELEASE
Date: January 17, 2012

Texas Banking Commissioner Charles G. Cooper and Edna J. Perry, Special Agent in Charge of the U.S. Secret Service Dallas Field Office, jointly announced efforts to assist financial institutions in adopting practices designed 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. The stolen funds are sent to a "money mule account" where they are quickly transferred to another account controlled by the thieves. Over the last few years, this type of electronic theft has caused significant financial harm to businesses and has impacted communities and financial institutions. These thefts have occurred through banks of all sizes and locations in Texas and across the nation.

Recognizing the significant impact of these thefts and the importance of reducing the risks of such attacks, the Texas Banking Department, in cooperation with the Secret Service, which is mandated with the mission of suppressing counterfeiting and protecting America's financial payment systems (among other duties), formed the Texas Bankers Electronic Crimes Task Force (Task Force) with a directive to develop and recommend practices to reduce the risk of electronic crimes such as corporate account takeover. The Task Force developed a list of *Best Practices* for a strong risk management program for reducing the risks of this type of electronic theft.

In conjunction with the formation of the Task Force, the Secret Service launched Operation Texas Money Mule to infiltrate the money mule networks and better understand how the criminals worked. Working with various task force member banks and other banks, Operation Texas Money Mule gained insight into the workings of these networks and provided helpful information to the task force for their work. The Secret Service believes that building trusted partnerships among all levels of law enforcement, the private sector, and academia is a proven model for addressing the challenges of securing cyberspace.

Based on the Task Force recommendations, the Texas Department of Banking recently issued minimum standards for the risk management of corporate account takeovers. Texas state-chartered banks are required to implement risk management practices that address these minimum standards.

Two key factors in a strong risk management program are education and communication. The need for cooperative learning and communication between financial institutions and their corporate account holders is reiterated in the *Best Practices.* Corporate account holders can

reduce the risks of these attacks by taking an active role in training their staff and implementing prudent security controls in the use of electronic financial transactions. “Banks and their business account holders must continually change, adapt and improve their security practices as cyber criminals are continually changing their techniques,” said Banking Commissioner Charles G. Cooper.

“Cybercriminals' ability to mount attacks against financial institutions is alarming. However, these problems are not insurmountable,” said Special Agent in Charge Perry. “Working with our established partners, such as the Texas Bankers Electronic Crimes Task Force, 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,”

The Department of Banking and the Secret Service extend their appreciation to all of the participants on the Texas Bankers Electronic Crimes Task Force for cooperatively working together on such an important issue.

More information can be found on the Department of Banking website at www.dob.texas.gov. Electronic thefts, such as corporate account takeovers, should be reported to your local Secret Service field office, and other applicable law enforcement and regulatory agencies.

Charles G. Cooper
Commissioner
Texas Department of Banking

Edna J. Perry
Special Agent in Charge, Dallas Field Office
U.S. Secret Service

# # #

Media Contact:
Wendy Rodriguez, Director of Strategic Support, cato@dob.texas.gov or 877.276.5554