Fields of Opportunities

IOWA DIVISION OF BANKING

TERRY E. BRANSTAD
GOVERNOR
KIM REYNOLDS
LT. GOVERNOR

JAMES M. SCHIPPER
SUPERINTENDENT

# SUPERVISORY MEMORANDUM

**December 18, 2012**

**TO:** All State-Chartered Banks;

**FROM:** James M. Schipper, Superintendent of Banking

**SUBJECT:** Standards for the Risk Management of Corporate Account Takeovers

## Purpose

This Supervisory Memorandum establishes minimum standards for a risk management program to specifically minimize the risks of Corporate Account Takeovers. Hundreds of electronic thefts through Corporate Account Takeover have impacted financial institutions and corporate account holders. Municipalities, school districts, churches, large non-profit organizations, corporate businesses, and any customers that perform electronic transfers are potential targets of cyber thieves. This type of theft can cause significant financial harm on its victims and impact entire communities and financial institutions. This Supervisory Memorandum reinforces the Iowa Division of Banking's position that all financial institutions should identify, develop, and implement appropriate risk management measures for electronic crimes.

## Background

Corporate Account Takeover is a form of corporate identity theft where cyber thieves gain control of a business' bank account by stealing employee passwords and other valid credentials. Thieves can then initiate fraudulent wire and ACH transactions to accounts controlled by the thieves. Businesses with limited or no internal computer safeguards and disbursement controls for use with the financial institution's online banking system are vulnerable to theft when cyber thieves gain access to their computer systems, typically through malicious software (malware). Malware infects a business' computer system not just through 'infected' documents attached to an email but also simply when an infected Web site is visited.

Businesses across the United States have suffered large financial losses over the last few years from these thefts through the banking system. Electronic thefts through financial institutions have ranged from a few thousand to several million dollars[1]. These thefts have occurred in financial institutions of all sizes and locations and may not be covered by the financial institution's insurance. Along with the financial impact, there is also a very high level of

[1] Based on Testimony of Gordon M. Snow, Assistant Director, Cyber Division, FBI, before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit, Washington, D.C., September 14, 2011.

reputation risk for financial institutions.

As a result of these growing thefts, the Iowa Division of Banking has been working with the Conference of State Bank Supervisors, the United States Secret Service, and the Financial Services Information Sharing and Analysis Center (FS-ISAC) to provide a risk mitigation program to assist banks in protecting corporate account holders. The risk mitigation program was developed by an Electronic Crimes Task Force (Task Force) of bankers in Texas working with the US Secret Service, bank trade associations, and a payment processing association. The Task Force was composed of operational executives from a diverse group of banks in terms of size, complexity, and market environment. This is an industry developed program designed specifically to assist other financial institutions.

The Task Force of banking industry executives also developed extensive resources to assists other financial institutions in implementing a risk mitigation program. These include resources such as a sample risk assessment, educational PowerPoint presentations for both employees and customer, and project tracking tool. We have worked with the Conference of State Bank Supervisors to make these available to you at www.csbs.org/ec/cato.

## Overview

The Task Force developed a list of recommended processes and controls which expanded on a three-part risk management framework of: 1) Protect; 2) Detect; and 3) Respond developed by the United States Secret Service, the Federal Bureau of Investigation, the Internet Crime Complaint Center (IC3), and the FS-ISAC[2]. The Task Force also developed *Best Practices for Reducing the Risks of Corporate Account Takeovers* (*Best Practices*) to help financial institutions establish specific practices to implement the recommended processes and controls. The *Best Practices* document is a valuable resource to effectively reduce risk.

As the Task Force was concluding its work related to Corporate Account Takeover, the Federal Financial Institutions Examination Council (FFIEC) released *Supplement to Authentication in an Internet Banking Environment* (FFIEC Supplemental Guidance). The FFIEC Supplemental Guidance, issued on June 28, 2011, reinforces previous FFIEC guidance related to risk management of online transactions and updates regulatory expectations regarding customer authentication, layered security, and other controls related to online activity. The Task Forces' recommended three-part Corporate Account Takeover risk management framework and related controls are similar to controls in the FFIEC Supplemental Guidance and include the minimum expectations conveyed in the FFIEC guidance. However, the Task Force guidance has a more specific focus on reducing the risk of Corporate Account Takeovers and therefore provides additional steps to help protect financial institutions and corporate customers.

## Minimum Standards for a Risk Management Program to Mitigate Risks of Corporate Account Takeover

There are nineteen processes and controls (components) to support the three-part risk management framework of Protect, Detect, and Respond. Management and the board of directors of all financial institution should address each of these nineteen components (attachment A) in a risk management program to mitigate the risk of Corporate Account Takeover. Since the industry Task Force that developed the program included both small and large bank representatives, the required components are broad enough to accommodate the

[2] Refer to the jointly issued "Fraud Advisory for Businesses: Corporate Account Takeover" available on the IC3 website (http://www.ic3.gov/media/2010/corporateaccounttakeover.pdf) or the FS-ISAC website (http://www.fsisac.com/files/public/db/p265.pdf).

unique needs of every financial institution and its customers utilizing online banking services. Financial institutions may adopt any practices to implement the components of Protect, Detect, and Respond. Although the use of the Task Force developed *Best Practices* is optional, it will greatly assist most financial institutions in implementing or expanding practices. The *Best Practices* are cross referenced to each of the components listed below and are attached. If your financial institution does not have any business customers that send electronic instructions to transfer funds, you would only need to complete the risk assessment mentioned in P1 below of this Supervisory Memorandum.

The Iowa Division of Banking is providing the attached documents addressing the Protect, Detect, and Respond framework to assist financial institutions in setting minimum standards for a risk management program to mitigate the risks of Corporate Account Takeover. The Iowa Division of Banking will review the financial institution's program for reducing the risks of these electronic crimes during examinations.

For further information about this memorandum, contact Brad Hart, Bank Analyst, at (515) 281-4014.

Attachment A – Corporate Account Takeover - Minimum Standards for a Risk Management Program
Attachment B – Best Practices - Reducing the Risks of Corporate Account Takeovers