



Department of Commerce

Division of Financial Institutions
John R. Kasich, Governor
Andre T. Porter, Director

SUPERVISORY BULLETIN

January 29, 2013

To: All Ohio-Chartered Depositories
From: Charles J. Dolezal, Superintendent
Subject: Standards for Risk Management of Corporate Account Takeovers

Purpose

This Supervisory Bulletin provides background information and establishes minimum standards for a risk management program to specifically minimize the risks of Corporate Account Takeover (CATO). Ohio chartered institutions have not been immune to electronic theft through Corporate Account Takeover. Business customers of varying types and sizes who utilize online banking services for electronic transfers provided by depository institutions are potential targets of cyber thieves. This type of theft can cause significant harm on its victims and impact communities and financial institutions. This Supervisory Bulletin reinforces the Division's position that all Ohio chartered depositories should be aware of the growing risks of electronic crimes, and the need to identify, develop, and implement appropriate risk management measures.

Background

CATO is a form of business 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 from legitimate bank accounts. Businesses with limited or no internal computer safeguards and disbursement controls for use with the 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 a malicious Web site is visited.

The Division is recommending that all Ohio-chartered depositories adopt and implement risk management practices developed by the Texas Bankers Electronic Crimes Task Force (Task Force) that included the Texas Banking Department and the United States Secret Service to mitigate the risks of electronic crimes such as corporate account takeover. The Task Force developed 19 recommended processes and controls which expand on a three part risk management framework of: 1) Protect; 2) Detect; and 3) Respond. This framework was previously developed by the United States Secret Service, the Federal Bureau of Investigation, the Internet Crime Complaint Center (IC3), and the Financial Services Information Sharing and Analysis Center (FS-ISAC)¹.

¹ Refer to the jointly issued "Fraud Advisory for Business: Corporate Account Takeover on the IC3 website <http://www.ic3.gov/media/2010/CorporateAccountTakeOver.pdf>

The Division is also recommending that all Ohio depository institutions review and implement where appropriate the associated *Best Practices for Reducing the Risks of Corporate Account Takeovers* (Best Practices) to help banks establish specific practices to implement the recommended processes and controls. The Best Practices document is intended to amplify the 19 components and is a valuable resource to effectively reduce risk. For more information on the best practices please go to <http://www.csbs.org/ec/cato/Pages/catorecom.aspx>

The Federal Financial Institutions Examination Council (FFIEC) released *Supplement to Authentication in an Internet Banking Environment* (FFIEC Supplemental Guidance) on June 28, 2011, which reinforces their previous 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 Division's recommended three-part CATO risk management framework and related controls are similar to controls in the FFIEC Supplemental Guidance and include the practices recommended by the FFIEC guidance. The Division's guidance differs from the FFIEC Supplemental Guidance in that it has a more specific focus on reducing the risk of CATO and therefore provides additional steps to implement.

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

There are 19 process and control components to support the three-part risk management framework of protect, detect, and respond. Management and the Board of Directors of Ohio depository institutions should address each of these 19 components in a risk management program to mitigate the risks of corporate account takeover. These 19 components are broad enough to accommodate the needs of depository institutions of varying asset size that provide business customers on-line account access and funds transfer services.

The minimum standards for a risk management program to mitigate the risks of corporate account takeover are as follows:

Protect

Implement processes and controls to protect the financial institution and corporate customers by:

- Expanding the risk assessment to include CATO.
- Rating each customer (or type of customer) that performs online transactions.
- Developing an outline for the Board of Directors regarding CATO issues.
- Communicating basic online security practices for corporate online banking customers.
- Implementing or enhancing customer security awareness education for retail and high risk business account holders.
- Establishing institution controls to mitigate risks of corporate accounts being taken over.
- Reviewing customer agreements.
- Contacting your vendors to regularly receive information regarding reducing the risk of CATO.

Detect

Establish monitoring systems to detect electronic theft and educate employees and customers on how to detect a theft in progress by:

- Establishing automated or manual monitoring systems.
- Educating employees of warning signs that a theft may be in progress.
- Educating account holders of warning signs of potentially compromised computer systems.

Respond

Prepare to respond to an incident as quickly as possible (measured in minutes, not hours) to increase the chance of recovering your customer's money by:

- Updating your incident response plans to include CATO.
- Immediately verifying if a suspicious transaction is fraudulent.
- Immediately attempting to reverse all fraudulent transactions.
- Sending a "Fraudulent File Alert" through FedLine.
- Immediately notifying the receiving institution(s) of the fraudulent transactions and asking them to hold or return the funds.
- Implementing a contingency plan to recover or suspend any systems suspected of being compromised.
- Contacting law enforcement and regulatory agencies once the initial recovery efforts have concluded.
- Implementing procedures for customer relations and documenting recovery efforts.

Division examination staff will be reviewing implementation efforts for reducing the risks of electronic crimes through on-site examinations. These reviews will focus on the 19 components in this memorandum as well as the FFIEC Supplemental Guidance.

For further information or questions about this memorandum, please contact Khozema Doctor, Information Technology Examination Supervisor at (740) 513-6645, or Jamie Heath, Review Examiner-Credit Unions at (614) 466-8996, or Sheila Schroer, Chief Examiner-Banks and Savings Institutions at (614) 644-6228.