

Attachment A

Corporate Account Takeover - Minimum Standards for a Risk Management Program

PROTECT

Implement processes and controls to protect the financial institution and corporate customers.

- P1.** Expand the risk assessment to include corporate account takeover.
- P2.** Rate each customer (or type of customer) that performs online transactions.
- P3.** Outline to the Board of Directors the Corporate Account Takeover issues.
- P4.** Communicate basic online security practices for corporate online banking customers.
- P5.** Implement/Enhance customer security awareness education for retail and high risk business account holders.
- P6.** Establish bank controls to mitigate risks of corporate accounts being taken over.
- P7.** Review customer agreements.
- P8.** Contact your vendors to regularly receive information regarding reducing the risk of Corporate Account Takeovers.

DETECT

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

- D1.** Establish automated or manual monitoring systems.
- D2.** Educate bank employees of warning signs that a theft may be in progress.
- D3.** Educate 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 the money for your customer.

- R1.** Update incident response plans to include Corporate Account Takeover.
- R2.** Immediately verify if a suspicious transaction is fraudulent.
- R3.** Immediately attempt to reverse all suspected fraudulent transactions.
- R4.** Send a "Fraudulent File Alert" through FedLine.
- R5.** Immediately notify the receiving bank(s) of the fraudulent transactions and ask them to hold or return the funds.
- R6.** Implement a contingency plan to recover or suspend any systems suspected of being compromised.
- R7.** Contact law enforcement and regulatory agencies once the initial recovery efforts have concluded.
- R8.** Implement procedures for customer relations and documentation of recovery efforts.