Bank Name

To: Board of Directors

From: Bank Employee Name, Title

Date: Month Date, Year

Re: **Corporate Account Takeover**

Please find the attached report on security measures and controls implemented by Bank Name for corporate account takeover risks.

**Corporate Account Takeover Description**

Corporate account takeover is a type of fraud where thieves gain access to a business’ finances to make unauthorized transactions, including transferring funds from the company, creating and adding new fake employees to payroll, and stealing sensitive customer information that may not be recoverable.

Cyber thieves target employees through phishing, phone calls, and even social networks. It is common for thieves to send emails posing as a bank, delivery company, court or the Better Business Bureau. Once the email is opened, malware is loaded on the computer which then records login credentials and passcodes and reports them back to the criminals.

**Customers**

Bank Name commercial customers authorized to submit ACH files via the Internet Banking System are low/medium/high risk customers. Describe what is being transmitted generally (e.g., mostly ACH payroll files). No customers are 3rd party payment providers, or there are 3rd party payment providers (note: if there are 3rd party payment providers, these would be high risk customers requiring extra due diligence and monitoring).

**Security Measures and Controls**

ACH files are submitted through the Internet Banking System. Hardware tokens have/have not been implemented as out of band authentication. These files do/do not automatically pass through to the ACH operator.

All submitted ACH files are/are not manually reviewed by bank personnel against a calendar of expected activity, then released.

Exposure limits have been implemented and are reviewed on an annual basis.

Annual in-person touch points are/are not performed and are/are not documented. Touch-points cover/do not cover areas such as anti-virus, phishing, NACHA changes.

Ongoing security awareness training is/is not provided to commercial customers.

Annually, each commercial customer is/is not evaluated based on type of business, financial strength, institution history, security measures in place, and type and volume of transactions.

Contracts specifically discuss/don’t discuss anti-virus and security control requirements on customer computers.

Exposure limits are/are not summarized and are/are not reported to the Board annually.

Calendar of expected activity is/is not formalized and is/is not available to responsible bank personnel.

**Action Plan**