Commercial Cash Management Onsite Visit Checklist

Company Name:__________________________________ Visit Date: ____________

Review Performed by:____

1. _________A single, stand-alone computer has been designated to perform Cash Management activities.

2. ________Observe whether antivirus software is being utilized and the date of most recent update and scan.

3. ________Confirm that company is maintaining confidential information (i.e., receiver's authorizations, account numbers, routing numbers, etc.) in a secure location.

4. ________Confirm that any confidential information is disposed of properly.

5. ________Confirm that all access security features (password protection, multi-factor authentication, tokens, biometrics, etc.) are kept secure from theft or outside access. In particular, features such as tokens should be kept securely under lock and key to avoid access of the security feature by unauthorized individuals.

6. ________Observe workstation used to access cash management. Inquire whether workstation is locked when unoccupied. Assess whether workstation is in a customer traffic area. Inform customer about the benefits of dual control.

7. _________Confirm that company representative has signed the Compliance Certification Statement found on the Commercial Cash Management (including ACH Origination) Customer Compliance Terms of Use and Procedures

Commercial Cash Management (including ACH Origination) Customer Compliance Terms of Use and Procedures

The Account Holder agrees to periodically assess and as appropriate update security policies, procedures and systems. The Account Holder will provide documentation to support the policies, procedures and systems that have been implemented to the Financial Institution upon request.

- The bank recommends that the Account Holder designate a single, stand-alone computer to perform Cash Management activities.

- The Account Holder is responsible for operator security procedures on the one personal computer licensed for use of the program. The Account Holder is responsible for the installation and maintenance of security features on the personal computer used in the system. These features may include anti-virus software, firewalls, anti-phishing software, penetration monitoring, etc.

- The Account Holder is responsible for making sure that all access security features (password protection, multi-factor authentication, tokens, biometrics, etc.) are kept secure from theft or outside access. In particular, features such as tokens should be kept securely under lock and key to avoid access of the security feature by unauthorized individuals.

In addition, as an ACH originator, there are many rules, laws and regulatory guidance that apply to you. While the entire list of rules is too long to list in this document, we would like to notify you about some of the more common rules that you will most likely encounter and be expected to follow. For a complete list of rules, laws and regulations, you may visit http://www.achrulesonline.org/ or may contact us at 888-728-1954.

8. You must obtain a signed authorization with every receiver of an ACH entry. The authorization should clearly state the terms of the agreement (i.e., transaction date(s), amount(s), frequency, account, etc.).

9. You must retain a copy of the signed authorization for two years after the authorization has been revoked.

10. You must provide a copy of the signed authorization to the Bank within two business days upon request.

11. Upon receipt of an ACH return, you must not retry the entry unless it was returned for insufficient funds (NSF) or uncollected funds. If you do retry an entry that was returned for NSF or uncollected funds, you will not retry the entry more than twice.

12. ACH entries will post based upon the account number no matter what name is listed as the receiver.

13. Upon receipt of a notification of change (NOC), you must correct future entries to which the NOC relates no later than six business days after the receipt of the NOC information or prior to initiating another entry to the receiver's account, whichever is later.

14. You must maintain confidential information (i.e., receiver's authorizations, account numbers, routing numbers, etc.) in a secure location. If transmitted over an unsecured electronic network (i.e., internet, email, etc.), the information must be encrypted using at a minimum 128-bit RC4 technology.

15. You must notify the Bank if you authorize a Third-Party to perform or handle any aspect of ACH origination. You may be required to provide a copy of the agreement in place with the Third-Party.

16. If you originate ACH entries on behalf of another company, you must notify the Bank. You must also provide a list of companies on whose behalf you originate as well as any agreements in place.

17. If you originate ACH entries on behalf of another company, you must complete an ACH Rules Compliance Audit in accordance to the ACH Rules. A copy of the audit must be submitted to the Bank by December 31st of each year.

18. If you suspect your Cash Management username and/or password have become compromised, you must notify us immediately. You also should notify us if an authorized ACH user is no longer with the company or goes on an extended leave.

19. If an ACH file was originated in error, you must notify us immediately (within 5 business days of the erroneous entry being originated). The file may be reversible, but the request does not need to be honored by the receiving financial institution or receiver.

20. If a reversing file is originated, the entire amount of the erroneous entry must be reversed and an entry for the correct amount should be sent, as applicable.

21. You should monitor activity on your account on a daily basis. If a suspicious transaction is located, you must notify us immediately.

22. You must maintain a working number during normal business hours that receivers may contact in case of questions. If this number changes, you must notify the Bank.

23. You must have collected funds in your account in order for an ACH credit file to be initiated.

24. You must maintain an account with sufficient collected funds to offset any ACH debits that are returned.

25. If the Bank requests any information or would like to perform a periodic audit of your ACH processing, you must comply with the request to the best of your ability. We will provide as much advance warning as possible.

26. You are required to have written security policy that relates to confidential ACH information (account and routing numbers).

Compliance Certification Statement

Company Name: ____________________________________

I certify that I have read and understand the above terms of use for Commercial Cash Management (including ACH Origination) with Peoples Bank & Trust. To the best of my knowledge, the company is complying with all security requirements listed above. I understand that non-compliance with the above or any other ACH rule or law governing ACH could lead to fines, suspension of ACH services or additional enforcement actions. If NACHA imposes any fines upon the Bank because of entries originated by the company, the company will be responsible for paying the fine.

Signature: ____ Date: ___________