Commercial Remote Deposit Capture Onsite Visit Checklist

Company Name:_____ Visit Date: _____

Review Performed by:_____

1. _____Observe whether antivirus software is being utilized and the date of most recent update and scan.

2. _____Confirm that company is maintaining confidential information (i.e. checks.) in a locked, fire-proof container with limited access to employees.

3. _____Confirm that any confidential information is disposed of properly. The Business should establish procedures such that at the end of the 60 days retention period, all checks should be destroyed to ensure that the checks cannot be submitted for payment and data on the checks cannot be reviewed or duplicated. The Business should maintain a check destruction log to ensure checks are destroyed and the end of the retention period (date of deposit + 60 days) and to evidence the actual date of destruction.

4. _____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.

5. _____Observe workstation used to access remote deposit scanner and computer. Inquire whether workstation is locked when unoccupied. Assess whether workstation is in a customer traffic area. Inform customer about the benefits of dual control.

6. _____Confirm that company representative has signed the Compliance Certification Statement found on the Commercial Remote Deposit Customer Compliance Terms of Use and Procedures

Commercial Remote Deposit Capture 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. Financial Institution reserves the right to issue new Security Procedures and/or cancel or change any Security Procedures from time to time.

- The Business shall hold the original written checks in a secure environment for a period of at least 14 days, but not to exceed 60 days. The Business agrees to shred or otherwise destroy all original checks after a reasonable period of time, after the Business verifies credit to their account for the check. The Business should establish procedures such that at the end of the 60 days retention period, all checks should be destroyed to ensure that the checks cannot be submitted for payment and data on the checks cannot be reviewed or duplicated. The Business should maintain a check destruction log to ensure checks are destroyed and the end of the retention period (date of deposit + 60 days) and to evidence the actual date of destruction.

- The Business will endorse the back of all checks presented for deposit to prevent redeposit.

- The Business will utilize minimum hardware, internet, and software requirements including use of Windows XP Professional (or) Windows XP Home (or) Windows Vista Home Edition (or) Windows Vista Business Edition (or) Windows Vista Enterprise Edition (or) Windows Vista Ultimate Edition, Internet Explorer 7 or 8, and Check Reader/Scanner (provided by Peoples Bank & Trust).

- The Business will utilize best acceptable computer use practices including but not limited to anti-virus software, firewall and password protections.

- Whenever the Security Procedures include the assigning to Business of any confidential password, logon identification, identification code, personal or location identification

number, repetitive code, or similar security device, Business shall not disclose such security device except to employees or agents authorized to act for Business in connection with the service. Business shall implement such safeguards as are reasonably necessary to ensure the confidentiality and integrity of such security devices, and shall immediately notify Financial Institution if the confidentiality or integrity of such security device is breached or threatened.

- The Business will allow the Financial Institution to review and inspect during reasonable business hours, and the Business will supply all financial information, financial records, and documentation of the Business regarding the checks that the Financial Institution may request.

Compliance Certification Statement

Company Name: _____

I certify that I have read and understand the above terms of use for Commercial Remote Deposit Capture with Peoples Bank & Trust. To the best of my knowledge, the company is complying with all security requirements listed above.

Signature: _____ Date: _____