RENASANT BANK

THE BEST BANK IN THE SOUTH

Best Practices for Commercial On-line Banking
Remain Secure and Reduce Processing Risk

Renasant Bank is pleased to provide this questionnaire to assist you in periodically reviewing your safeguards and daily procedures related to disbursement, receipts and/or information provided via on-line banking services. Services may include but not limited to Business Check Express Service, ACH Origination Services, BillPay Service, On-line Wire Initiation, Mobile Banking Services, Positive Pay Service and Information Reporting. This is for your use internally however we recommend completing this questionnaire a minimum of annually and/or when there is a change in personnel. Our Treasury Solutions Sales Team is available to review all of these services with you.

Business Name:_____

Business Location:_____

Completed by:_____
Phone#:_____
Email address:_____

Date:_____

Daily Deposit Limit

ACH Origination: Is your daily limit still set suitably for your business? Yes_____ No_____

Business Check Express: Is your daily deposit limit still set suitably for your business?

Yes_____ No_____

Operational Controls

Are there procedures that require a separation of duties? Yes_____ No_____

Do you utilize dual control for administrative changes (e.g., new users)? Yes_____ No_____

Do you utilize dual control for transmitting the file? Yes_____ No_____

Is your equipment and designated computer(s) that you use physically secure? Yes_____ No_____

For Business Check Express: How are the scanned checks secured? _____

Do you retain the scanned checks for the required retention time of 14 days? Yes_____ No_____

Do you use multiple RDC systems with other Financial Institutions? Yes_____ No_____

System Security

Do you utilize anti-virus, anti-spyware, and anti-malware programs? Yes_____ No_____

Do you keep the above software updated and install security patches promptly? Yes_____ No_____

RENASANT BANK

THE BEST BANK IN THE SOUTH

Are firewalls in place? Yes_____ No_____
Do you monitor for unauthorized system activity or scan for vulnerabilities? Yes_____ No_____
Does each user have a unique user name and password? Yes_____ No_____
Are strong passwords required of all users? Yes_____ No_____
Do you have a computer dedicated for online banking functions? Yes_____ No_____
Do you restrict web browsing and social networking on the computer used for scanning checks? Yes_____ No_____
Are security procedures reviewed annually and adjusted? Yes_____ No_____

Staff Controls

Does staff receive initial and periodic training on the banking services software? Yes_____ No_____

Are written procedures maintained for depositing items via RDC and originating items via ACH? Yes_____ No_____

Has there been a change in the Security Admin user? Yes_____ No_____

Have there been any general staff changes in relation to banking services? Yes_____ No_____

Corporate Account Takeover

Does staff receive periodic training on fraud and corporate account takeover? Yes_____ No_____
(including details on current fraud schemes that target businesses)

Activity Monitoring

Do you utilize alerts to monitor online banking administrative functions?
(e.g., new users added, password changes, disabling of security features) Yes_____ No_____

Do you utilize alerts to monitor online banking user activity?
(e.g., attempts to exceed deposit limit, unsuccessful log in attempts) Yes_____ No_____

Is your depository account activity reviewed daily for accuracy? Yes_____ No_____