BUSINESS SELF ASSESSMENT
FOR ELECTRONIC PAYMENT SERVICES

Your company is being asked to complete this Self-Assessment because you either currently use or are requesting use of IncredibleBank's ACH Payment and Collection and/or Remote Deposit systems.

Section I - Business Information

Business Name _____ Date _____

Completed By _____

This may be your accounting firm if their systems are used/will be used to send your ACH file to IncredibleBank or if the Remote Deposit Scanner is installed/will be installed on their computer.

Customer Contact Name _____

Customer Contact Phone _____

Customer Contact Email _____

Select all the services for which you are completing this Self-Assessment:

☐ ACH Origination ☐ Remote Deposit Capture ☐ Online Wire Transfer

Section II - General Payment Information

The following two questions apply to existing IncredibleBank ACH or Remote Deposit customers only.

☐ Yes ☐ No Have you reviewed your payment agreement(s) recently?

☐ Yes ☐ No Are you in compliance with the agreement(s)?

The following questions apply to all new or existing IncredibleBank ACH or Remote Deposit customers only.

Operational Controls

☐ Yes ☐ No Is your payment equipment and designated computer physically secure?

☐ Yes ☐ No Do you have business continuity plan(s) for your payment product(s)?

Section II continued on page 2

System Security

- ☐ Yes ☐ No Do you utilize anti-virus, anti-spyware, and anti-malware programs?
- ☐ Yes ☐ No Do you keep software updated and install security patches promptly?
- ☐ Yes ☐ No Do you have firewalls in place to protect your data?
- ☐ 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 Do you require strong passwords for all users?
- ☐ Yes ☐ No Do users "log off" or lock computers when not in use?
- ☐ Yes ☐ No Do you utilize a dedicated computer for online financial functions?
- ☐ Yes ☐ No *If no, do you restrict web browsing and social networking on the computer used?*
- ☐ Yes ☐ No Do you review your internal security procedures annually and adjust if necessary?
- ☐ Yes ☐ No Do you use dual control for external transfer transmissions? *(Business Bill Pay, ACH, Wire Transfer, Remote Deposit)*

Staff Controls

- ☐ Yes ☐ No Do you perform background checks on staff involved with payment processing?
- ☐ Yes ☐ No Does staff receive initial and periodic payment training?
- ☐ Yes ☐ No Are written procedures maintained on your electronic payment products?
- ☐ Yes ☐ No Do you contact IncredibleBank when authorized employees are terminated?

Fraud and Account Compromise

- ☐ Yes ☐ No Does staff receive period training on fraud and corporate account takeover, including current fraud schemes that target businesses?
- ☐ Yes ☐ No Do you have a corporate account takeover incident response plan?
- ☐ Yes ☐ No Do you have data breach insurance?
- ☐ Yes ☐ No Do you verbally validate any requests for changes to payment instructions, i.e. payroll or vendor, via a validated method of verification?

Activity Monitoring

- ☐ Yes ☐ No Is your depository account activity reviewed daily for accuracy?
- ☐ Yes ☐ No Do you utilize alerts to monitor online banking administrative functions?
- ☐ Yes ☐ No Do you utilize alerts to monitor online banking user activity?

Section III - ACH Origination Information

The following questions and the ACH Originator Security Framework Certification apply to all new or existing IncredibleBank ACH customers.

☐ Yes	☐ No	For recurring debit entries, do you provide proper notice to the Receiver if the amount or the date is to be changed? (Skip if you do not originate recurring debit entries)
☐ Yes	☐ No	Do you initiate Prenote entries at least three (3) banking days prior to the live dollar entry?
☐ Yes	☐ No	If you receive a Notification of Change indicating a correction is needed on an entry previously sent, do you make the correction within six (6) banking days or prior to initiating another entry?
☐ Yes	☐ No	If an ACH entry is returned to you because of Insufficient Funds, are you aware that the entry may only be resubmitted two (2) more times in attempt to clear it?
☐ Yes	☐ No	Are you aware of and do you follow the specific authorization requirements?
☐ Yes	☐ No	Do you store authorizations in a physically secure location?
☐ Yes	☐ No	Do you retain the authorization for two (2) years after it is terminated or revoked?
☐ Yes	☐ No	After the retention timeframe, do you destroy the authorization along with any other documents containing private information by cross-cut shredding or incineration?
☐ Yes	☐ No	Are you aware of your company's assigned ACH Origination Daily Exposure Limit?
☐ Yes	☐ No	Do you conduct due diligence to ensure you are keeping consumer information protected as required by the ACH Data Security Framework (see next page)?

ACH Originator Security Framework Certification

Effective September 20, 2013, the NACHA Operating Rules ("Rules") require that financial institutions conducting ACH transactions employ a "security framework" aimed at protecting the security and integrity of certain ACH data throughout its lifecycle. One element of that security framework is the requirement that financial institutions require non-consumer originators, Third-Party Service Providers and Third-Party Senders to establish, implement and, as appropriate, update security policies, procedures and systems related to the initiation, processing and storage of ACH entries and the related "Protected Information."

Protected Information is defined as "the non-public personal information, including financial information, of a natural person used to create, or contained within, an [ACH] Entry and any related Addenda Record."

The purpose of this section is to assist all the parties involved in an ACH transaction to comply with the data security requirements as set forth in the Rules.

Questions and Certification

☐ Yes ☐ No Do you have written security policies and procedures governing the initiation, processing and storage of ACH transactions and any related Protected Information?

☐ Yes ☐ No Do you have written security policies and procedures governing the initiation, processing and storage of ACH transactions and any related Protected Information?

In conducting ACH transactions, through which methods and channels do you gather and obtain Protected Information? (Check all that apply)

- ☐ Mail
- ☐ Web
- ☐ Phone
- ☐ Other _____

Identify all steps that you utilize to secure Protected Information. (Check all that apply)

- ☐ Locked Cabinet
- ☐ Encryption
- ☐ Password
- ☐ Other _____

How do you dispose of Protected Information?

Section IV - Remote Deposit Capture Information

The following questions apply to all new or existing IncredibleBank Remote Deposit customers.

Equipment

Please indicate the serial number of each IncredibleBank Remote Deposit scanner your business utilizes. This can be found on the bottom of the machine. If you have not yet received your scanner, respond "NEW".

_____ _____ _____

Data Protection

☐ Yes ☐ No Do you keep scanned checks physically secure?

☐ Yes ☐ No Do you retain the scanned checks for no more than 30 days?

☐ Yes ☐ No Do you destroy the scanned checks by cross-cut shredding or incineration so that they cannot be reconstructed?

☐ Yes ☐ No Do you print check images and reports from the Remote Deposit system?

☐ Yes ☐ No Do you keep images and reports physically secure?

☐ Locked File Cabinet ☐ Locked Drawer ☐ Fireproof Safe ☐ Other

Signatures

Business Name _____

Signature _____ Date _____

Name and Title of Authorized Signer

_____ _____

Name *Title*