SCHEDULE A

ACH/Cash Management Originator Best Practices

Authorization

1. All debits to consumer accounts via the ACH network must be authorized by the consumer in writing and signed by the consumer. This authorization may be sent in by email or fax.
2. The consumer should be advised to retain a paper copy of this authorization for their records. Your commercial user must be able to provide a hard copy of the authorization upon request.
3. We require that files are sent by authorized senders as documented in the agreement.

Retention

1. The signed authorization must be retained by your commercial user for a period of two years following the termination or revocation of the authorization. Your commercial user must retain either the original or micro-film equivalent copy of the signed authorization.

Pre-Notes

1. Pre-notes are not required but it is recommended by the bank that pre-notes are sent.
2. May not initiate entries sooner than six banking days following the settlement date of the pre-note entry.

Processing

1. Once you have loaded the batch, you must approve it or the batch will not be sent.
2. Once you have approved the batch, perform a print screen of the processing dates.

Notification of Changes (NOC's)

1. Upon receipt of Notifications of Change, requested changes should be made within six banking days or prior to the initiation of the next entry, whichever is later.
2. It is a rules violation not to respond to NOC's.
3. Make sure the bank has the correct person to contact for NOC's.

Returns

1. If returned by the ACH operator, RDFI has never seen it, make corrections and pre-note again.
2. If returned by a RDFI, research based on the Return Reason Code.
3. Entries returned R01 or R09 are not reinitiated in excess of the limits prescribed by the Rules.

Security

1. Originator's files are properly secured as required by NACHA rules.
2. When an employee is terminated or is no longer employed, notify the financial institution.
3. When an employee's job description changes, so they no longer need access to the cash management application, notify the financial institution.
4. We require that you implement and maintain current Anti-Virus/Internet Security software and Microsoft critical security patches for Windows Operating Systems.
5. We require setting Anti-Virus/Internet Security software to download signature updates daily. You should also ensure real-time protection is activated and schedule a complete system scan of all files at least weekly.
6. We require the use of the Microsoft based operating system or MAC operating system running in parallel and you should also automatically download and install all critical security patches as soon as they are available.
7. We require the use of network or PC based firewalls.
8. Surfing the Internet on the PC used to process cash management is not recommended.
9. We require that employees use strong passwords to access the system.
10. Profiles cannot be shared by co-workers and access to the cash management application can only be obtained thru the bank supplied user profiles.
11. Each cash management user profile must utilize an IP address restriction, unless the IP waiver form has been filled out acknowledging and accepting the risk associated with not using the IP address restriction.
12. Out-of-band security must be utilized for authenticating into the cash management application and must include a security pin being sent as a SMS text message or a voice pin. Security pins sent to an email address is not allowed.