ACCEPTANCE OF SERVICES

WELLS FARGO

Part I – Certification.

The person(s) signing this Acceptance of Services ("Acceptance") certifies/certify that:

(a) the company identified in the signature block of this Acceptance ("Company") has received and agrees to be bound by the Service Documentation, as defined in Wells Fargo Bank, N.A.'s ("Bank") Master Agreement for Treasury Management Services;

(b) Company has granted the person(s) signing this Acceptance the authority on Company's behalf to (i) execute this Acceptance, (ii) enter into other agreements with Bank for treasury management services Bank offers on or after the Effective Date of this Acceptance (each, a "Service") and (iii) amend, terminate or otherwise act on behalf of Company with respect to this Acceptance and such other agreements and Services; and

(c) Company's use of any Service, including without limitation each Service Company begins using after the Effective Date of this Acceptance, confirms Company's receipt of and agreement to be bound by the Service Documentation relating to that Service.

Part II – ACH Origination Services.

A. Description of Security Procedure.

1. **General.** An "Entry" is an automated clearing house ("ACH") debit or credit entry issued in Company's name, and a "File" is the data file or batch release used to transmit one or more Entries (or a communication amending or canceling an Entry or File) to Bank. Bank will verify each File Bank receives in Company's name solely in accordance with the Security Procedure(s) Company elects in this Acceptance ("Security Procedure" is defined in Bank's ACH Origination Service Description). The purpose of the Security Procedure is to verify the authenticity of a File, not to detect an erroneous or duplicate Entry or File.

2. **Commercially Reasonable.** Company has determined the Security Procedure Company has elected (a) best meets Company's requirements with regard to the size, type and frequency of Files issued by Company to Bank and (b) is commercially reasonable. Company refuses to have its Files verified by any security procedure other than the Security Procedure Company has elected.

3. **Binding Instructions.** Company will be responsible for any erroneous or duplicate Entry or File Bank receives in Company's name. Company agrees to be bound by each Entry and File, or request to cancel or amend an Entry or File, whether or not authorized by Company, issued in Company's name and accepted by Bank in compliance with the Security Procedure Company has elected.

4. **Confidentiality.** Company and Bank will preserve the confidentiality of the Security Procedure and any passwords, codes, security devices and related instructions provided by Bank. If Company becomes aware of a breach, or suspects a breach may occur, it will immediately notify Bank.

5. **Authorized Person(s).** Company will promptly notify Bank in writing of the identity of each person authorized to receive information regarding the Security Procedure (each, an "Authorized Person") and when a person is no longer an Authorized Person. Company will maintain effective internal procedures to safeguard against unauthorized Entries or Files and warrants that no individual will be allowed to initiate an Entry or File without proper supervision and safeguards.

B. Election of Initiation Methods and Security Procedures.

The Initiation Methods and Security Procedures Company has elected for ACH origination are:

☒ Commercial Electronic Office® (CEO®) Initiation Method.

CEO is Bank's electronic banking portal that is accessed via the Internet. Authorized users may access Bank's CEO Internet ACH Service through the portal. CEO security procedures include log-on credentials specified by Bank (that may include a Company ID, user ID and password) and any other authentication or authorization process Bank requires from time to time. Bank will use the CEO security procedures to authenticate each File received through CEO in Company's name.

☐ Payment Manager® Initiation Method.

☐ **Secure Application File Exchange Transmission ("SAFE-T").** This transmission platform offers a variety of transmission protocols including hypertext transfer protocol secured (https), FTP over SSL (FTP/S), secure FTP (S-FTP), and Applicability Statement 2 (AS2) that Bank uses to authenticate each File transmitted to Bank in Company's name.

☐ **Machine-to-Machine ("M2M").** This transmission method uses an XML message interface that is based on the Interactive Financial eXchange (IFX) message standard using SOAP structured messages. Data is communicated via the Internet using 128-bit encryption and Secure Socket Layers (SSL). Bank uses digital certificates to authenticate each File transmitted to Bank in Company's name.

☐ IBM® **Connect:Direct® with Secure Plus+.** Secure Plus+ is an add-on to Connect Direct to enhance security by means of Secure Socket Layer ("SSL") or Transport Layer Security ("TLS"). Connect Direct® is a registered trademark of Sterling Commerce, Inc. an IBM Company.

☐ **Value-Added Network ("VAN").** With this transmission method, a third party serves as an intermediary for transmitting data between Company and Bank. Procedures for transmitting files may vary by VAN. Bank follows the procedures of the VAN selected by Company to authenticate each File transmitted to Bank through the VAN in Company's name.

☒ Direct Origination Initiation Method.

☒ **Secure Application File Exchange Transmission ("SAFE-T").** This transmission platform offers a variety of transmission protocols including hypertext transfer protocol secured (https), FTP over SSL (FTP/S), secure FTP (S-FTP), and Applicability Statement 2 (AS2) that Bank uses to authenticate each File transmitted to Bank in Company's name.

☐ IBM® **Connect:Direct® with Secure Plus+.** Secure Plus+ is an add-on to Connect Direct to enhance security by means of Secure Socket Layer ("SSL") or Transport Layer Security ("TLS"). Connect Direct® is a registered trademark of Sterling Commerce, Inc. an IBM Company.

☐ SWIFT® Initiation Method.

SWIFT has established procedures for controlling access to SWIFT messaging services (each, an "Access Control") that may include without limitation access codes, message authentication codes, secure card readers, digital signatures, and Hardware Security Modules. In addition, SWIFT authenticates certain messages including without limitation Files based on SWIFT message type prior to accepting them for routing as SWIFT messages (each, an "Authenticated Message"). This authentication may include confirming that the sender and recipient of the message have exchanged bilateral keys ("BKE"), entered into a relationship management application ("RMA") agreement, or taken other steps to secure the transmission of SWIFT messages between them as SWIFT requires from time to time (each, an "Authentication Procedure").

☐ Security Procedure Elected by Company's Third Party Service Provider.

Company is utilizing a Third Party Service Provider ("TPSP") as defined in the ACH Rules to originate Entries and Files on Company's behalf. Bank will authenticate each File transmitted to Bank in Company's name in accordance with the security procedure the Company's TPSP has elected. Company will notify Bank of any change to Company's TPSP in a manner affording Bank a reasonable opportunity to act on the information. Company's TPSP is:

Third Party Service Provider: _____

Contact Person: _____

Telephone: _____ Fax: _____

Non-Standard Security Procedure.

Company has refused to utilize any of the security procedures described above and has elected to use the Security Procedure set forth in Attachment B.

Part III – Wire Transfer Services.

A. Description of Security Procedure.

1. **General.** Bank will verify instructions to transfer funds from Company's Account that Bank receives in Company's name (each, a "Payment Order") solely in accordance with the Security Procedure(s) Company elects in this Acceptance ("Security Procedure" is defined in Bank's Wire Transfer Service Description). The purpose of the Security Procedure is to verify the authenticity of a Payment Order, not to detect an erroneous or duplicate Payment Order.

2. **Commercially Reasonable.** Company has determined the Security Procedure Company has elected (a) best meets Company's requirements with regard to the size, type and frequency of Payment Orders issued by Company to Bank and (b) is commercially reasonable. Company refuses to have its Payment Orders verified by any security procedure other than the Security Procedure Company has elected.

3. **Binding Instructions.** Company will be responsible for any erroneous or duplicate Payment Order Bank receives in Company's name. Company agrees to be bound by each Payment Order, or request to cancel or amend a Payment Order, whether or not authorized by Company, issued in Company's name and accepted by Bank in compliance with the Security Procedure Company has elected.

4. **Confidentiality.** Company and Bank will preserve the confidentiality of the Security Procedure and any passwords, codes, security devices and related instructions provided by Bank. If Company becomes aware of a breach, or suspects that a breach may occur, it will immediately notify Bank.

5. **Authorized Person(s).** Company will promptly notify Bank in writing of the identity of each person authorized to receive information regarding the Security Procedure (each, an "Authorized Person") and when a person is no longer an Authorized Person. Company will maintain effective internal procedures to safeguard against unauthorized Payment Orders and warrants that no individual will be allowed to initiate a Payment Order without proper supervision and safeguards.

B. Election of Initiation Method(s) and Security Procedure(s).

The Initiation Method(s) and Security Procedure(s) Company has elected for Wire Transfers are:

☒ Voice Initiation Method.

Bank's voice initiation security procedure consists of confirming that the personal identification number ("PIN") accompanying a Payment Order corresponds with a valid PIN assigned to Company for voice-initiated Payment Orders.

☐ **Telephone Verification Service.** If Bank receives a voice-initiated, non-repetitive Payment Order of $_____ or more, Bank will make one attempt to telephone person(s) designated by Company on the most current setup form for Company in Bank's records to authenticate the Payment Order. If Bank is unable to complete the call, Bank will not process the Payment Order.

☒ Commercial Electronic Office® (CEO®) Initiation Method.

CEO is Bank's electronic banking portal that is accessed via the Internet. Authorized users may access Bank's CEO Wire Transfer Service through the portal. CEO security procedures include log-on credentials specified by Bank that may include a Company ID, user ID and password and any other authentication or authorization process Bank requires from time to time. Bank will use the CEO security procedures to authenticate each Payment Order received through CEO in Company's name.

☐ Payment Manager® Initiation Method.

☐ **Secure Application File Exchange Transmission ("SAFE-T").** This transmission platform offers a variety of transmission protocols including hypertext transfer protocol secured (https), FTP over SSL (FTP/S), secure FTP (S-FTP), and Applicability Statement 2 (AS2) that Bank uses to authenticate each Payment Order transmitted to Bank in Company's name.

☐ **Machine-to-Machine ("M2M").** This transmission method uses an XML message interface that is based on the Interactive Financial eXchange (IFX) message standard using SOAP structured messages. Data is communicated via the Internet using 128-bit encryption and Secure Socket Layers (SSL). Bank uses digital certificates to authenticate each Payment Order transmitted to Bank in Company's name.

☐ IBM® **Connect:Direct® with Secure Plus+.** Secure Plus+ is an add-on to Connect Direct to enhance security by means of Secure Socket Layer ("SSL") or Transport Layer Security ("TLS"). Connect Direct® is a registered trademark of Sterling Commerce, Inc. an IBM Company.

☐ **Value-Added Network ("VAN").** With this transmission method, a third party serves as an intermediary for transmitting data between Company and Bank. Procedures for transmitting Payment Orders may vary by VAN. Bank follows the procedures of the VAN selected by Company to authenticate each Payment Order transmitted to Bank through the VAN in Company's name.

☐ Direct Origination Initiation Method.

☐ **Secure Application File Exchange Transmission ("SAFE-T").** This transmission platform offers a variety of transmission protocols including hypertext transfer protocol secured (https), FTP over SSL (FTP/S), secure FTP (S-FTP), and Applicability Statement 2 (AS2) that Bank uses to authenticate each Payment Order transmitted to Bank in Company's name.

☐ IBM® **Connect:Direct® with Secure Plus+.** Secure Plus+ is an add-on to Connect Direct to enhance security by means of Secure Socket Layer ("SSL") or Transport Layer Security ("TLS"). Connect Direct® is a registered trademark of Sterling Commerce, Inc. an IBM Company.

☐ SWIFT® Initiation Method.

SWIFT has established procedures for controlling access to SWIFT messaging services (each, an "Access Control") that may include without limitation access codes, message authentication codes, secure card readers, digital signatures, and Hardware Security Modules. In addition, SWIFT authenticates certain messages based on SWIFT message type prior to accepting them for routing as SWIFT messages (each, an "Authenticated Message"). This authentication may include confirming that the sender and recipient of the message have exchanged bilateral keys ("BKE"), entered into a relationship management application ("RMA") agreement, or taken other steps to secure the transmission of SWIFT messages between them as SWIFT requires from time to time (each, an "Authentication Procedure").

☐ Non-Standard Security Procedure.

Company has refused to utilize any of the security procedures described above and has elected to use the Security Procedure set forth in Attachment B.

Remainder of page intentionally left blank

Part IV – Designation of *Wells Fargo Stagecoach Sweep*® Option.

A. Investment Sweep Options.

Company elects the following Option (check one box only):

☐ ***Wells Fargo Stagecoach Sweep*** **Preferred Option.**

☐ ***Wells Fargo Stagecoach Sweep*** **Preferred Option with secondary Wells Fargo Stagecoach Sweep, Repurchase Agreement Option.**

☐ ***Wells Fargo Stagecoach Sweep*** **Commercial Paper Option.**

☐ ***Wells Fargo Stagecoach Sweep*** **Repurchase Agreement Option with secondary Wells Fargo Stagecoach Sweep, Preferred Option.**

☐ ***Wells Fargo Stagecoach Sweep*** **Repurchase Agreement Option.**

☐ ***Wells Fargo Stagecoach Sweep*** **Money Market Mutual Fund Option.**
(Check one box only.)

- ☐ Wells Fargo Advantage Money Market Fund - Fund 3951.
- ☐ California Municipal Money Market Fund - Class A - Fund 29.
- ☐ Treasury Plus Money Market Fund - Class A - Fund 453.
- ☐ National Tax-Free Money Market Fund - Class A - Fund 452.
- ☐ 100% Treasury Money Market Fund - Service Class - Fund 8.

B Savings Account Sweep Option.

☐ Company elects the Wells Fargo Money Market Savings Account Sweep Option.

C. Credit Sweep Option.

☐ Company elects Bank's Credit Sweep Option.

- Company's LOC number is _____.

D. Additional Information.

- Company's Checking Account Number: _____.
- Statements and/or Confirmations will be sent to Company by electronic means unless otherwise requested by Company. Electronic means include Bank's Commercial Electronic Office®, facsimile and/or Secure E-Mail.

Part V – Signature and Effective Date.

Agreed To and Accepted By:

Company: Wells Fargo Bank

By: Liam F. Higgins

Name: Liam F. Higgins

Title: Vice President

Effective Date: 5/1/2013

Company: _____

By: _____

Name: _____

Title: _____

Effective Date: _____

Company: _____

By: _____

Name: _____

Title: _____

Effective Date: _____

Company: _____

By: _____

Name: _____

Title: _____

Effective Date: _____