ELECTRONIC PAYMENTS SECURITY ACCESS CIRCULAR

1) **AUTHORIZATION WITH RESPECT TO WIRE TRANSFERS AND ACH.** Prior to commencement of wire transfer or automated clearing house ("ACH") services, the Customer will complete and execute the Master Transactions Agreement. The Bank will not accept outgoing wire transfer requests from the Customer without having on file a completed Master Transactions Agreement executed by the Customer. The Customer will also complete and execute the FHLB Dallas Services Signature Card for wire transfer services and ACH services.

2) **PERSONAL IDENTIFICATION NUMBERS ("PINS").** The Customer shall authorize certain individuals to request outgoing wire transfers ("Initiators") and certain individuals to confirm outgoing wire transfers ("Authorizers" and collectively with the Initiators, the ("Authorized Individuals"). The Bank, upon its receipt of a properly completed Signature Card fully executed by the designated Initiators and Authorizers and certified by a person authorized by the Customer's board of directors in certified resolutions, Certificate of Incumbency (COI) or Corporate Certificate of Authority (CCA) provided to the Bank whose signature is on file with the Bank, will issue PINs to the Authorized Individuals based on the caller information provided to the Bank on the signature cards. Upon the Bank's receipt of the Wire Transfer PIN Receipt Form executed by an Initiator or an Authorizer, the Bank will activate the PIN for such Initiator or Authorizer according to the Bank's policies and procedures. It is the responsibility of the Customer to ensure that the confidentiality of PINs is maintained and to inform the Bank immediately of the addition or deletion of persons who are Authorized Individuals and the addition or deletion of the authority of any Authorized Individual. Except with respect to requests made in Paragraphs 5 and 6 of this Electronic Payments Security Access Circular, each Initiator must provide his or her PIN when initiating an outgoing wire transfer request. If an Initiator cannot provide his or her valid PIN, the Bank will not accept a wire transfer request unless the Bank in its sole discretion elects to honor such request. The authority of a person to make a request for wire transfer of funds and to issue other directions and instructions to the Bank for the account of the Customer shall be presumed if the person making the request uses the PIN associated with an Initiator. Except with respect to requests made pursuant to Paragraphs 4 and 6 of this Electronic Payments Security Access Circular, each Authorizer must provide his or her PIN when confirming an outgoing wire transfer of funds. If an Authorizer cannot provide his or her valid PIN, the Bank will not accept a wire transfer request unless the Bank in its sole discretion elects to honor such request. The authority of a person to confirm an outgoing wire transfer of funds shall be presumed if the person confirming the outgoing wire transfer of funds uses the PIN associated with an Authorizer.

At least annually, the Bank will issue each Authorized Individual a new PIN to replace his or her current PIN which will expire seven (7) days from date of issuance. The Authorized Individual is required to return to the Bank a Wire Transfer PIN Receipt Form for the new PIN to be activated. If the Authorized Individual does not return his or her properly executed Wire Transfer PIN Receipt Form for the new PIN within seven (7) days from the date of issuance, the individual's authority to initiate or confirm wire transfers under this PIN will not be activated. The individual must be an Authorized Individual on the wire signature card to request a new PIN be generated.

3) **WIRE TRANSFER REQUESTS PRIOR TO ISSUANCE OF A PIN, INVALID PIN or LOST PIN.** If an Initiator or Authorizer has lost their PIN, the PIN is invalid for any reason, or not yet received his or her PIN, an Initiator or Authorizer may, at the Bank's discretion, initiate a wire transfer via telephone without a PIN, provided that the Bank has received a PDF copy of the Wire Transfer PIN Waiver Form executed by an individual authorized by the Customer's board of directors in certified resolutions, COI or CCA. Once received, the Bank will execute the wire on behalf of the member and debit the member's Demand Deposit Account (DDA).

4) **WIRE TRANSFER REQUESTS INITIATED OR AUTHORIZED WITH AN INVALID PIN.** If the PIN is invalid, the Bank or SecureConnect will inform the Initiator or Authorizer that the PIN is invalid on the telephone or through a message delivered through Secure Connect as follows:

Secure Connect

- Initiator
  - Secure Connect will display an “Invalid value” error upon entering an invalid PIN.
  - After the 3rd invalid PIN attempt, Secure Connect will display a “Payment Validated” message, however the wire request will route wire to a breach queue where the wire will be canceled.
  - The Bank will inform the Initiator, or another individual listed on the Signature Card, the wire transfer request was canceled due to invalid PIN.
- Authorizer
  - Receives wire from Initiator with a valid PIN.
  - Secure Connect will not allow the authorization of a wire with an invalid PIN.
  - A valid PIN is needed to go past this stage.

Phone Wires

- Initiator
  - Initiator will need to have a valid PIN to execute a wire via phone. The wire system will not proceed with the creation of a wire without a valid PIN.
  - A one-time passcode will be sent to the initiator’s email on file to confirm the Initiator’s identity for all phone wires, including repeat, semi-repeat, non-repeat, , and drawdowns.
- Authorizer
  - Authorizer will need to have a valid PIN to authorize a wire initiated by phone.
  - A valid Authorizer PIN is needed to move the wire from a pending authorize state to the release queue.
  - A one-time passcode will be sent to the Authorizer’s email on file to confirm the Authorizer’s identity for all phone wires, including repeat, semi-repeat, non-repeat, , and drawdowns.

The Customer may elect to submit a wire request in accordance with the procedures set forth in Paragraph 3. This process applies to wires initiated through SecureConnect or over the telephone (Paragraph 7) and and to callbacks to Authorizers (Paragraph 10).

5) **REPETITIVE AND SEMI-REPETITIVE WIRE TRANSFER REQUESTS.** Upon the Bank’s receipt of a Repetitive Wire Transfer Form executed by an Initiator and an Authorizer, the Bank will call the Initiator at the phone number listed on the Signature Card for such Initiator or at such other phone number as designated by the Customer to the Bank in accordance with Paragraph 15 of this Electronic Payments Security Access Circular to verbally verify all of the information included in the Repetitive Wire Transfer Form. A one-time passcode will be sent to the Initiator’s email on file to confirm the Initiator’s identity. If the Initiator verifies identity and all of the information included in the Repetitive Wire Transfer Form, the Bank will call the Authorizer that executed the Repetitive Wire Transfer Form at the phone number listed on the Signature Card for such Authorizer or at such other phone number as designated by the Customer to the Bank in accordance with Paragraph 15 of this Electronic Payments Security Access Circular to confirm all of the information included in the Repetitive Wire Transfer Form. A one-time passcode will be sent to the Authorizer’s email on file to confirm the Authorizer’s identity. If the Authorizer confirms identity and all of the information included in the Repetitive Wire Transfer Form, the Bank will approve the request for a repetitive wire set up and call and verify identity of the Initiator at the phone number listed on the Signature Card for such Initiator or at such other phone number as designated by the Customer to the Bank in accordance with Paragraph 15 of this Electronic Payments Security Access Circular to give the Initiator the repeat code. The authority of a person to verify or confirm information included in a Repetitive Wire Transfer Form shall be presumed if the Bank calls the phone number listed on the Signature Card for an Initiator or Authorizer, as applicable, or at such other phone number as designated by the Customer to the Bank in accordance with Paragraph 15 of this Electronic Payments Security Access Circular and the person who answers the phone verifies identity and confirms all of the information included in such Repetitive Wire Transfer Form. These authorizations will remain in effect until revoked in writing by an authorized Initiator or Authorizer as identified on the Signature Card.

6) **DRAWDOWN REQUESTS FOR TRANSFER OF FUNDS.** Upon the Bank’s receipt of a Drawdown Request Set Up and Authorization Form executed by an Initiator and an Authorizer, the Bank will call the Initiator at the phone number listed on the Signature Card for such Initiator or at such other phone number as designated by the Customer to the Bank in accordance with Paragraph 15 of this Electronic Payments Security Access Circular to verbally verify all of the information included in the Drawdown Request Set Up and Authorization Form. A one-time passcode will be sent to the Initiator’s email on file to confirm the Initiator’s identity. If the Initiator verifies identity and all of the information included in the Drawdown Request Set Up and Authorization Form, the Bank will call the Authorizer that executed the Drawdown Request Set Up and Authorization Form at the phone number listed on the Signature Card for such Authorizer or at such other phone number as designated by the Customer to the Bank in accordance with Paragraph 15 of this Electronic Payments Security Access Circular to confirm all of the information included in the Drawdown Request Set Up and Authorization Form and such other information as requested by the Bank. A one-time passcode will be sent to the Authorizer’s email on file to confirm the Authorizer’s identity. If the Authorizer confirms identity and all the information included

in the Drawdown Request Set Up and Authorization Form and such other information as requested by the Bank, the Bank will approve the request for a drawdown request set up. The authority of a person to verify or confirm information included in a Drawdown Request Set Up and Authorization Form shall be presumed if the Bank calls the phone number listed on the Signature Card for an Initiator or Authorizer, as applicable, or at such other phone number as designated by the Customer to the Bank in accordance with Paragraph 15 of this Electronic Payments Security Access Circular and the person who answers the phone verifies identity and confirms all of the information included in such Drawdown Request Set Up and Authorization Form. Any inbound drawdown request that originates from the Originating Bank that matches the debiting FHLB account and crediting Beneficiary account approved on the Drawdown Request Set-up Form will be authorized without further approvals and the referenced account at FHLB will be debited. These authorizations will remain in effect until revoked in writing by an authorized Initiator or Authorizer as identified on the Signature Card.

7) **WIRES PROCESSED THROUGH THE TELEPHONE.** Requests for wire transfers initiated by an Initiator through the telephone will require the caller to provide:

- His or her name
- A one-time passcode to verify identity
- A valid and activated PIN
- Repeat code, if applicable
- Account to be debited
- Amount of the wire
- Any additional information that may be required for non-repetitive wire transfer requests.

If the one-time passcode, repeat code (in the case of a repetitive or semi-repetitive wire transfer request) or the number of the account to be debited (in the case of non-repetitive wire transfer requests) is invalid, then the Bank will inform the Initiator on the telephone that the wire transfer request will not be accepted. For every non-repetitive wire transfer request initiated by an Initiator through the telephone, the Bank will perform a callback to an Authorizer (in accordance with the procedures set forth in Paragraph 10), other than the Initiator requesting the wire transfer of funds, a one-time passcode will be sent to the Authorizer's email on file to confirm the Authorizer's identity, confirm valid PIN, and approve the wire transfer request.

8) **WIRES PROCESSED THROUGH SECURECONNECT.** Requests for wire transfers processed through SecureConnect will be governed by the Master Transactions Agreement, this Electronic Payments Security Access Circular, Correspondent Product Services Guide, and the Wire Transfer System User's Guide, all of which may be amended, restated, modified, or replaced from time to time. Information concerning the security requirements surrounding the use of SecureConnect for requests for wire transfers can be found in the Wire Transfer System User's Guide, as in effect from time to time. All non-repetitive wire transfer requests initiated via SecureConnect will require a "Secondary Authorization" which is not from the Initiator.

9) **WIRES IN EXCESS OF AN INITIATOR'S AUTHORITY.** Wires more than an Initiator's authority will not be permitted. If the amount of a wire transfer request exceeds the dollar limit for the Initiator initiating the wire transfer request, the wire transfer request will not be accepted.

10) **CALLBACKS.** As previously identified in this Electronic Payments Security Access Circular, in connection with certain wire transfer requests the Bank will perform a callback to an Authorizer at the phone number listed on the Signature Card for such Authorizer. A one-time passcode will be sent to the Authorizer's email on file to confirm the Authorizer's identity. If the individual who answers the Bank's call to the phone number listed on the Signature Card for an Authorizer is not the Authorizer and (b) directs the Bank to call the Authorizer at an alternate telephone number, the Bank, for that wire transfer request only, will call the Authorizer at the alternate telephone number in accordance with Paragraph 15 of this Electronic Payments Security Access Circular. In all cases (including when an Authorizer calls the Bank directly, when an Authorizer answers the Bank's callback at the phone number listed on the Signature Card for that Authorizer, and when the Bank is directed to callback an Authorizer at an alternate phone number), the Authorizer will need to provide his or her name, one time passcode to verify identity, his or her PIN, and any additional information that may be required to confirm the wire transfer request. In addition to performing the callbacks specifically identified in this Electronic Payments Security Access Circular, the Bank may, at the Bank's discretion, call an Authorizer to verify the authenticity and accuracy of any of the Customer's wire transfer requests. If the Authorizer receiving the callback is unable to verify identity, provide his or her PIN and verify the wire transfer request(s), the Bank may refuse to accept the wire transfer request.

11) **SPECIALLY DESIGNATED NATIONALS AND OFAC.** Every outgoing wire transfer requested by the Customer and every incoming wire transfer received for the benefit of the Customer whether processed through a telephone call, through SecureConnect, through a PDF, or through any other means will automatically be passed through a scanner looking for specially designated nationals ("SDN"). If the scanner responds with a potential positive match, the Customer agrees to provide any additional information available to the Bank to verify the wire does not violate any rule, regulation, or order of

such agency. e If the Customer is unable to provide sufficient details to determine the match is a false positive to a name listed on the Office of Foreign Assets Control ("OFAC") SDN list on an outgoing wire transfer request then the Bank shall not process the outgoing wire transfer request, shall freeze the funds, and place them in a restricted interest-bearing account, and shall notify OFAC Compliance of the positive match unless the Bank, in accordance with its policies and procedures and in its sole discretion, determines to permit such wire transfer. If the scanner responds with a positive match or the Customer is unable to provide sufficient details to determine the match is a false positive on an incoming wire transfer, then the Bank shall accept the incoming wire transfer and place the funds from the incoming wire transfer in a restricted interest-bearing account and notify OFAC Compliance of the positive match.

The Customer hereby warrants that it will maintain its own filter to test each wire transfer request initiated against the list of prohibited names maintained by OFAC, and further warrants that it will not request any wire transfer which, if accepted by the Bank, will cause the Bank to be in violation of any rule, regulation, or order of such agency or subject the Bank to any sanction imposed by such agency. All penalties imposed by OFAC on the Bank for any violation caused by the Customer's breach of this Paragraph 11 will be passed on to the Customer. The Customer agrees it will indemnify, defend, and hold harmless the Bank against any loss or cost arising from the Customer's failure to screen its funds transfers.

12) **RECEIPT OF ACH TRANSACTIONS TO A CUSTOMER'S DDA.** All DDAs, opened by an individual listed on the Customer's Signature Card or Corporate Certificate of Authority, are eligible to receive ACH debits and credits without having additional agreements on file with the Bank. The Bank acts a Receiving Depository Financial Institution ("RDFI") for the Customer, and the Customer is deemed the Receiver as outlined by the ACH Rules of the National Automated Clearing House Association ("NACHA"). The rights and obligations of the Receiver concerning any Entry are governed by and construed in accordance with the laws of the State of Texas as provided by the operating rules of NACHA and Federal Reserve Banks ("Reserve Banks") Operating Circular No. 4 which are applicable to ACH transactions involving your account. Note that the Federal Reserve Banks may provide features or services under appendices to Operating Circular 4 that involve the use, disclosure or sharing of information amongst banks and the Reserve Banks as more fully described in such appendices. By Customer's use of its DDA, Customer consents to such sharing of information in connection with ACH activities in its DDA. Customer authorizes the Bank to share information with the Reserve Banks and authorizes the Reserve Banks to use and disclose information as described in the appendix to Operating Circular 4, in each case without further consent of or disclosure to any person.

The Bank cannot restrict an account from receiving ACH entries as the Bank is required to accept Entries that comply with all operating rules. The Bank may rely solely on the account number contained in an Entry for the purpose of posting the Entry to a Receiver's account, regardless of whether the name of the Receiver in the Entry matches the name associated with the account number in the Entry. The Customer should examine their Demand Deposit Account statement daily to monitor for ACH activity and notify the Bank of any alleged unauthorized debit activity. Any unauthorized or refused debit Entry can be returned by the Customer by completing the Written Statement to Return or Modify ACH Transaction form and providing it to the Bank with sufficient time to return the Entry within two Banking days from the date of the entry as required by NACHA rules.

13) **OTHER AGREEMENTS.** Except to the extent inconsistent herewith, the terms and conditions of the Master

Transactions Agreement between the Bank and the Customer shall apply to this Electronic Payments Security Access Circular as though set forth expressly herein.

14) **CHANGE OF PROCEDURES OR FEES.** The Bank may change procedures for handling wire transfer or ACH requests, as set forth in this Electronic Payments Security Access Circular or any other materials provided to Customer, at any time with ten (10) business days' prior notice, in writing or by a transmission in electronic or other form, of such change given to the Customer. Notice shall be deemed given to Customer if posted on the Bank's website or on the Bank's private internet network made available to Customer.

Customers will pay fees according to the Bank's fee schedules in effect from time to time. The Bank reserves the right to change the fee schedules at any time with thirty (30) calendar days' prior notice, in writing or by transmission in electronic or other form, of such change given to the Customer. Notice shall be deemed given to Customer if posted on the Bank's website or on the Bank's private internet network made available to Customer.

15) **CHANGE OF PHONE NUMBERS AND ADDRESSES.** The Customer may request that for a specified day the Bank contact an Authorized Individual at a telephone number or address other than as designated on the Signature Card for such Authorized Individual by sending the Bank an original or PDF of a letter asking the Bank to make such change(s) for that day on the Customer's letterhead signed by a person authorized by the Customer's board of directors in certified resolutions, COI or CCA, provided to the Bank whose signature is on file at the Bank. The letter must provide the name of the Authorized Individual as it appears on the Signature Card, provide the new telephone number and/or new

address at which the Bank should contact such Authorized Individual, and provide the date on which the Bank should contact such Authorized Individual at such new telephone number and/or new address.

16) **FORCE MAJEURE.** At any time during or after a hurricane, flood, tornado, act of God, war, explosion, or other similar event beyond the Bank's or the Customer's control occurs, the Bank may, in its sole discretion and without notice to the Customer, waive and/or change the procedures for handling wire transfer or ACH requests set forth in this Electronic Payments Security Access Circular in order to address the Customer's needs in the face of such events.