FIFTH THIRD

38 Fountain Square Plaza
Cincinnati, Ohio 45263

Security Procedures for Commercial Wire Transfer, Automated Clearing House Services, and Instant Payments

The Treasury Management Services ("Services") offered by Fifth Third Bank, N.A. ("Bank") give Customers the opportunity to select the Services that best meet their business needs. This explanation of Bank's Security Procedures for Commercial Wire Transfer, Automated Clearing House (ACH) Services, and Instant Payments is intended to offer Customer a high-level understanding of the requirements and recommendations for secure authentication of Instructions received by Bank from Customer for the various Services available from Bank. These procedures shall be considered "Security Procedures" as defined in the Master Treasury Management Agreement (the "Master Agreement"). Unless stated otherwise in these Security Procedures or the Implementation Materials, Bank will have no obligations under the Security Procedures, and Customer agrees that failure by Bank to use or comply with any Security Procedure shall not excuse Customer from its obligation to pay Bank the amount of any Payment Order for which Customer is otherwise liable. Bank may implement different or additional Security Procedures for use by Customer from time to time upon notice to Customer, and Customer's continued use of the Services and implementation of those additional Security Procedures shall be Customer's agreement to such Security Procedures. Any capitalized terms not defined herein shall have the same meaning as set forth in the Master Agreement or Online Channel Access Agreement ("OCAA"), as applicable.

1. AUTHORIZED AGENTS & SETUP

In the setup process for the Wire Transfer Service and ACH Service, and the other Services for the origination of Payment Orders, as permitted by Bank from time to time, Customer (also referred to herein as "*you*") and authorized persons acting on Customer's behalf (each, a "*Designator*," defined as an Authorized Person from Customer's account resolutions), designate to Bank those individuals as *Authorized Agents*, including Customer's Channel Administrator, and such term includes all Designators who have the authority on Customer's behalf for the following: (A) to originate Payment Orders (including wire transfers, ACH Entries, and Instant Payments) to Bank for execution; (B) for certain means of communication, to confirm or verify Payment Orders; (C) to transmit and confirm ACH Files to Bank; (D) to originate and confirm other types of Payment Orders for the Services that Customer enrolls in; and (E) to serve as a principal contact for any confirmations Bank may seek as described herein below.

Customer will indicate such authorization to Bank on Implementation Documentation that Bank supplies to Customer for that purpose or on other forms that Bank approves for this purpose. Customer understands that Bank will rely on all Payment Orders and other Instructions from the Authorized Agents. The procedures described herein below are "Security Procedures" as that term is defined in the Master Agreement for the wire transfer instructions, ACH Entries/Files, and any other Payment Orders resulting in electronic funds transfers, including any Instant Payments Request and other Services offered by Bank from time to time, sent to Bank in Customer's name.

2. INTERNET-INITIATED TRANSFERS

A. Service Setup

If you wish to communicate wire transfer instructions, or transmit or confirm ACH Files, or any other types of Payment Orders, to Bank via *Fifth Third Direct*, Customer must execute an OCAA. Customer must have in place a Channel Administrator (as that term is defined in the OCAA). For information on setting up channel administration, instructions for designating the Channel Administrator, and the scope of the Channel Administrator's authorities, please see the OCAA. Each User authorized by the Channel Administrator is considered an Authorized Agent for purposes of the Services enrollment and authorization granted to Users and other Channel Administrators through *Fifth Third Direct*.

The Channel Administrator has the option to require "*Dual Administration Control*," meaning that the approval of a second Channel Administrator is required to verify the designation and authorization of another User for the Wire Transfer and ACH Services. Bank strongly recommends and may require that you select the option of Dual Administration Control and Dual Transaction Approval, which are more fully described in Section 3 of the OCAA.

Customer acknowledges that the Channel Administrator's authorities include, but are not limited to, issuing Instructions, entering into transactions, originating, confirming, amending or canceling Payment Orders, adding or removing Users, establishing the authority of Users, agreeing upon or declining and waiving the use of Security Procedures. A Channel Administrator will also have the ability to, through the use of *Fifth Third Direct*, to designate additional Administrators with the same level of authority as the Administrator Customer designates. Bank shall only act upon an order from the Channel Administrator using its established Security Procedures to verify that the Channel Administrator provided the order. <u>To help reduce the risk of unauthorized activity on the Accounts, Bank recommends that Customer designate at least two (2) Channel Administrators so that when a Channel Administrator creates or modifies Users or their entitlements, another Channel Administrator must review and approve these actions. By waiving use of at least two Administrators to make additions and changes, Customer accepts the risk and liability associated with Bank accepting instructions that are purportedly from the single Channel Administrator or received through the use of the Security Procedures assigned to the single Channel Administrator.</u>

Credentials (as defined in the Master Agreement) are required for all Wire and ACH originations (and other types of Services for the origination of Payment Orders offered by Bank from time to time) for the origination and approval of Payment Orders through *Fifth Third Direct*, in order to provide two-factor authentication. Credentials are provided to Users as directed by the Channel Administrator.

If Customer wishes to communicate Instant Payments requests (or other Payment Orders as permitted by Bank from time to time) to Bank via API, Customer must execute an OCAA to establish the API as your Access Channel for such services. Customer will be responsible for securing authentication Credentials including access tokens, and configuring its infrastructures and applications appropriately to access Bank's API and to handle exception scenarios. Customer is also responsible for managing its users/systems/applications access including users and approvers' access when applicable, and application access.

B. Internet Wire Transfer Instructions

I. ***Procedure*** Bank will supply to the Channel Administrator a User ID and an initial login password, which must be changed upon logging in the first time. The Channel Administrator can then designate and establish Credentials for Users. All Users are assigned a unique, system-generated User ID that identifies them to the system and a confidential password which must be changed upon initial login. Both ID and password must be entered correctly to gain access to *Fifth Third Direct*, and if that User has been provisioned for wire transfers, to the wire transfer module within *Fifth Third Direct*. Users will also be required to enter a passcode generated by Credentials assigned to the User.

II. ***Controls*** As described in the OCAA, the Channel Administrator has the option to require Dual Control Administration in *Fifth Third Direct* for the approval of any changes made in the Administrator section of *Fifth Third* Direct, as described in more detail above. The Channel Administrator also has the option to setup Dual Transaction Approval and "*Approval Workflows*," which allow an Administrator to require as many approvers as they desire for any Payment Orders using the Services. Users can also be provisioned to initiate only selected types of Payment Orders, or Payment Orders only from selected Accounts as determined by the Administrator. Dual Administration Control can also be added to require a second approval for any changes made to Approval Workflows. Dual Control Administration and the creation of Approval Workflows can be important tools for addressing unauthorized wire activity.

<u>Dual Transaction Approval / Dual Administration Control.</u> Bank recommends that Customers originating wire transfers or ACH Entries (or other Service for the origination of Payment Orders where available) use Dual Administration Control or Dual Transaction

Approval to originate and approve or release wire transfers, ACH Entries, and other electronic funds transfers. Dual Administration Control means that a second Channel Administrator is required to verify the designation and authorization of an additional User. Dual Transaction Approval means that one User originates the wire transfer, ACH Entry or other Payment Order, and another User releases or approves the wire transfer, ACH Entry or other Payment Order for processing (a “Secondary Authorization”). Separate Users will have unique Credentials and should perform their approvals on separate devices to eliminate the ability of one person to unilaterally complete an electronic funds transfer. Dual Administration Control or Dual Transaction Approval shall be deemed a Security Procedure.

The Bank strongly recommends the implementation of these controls. The Customer is responsible for enabling and informing the Bank of Customer’s desire to enable Approval Workflows and/or Dual Administration Control and Dual Transaction Approval.

III. ***Recommended Customer Measures*** Among the many measures that Customer should employ to prevent unauthorized transactions, Bank strongly recommends that Customer download and properly utilize internet security software to aid in fraud prevention.

IV. ***Effect*** Bank will conclusively presume that all Payment Orders submitted through *Fifth Third Direct* using these procedures were authorized by you. The authority of a User may be withdrawn or modified through the Administrator through *Fifth Third Direct*. If you wish to revoke the authority of a User upon termination of employment or responsibility or for any other reason, the Administrator must delete such authorization within *Fifth Third Direct*. A User’s credentials are intended for that User and may not be transferred. You are solely responsible for controlling the use of a User’s credentials.

C. Options for Electronic Submission of ACH, Instant Payments & Wire Entries/Files

I. ***Data Exchange via Fifth Third Direct*** Users can upload ACH Files, Instant Payments or Wire Transfer files containing multiple Payment Orders per file, through *Fifth Third Direct*. A User with the necessary entitlements is required to transmit ACH Files to the IP Address/Port that Bank designates, and log in using a recognized User ID and password for this method. If the Channel Administrator has established Dual Transaction Approval, a second User is required to approve the transmission. The User (or, if Dual Transaction Approval is in effect, both Users) is also required to use the Credentials and enter a security code generated by the Credentials.

II. ***Payments and Transfers via Fifth Third Direct*** Users so enabled by the Channel Administrator can initiate ACH Entries and Wire transfers via the Payments and Transfers module in *Fifth Third Direct*. A User with the necessary entitlements is required to login using a recognized User ID and password. If the Channel Administrator has established Dual Transaction Approval, a second User is required to approve the transmission. The User (or, if Dual Transaction Approval is in effect, both Users) is also required to use the Credentials and enter a security code generated by the Credentials.

III. ***Direct Send Transmission*** This is a direct transmission to Bank’s servers via Secure File Transfer Protocol (SFTP). Prior to sending any Payment Orders, Bank will establish with Customer the public keys to be used for transmission. Customer’s Authorized Agent will be required to log in using the recognized User ID and password. Customer’s Authorized Agent will then confirm debit and credit totals (Authenticate) by one of the means described in Section II.C.3.ii below.

i. **Authentication of Direct Send Files:**
Bank requires that Customer authenticate all Direct Send Files. File Authentication requires the entry of the total debit and credit amounts of all ACH, Instant Payments & Wire files. Bank will compare the communicated totals to the corresponding ACH, Instant Payments and/or Wire file, and if they match, Bank will release the associated file(s) for processing. If they do not match, Bank will contact the Authorized Agent designated by the Designator in the set-up process to investigate and seek confirmation of the authenticity of the transmission. Further instructions for submitting the ACH authentication may be found in the ACH Operations Reference Information Customer Guide Bank provided to Customer.

ii. **File Authentication:**

a. *Fifth Third Direct* The Channel Administrator is automatically set up for File Authentication and has the authority to establish Users with similar authority. Each User is required to enter their User ID and password to initiate authentication and transmit the control totals.

b. *Electronic File Authentication* Electronic File Authentication allows you to submit a separate file of control totals through secure FTP separate from the ACH and/or Wire file. The confirmation is sent using the same method as the ACH and/or Wire File. This is a one record file.

c. *Telephone File Authentication* An Authorized Agent (as described in Section III.A below) can authenticate an ACH File by calling Fifth Third Commercial Support (1-866-475-0729 Press 2,1) and entering the PIN then the control total as prompted. ***This file authentication method can be only used for ACH files and is not permitted for Wire files.***

IV. ***API*** This is an internet-based Access Channel to send API requests to our gateways in accordance to specifications defined by the Bank. Bank will provide your Authorized Agent with Credentials to obtain an access token that is entitled to a specific Service or API functions. Your Authorized Agent will then use the access token to send API requests.

i. **Supported Products**

a. The API Access Channel is currently available as a Security Procedure for Instant Payments but may be offered by Bank to Customer for additional Services from time to time in Bank's discretion.

ii. **Authentication**

a. The API Access Channel uses a token-based authentication protocol to ensure secure access for all customers. Unique Client ID and Client Secret as Credentials will be provisioned to obtain Access Tokens at the time of onboarding.
b. Bank will require Customer to determine IP addresses from which Customer is originating such Payment Orders or other transactions as permitted by Bank.
c. Bank has developed an appropriate token management process to secure all Access Tokens. Only valid tokens will be accepted for API calls.

3. TELEPHONE WIRE TRANSFER REQUESTS

A. Service Setup

If Customer elects to send Payment Orders to us Bank telephone with the use of a Personal Identification Number ("PIN"), a Designator must complete, execute and submit to us a service form for telephone authorization. In that form, you will designate the Authorized Agents who shall have the authority to initiate wire transfers using our telephone PIN process. In the form, Customer may limit the authority of any Authorized Agent by dollar amount. Customer may also require that the Payment Order always be subject to a second PIN. For example, Customer may limit the authority associated with any PIN by dollar amount or function (callback/verification only). Customer is responsible for notifying Bank in the event of any changes in Authorized Agents. PINS may be revoked but under no circumstances may they be transferred.

B. Procedures

Bank will provide to each Authorized Agent designated for telephone PIN authority a PIN assigned by Bank. PINs are mailed directly to the Authorized Agents and must be confirmed annually. If not confirmed, the PIN may no longer be valid. The PINs must be entered into our system to initiate Payment Orders by telephone. Bank may, but is not obligated to, tape or otherwise record telephonic payment order requests and confirmations.

C. Approval

I. For all domestic and international non-repetitive wires initiated by telephone using a PIN in an amount greater than $250,000, Bank requires approval of the initiation by an Authorized Agent or User with a PIN designated by Customer for approvals, someone other than the initiator. Such confirming Authorized Agent or User must have authority to approve wires in an amount equal to or greater than that being initiated. Bank will call one such individual at the number specified for the Approver in the PIN Form and Bank will require they provide their PIN and confirmation of the non-repetitive wire. Bank will not seek approval for telephone payment orders of less than $250,000 unless Bank is instructed to do so by Customer via a service form denoting the intended lesser wire payment value denominations.

II. For Payment Orders initiated by telephone that are $250,000 or less and all repetitive Payment Orders regardless of size or approval, the holder of PIN may submit the Payment Order, and no further approval is required unless specified by the Customer.

D. Duration

Until a Designator gives Bank notice in writing and signed by such Designator that an Authorized Agent is no longer authorized to act as designated, and Bank has had a reasonable opportunity to act on that notice, Bank will conclusively presume that any caller possessing the appropriate PIN and authorization for an account is Customer’s Authorized Agent, and wire transfer instructions and approvals from such callers will be considered authorized by Customer.

4. AUTOMATED STANDING WIRE TRANSFER AND WIRE TRANSFER DRAWDOWN REQUESTS

A. Service Setup

Standing Order Wire and Wire Transfer Drawdown Requests may only be communicated to us in writing pursuant to a service form provided to Customer by Bank, and executed by an Authorized Agent and returned to Bank for attachment to and submission with the appropriate service form. Such service form must contain the following information: (1) receiving bank name; (2) receiving bank ABA number; (3) beneficiary account number; (4) beneficiary account title; and (5) amount to be transferred.

B. Effect

Once the requisite form has been received and processed by Bank, individual wires pursuant to the form are not subject to further verification or approvals.

C. Duration

Bank will continue to execute the Standing Order and Drawdown Requests until the order or request is canceled by Customer through an Authorized Agent in writing and signed by such Authorized Agent identifying the Standing Order or Drawdown Request with the information listed above. Bank will conclusively presume that any Standing Order or Drawdown Request received from an Authorized Agent is authorized by Customer. Customer can obtain a listing of established Standing Orders and Drawdown Requests upon request. Bank urges Customer to periodically review all established Standing Orders and Drawdown Requests for currency and continued validity and immediately report any changes or problems to Bank by contacting an Authorized Bank Representative.

5. MANUAL WIRE PROCEDURES

A. CAUTION

Bank recognizes that there may be circumstances under which a Customer may wish to submit a written request for a wire transfer to, or call, an authorized Bank employee associated with the relationship with Customer (an "*Authorized FTB Person*") to request a wire transfer. ***Bank strongly recommends that Customer utilize this manual procedure only when one of the communication methods described above is unavailable, such that Customer may take advantage of the greater security afforded by the other above-described methods.*** The manual procedures carry higher risks of unauthorized activity.

If Customer chooses to use this higher risk procedure, Customer is rejecting the procedure Bank recommends and Customer assumes all risks of unauthorized activity through this method of communication. Customer will be required to sign a waiver of security procedures if the manual wire procedure is used.

B. Written Authorization

Although Customer may call an Authorized FTB Person to discuss the initiation of a manual wire request, Bank cannot accept or initiate such a request until Bank has received, by email or in person, an appropriately executed Outgoing Wire Transfer Request Agreement (*"Outgoing Wire Agreement*") and written authorization. Before a manual wire may be initiated, a Designator (or an Authorized Individual designated on the Account Resolution) must execute an Outgoing Wire Agreement and provide the same to Bank. If Bank has a valid Outgoing Wire Agreement, and the authorization provided therein has not been revoked, the designated individuals may initiate a wire by providing us the payment order in person or via e-mail (a "Customer Manual Request"), and the following procedures shall apply:

I. One of the persons designated in the Outgoing Wire Agreement must provide to an Authorized FTB Person, via email or in person, the Customer Manual Request that includes the following information: (a) receiving bank name; (b) receiving bank ABA number; (c) beneficiary account number and title; (d) amount to be transferred; and (e) the signature of a Designator or Account Signer.

II. Bank will verify the name and authority of the individual purportedly signing the Customer Manual Request with the name and authority of the individual(s) in the Outgoing Wire Agreement as Authorized Agents for Customer's originating electronic funds transfers.

III. If Bank in good faith believes the name and authority:

- **i. Match**, then an Authorized FTB Person will perform confirmation steps, which will include one or more of the following:

    - *a.* Callback to a secondary individual that is evidenced on Bank's records for the Account (preferably an individual that is not the initiator of the manual wire transfer); and/or, *b.* Telephone confirmation by presentment of a series of in- and out-of-wallet security questions presented to the initiator at the time of the phone request.

Failure to carry out either method of confirmation will result in the Payment Order being deemed to have been canceled prior to acceptance by Bank and Bank shall not be required to execute the Payment Order.

ii. Do not match, then Bank will not execute the Payment Order. Bank will call an Authorized Agent to explain and request that a new Outgoing Wire Agreement be submitted with a signature Bank has on file in order to complete a verification of authority as set forth above.

IV. ***NOTE*** *Alternative Payment Order Initiation Procedures*. If, notwithstanding the Security Procedures above that are offered and recommended by Bank as commercially reasonable, Customer requests to originate Payment Orders resulting in funds transfers using the Manual Procedure, without a Secondary Authorization or Security Procedures offered and recommended by Bank, Customer must complete a Dual Control Security Waiver or other waiver requested by Bank and signed by an Authorized Agent of Customer. Customer shall be deemed to have waived the Security Procedures offered and recommended by Bank the alternative Security Procedure adopted by Customer shall be deemed to be commercially reasonable for the types of Payment Orders originated and funds transfers made by Customer. Bank recommends against a waiver of Dual Control or other Security Procedures as set forth above.

6. FIFTH THIRD BANK APPLICATIONS

A. Transaction Monitoring

Fifth Third Bank may subject each initiated wire, each initiated Instant Payment, and each ACH Entry submitted through *Fifth Third Direct*, to our proprietary electronic funds transfer analysis software applications. The analysis performed by this software evaluates a variety of factors relating to each transaction, which evaluation may trigger a halt or delay on a transfer that may lead to a follow-up call from an Authorized FTB Person to an Authorized Agent in order to take necessary action with respect to the matter that triggered the halt or delay. Bank will not release any affected payment until such time as Bank receives any necessary confirmation that Bank seeks. ***Please note that our analysis and potential follow-up are <u>NOT</u> a part of or a substitute for the Security Procedures or Customer's proper account and security management and may not be relied upon by Customer in any way.***

B. Limits on Transaction Amounts and Types

Customer may implement transaction limits on the type or amount of transactions that may be made on a daily basis. These transaction limits may be set at the Account and overall dollar amount of transactions (Payment Orders) on all Accounts and may be permitted for certain types of transactions. Users will be blocked from approving Payment Orders that exceed limits imposed by Customer. In the event that Customer must exceed any of the limits, Bank requires that Customer raise or remove such limits by submitting replacement Implementation Materials (or other documentation as required by Bank) that is purportedly executed by an Authorized Agent of Customer. <u>Bank recommends that Customer implement transaction limits as part of its procedures</u>. ***Please note that the ability to set transaction limits, and adherence to such limits, is for the protection of the Bank, and <u>NOT</u> part of the Security Procedures, not a substitute for the Security Procedures or proper Account and security management by Customer, and may not be relied upon by Customer in any way.***