Cash Management User Guide

Paraguay

Treasury and Trade Solutions

citi

Table of Contents

I. Introduction 3

II. Payment Services 4

A. Types of Payment Services in Paraguay 4
B. Sending a Payment 4
C. Revocation, Modification and Rejection of Payments 5
D. Payable Checks 5
E. Availability of Payments 7

III. Receivables Services 8

A. Receiving an ACH Payment 8
B. Cash & Check Deposits Channel 8

IV. Manual Initiation of Instructions 10

V. Information Services: Data Aggregation- Infopool 13

A. Consolidation Service 13
B. Procedure 13

VI. TTS Consolidated Security Procedures – Same (always use the last version) 14

A. Security Manager Roles and Responsibilities* 14
B. Authentication Methods 16
C. Data Integrity and Secured Communications 19

VII. Other considerations - Fees and Interest 20

VIII. Conclusion 21

I. Introduction

Thank you for choosing Citi's Treasury and Trade Solutions (TTS) for your cash management business needs. The objective of this Cash Management User Guide (Guide) is to provide you with a manual containing detailed information of Services available to you and is to be read together with your Account terms and conditions. In this Guide, Citibank N.A. Paraguay Branch, Citi and Bank may be used interchangeably. This Guide may be updated from time to time and any changes will be communicated through our regular channels.

II. Payment Services

Payments can be instructed through the following channels: CitiDirect BE® and CitiConnect®.

A. Types of Payment Services in Paraguay

- Domestic Funds Transfers Interbank electronic transfers payment system.
- Real Time Gross Settlement (RTGS): Transfers of funds, large or small, on a real-time basis to accounts at other domestic financial institutions
- Book to Book: Transfers between Citi accounts. The bank offers the option of automatic transfers within checking account and savings account, with a requirement of a minimum monthly amount to be maintained in said accounts.
- Cross Border Funds Transfers (International transfers): Allow Customers to transfer funds to accounts in other countries in different currencies using wire transfers.
- Checks: Negotiable paper-based instruments that can be passed from one person or entity to another and exchanged for money. A check unconditionally instructs a bank to pay a specific amount in a specific currency to a specified person, to a “bearer”, or to “cash”. (See Section E below)

B. Sending a Payment

1. The Customer instructs Citi to pay the beneficiary through CitiDirect BE®, CitiConnect®, or SWIFT using files or a user interface, or via a Manually Initiated Funds Transfer (MIFT), prior to the cut-off time. The instruction must be irrevocable and formatted according to market specifications and as outlined during the implementation stage.
2. Citi forwards the instruction to the relevant payment system for further processing.
3. The payment system forwards the instruction to the beneficiary bank based on the locally defined clearing cycle.
4. The beneficiary bank then credits the beneficiary account.

The Customer may require one or more authorization levels for payments and may establish different approval limits. All transactions require at least one originator and one user with the appropriate approval level. Each authorized approver is issued and must use a unique identification code and a dynamic password, or other procedure defined by Citi. The security of payment information is provided through Customer-controlled authorizations and by Citi’s internal security system. The Customer must designate those users who may initiate and approve transactions carried out through CitiDirect BE®. The Citi electronic platform includes up to nine levels of authorization. Payment instructions, however they are generated, must contain information about the payment beneficiary, the payment amount, the day on which the payment

is to be made, the person authorized to withdraw it, supporting documentation to evidence payment, among other data.

C. Revocation, Modification and Rejection of Payments

Each payment instruction confirmed by the Customer in CitiDirect BE® and/or CitiConnect® and received by Citi is irrevocable upon receipt of such instruction by Citi.

If the payment instruction for credit to an account has been sent to the intended beneficiary and the Customer wishes to revoke such instruction, a written request must be sent to Citi (signed by legal representative) to reverse the respective transaction. In such cases, Citi will put forth its best efforts to arrange for the pertinent entities to process the reversal. However, this does not imply any obligation whatsoever vis-a-vis the Customer or third parties (including Citi) for the result of such a process.

If the payment instruction has not been transmitted to the beneficiary (payment instructions with future date) the Customer may choose to cancel or to modify the payment instruction through the system (CitiDirect BE® or CitiConnect®).

D. Payable Checks

The following types of checks are available:

1. Cashier's checks (PayLink Checks): Checks instructed through the CitiDirect BE® platform to be issued in a specific local branch. The funds are debited from the Customer’s account at the time they are issued. The checks are issued from the Bank's own account and are instruments whose funds are guaranteed. This ensures the payment of the funds to the beneficiary, since they are reserved.

2. Standard checks Negotiable instruments, which can be passed from one person or entity to another and exchanged for money. Checks are drawn upon the Customer's account and are debited against the Customer's account when they are presented for payment at the cashier's window or through the clearinghouse. These checks are paid provided the issuer has sufficient funds to cover them.

3. Special checks (WorldLink® Checks): Check instructed through WorldLink for international payments, drawn against the branches where Citi has a presence, and issued in the local currency of that branch.

Issuance of Checks

Citi can manage the issuance of checks initiated by the Customer with negotiability or other legal restrictions, or as a crossed check, as it deems advisable.

The Customer instructs the bank to issue the PayLink® check(s) through the agreed electronic channel and the process defined by the administrator of the Customer's electronic platform.

Citi debits the funds from the Customer's account and prints the check(s) with a facsimile signature of the Bank's officer(s) and with the wording "Not Transferable"
If a check is not claimed within three months of issuance, Citi will proceed on the same date to process the credit for the pertinent amount to the Customer's account.

Delivery of Checks

Paylink Checks will be delivered according to the following procedures:

1. The beneficiary may go personally to the branch to cash the check or to deposit it in his or her account for collection through the settlement process, subject to the rules of the clearinghouse and the bank's internal policies.

2. For the delivery of checks whose beneficiary is an individual, the beneficiary must present to Citi his or her original citizen's identification document (ID) and a photocopy of it that Citi must retain as supporting documentation for the delivery of the check(s).

3. For the delivery of checks to an individual other than the beneficiary, Citi will deliver the check to the third party only with an authorization issued by any persons authorized to draw on the Customer's Account.

4. For the delivery of checks whose beneficiary is a legal entity, the request for check delivery must be made by an authorized who must present entity's certificate of existence, and evidence that he or she is an authorized representative of the legal entity. These documents should be notarized; he or she must provide the original and a copy of his or her citizen's identification document (ID).

5. When the person who requests the check delivery is an individual other than the entity's authorized representative, he or she must deliver to Citi:

    a. A power of attorney signed by the entity's legal representative, duly notarized and registered at the public records, identifying and authorizing the individual to claim the check and specifying the required identity document. A photocopy of the individual's citizenship ID and the original of the legal entity's certificate of existence must be attached, plus a copy of the ID document of the entity's legal representative.

    Checks will be delivered if the required documents have been attached to Citi's satisfaction. Before delivering the checks, Citi, if it deems necessary, may confirm beneficiary information by calling the telephone numbers registered by the Customer in Citi's system. Citi ~~may~~ can amend these check delivery procedures at any time and for any reason, subject to the respective notification terms.

Stop Payment Request on Payable Checks

1. The Customer may request that the bank stop payment on any payable check, in accordance with the bank procedures and applicable local laws.
2. The Customer communicates the stop payments instructions to Citi in writing. The stop payment instructions will specify the serial number of the check, the date of issue, the beneficiary's name and the amount and If checks or drafts are lost, stolen, destroyed, stale or invalid, the Customer must inform Citi in writing per the pre-agreed formats for stopping payments plus the police report Stop payment on checks will be processed based on the information specified in the stop payment instructions.
3. If the check to be stopped has not been paid, the Bank will refund the proceeds of all the stop payment requests and cancellations to the account from which the payments were derived, except in cases where the Customer requests a replacement payable check to be issued.

Citi will put forth its best efforts to arrange for the pertinent entities to process the reversal. However, this does not imply any obligation whatsoever vis-a-vis the Customer or third parties (including Citi) for the result of such a process.

E. Availability of Payments

Citi will inform the Customer of any change to the cut-off times and deposit hours.

- Checks: 1:30 p.m. on the business day prior to the transaction payment date.
- Local Interbank Transfers: 4:30 p.m. on the transaction payment date.
- Transfers between Citibank, N.A. accounts: 4:00 p.m. on the transaction payment date.
- Check cashing and deposit hours: Monday through Friday, 8:30 a.m. to 1:30 p.m.
- Cross Border Funds Transfer: Monday through Friday, 8:30 a.m. to 2:30 p.m. on the transaction payment date

III. Receivables Services

A. Receiving an ACH Payment

1. The clearing house forwards the instruction to Citi based on the locally defined clearing cycle.

2. Citi credits the account of the Customer.

Any rejections or returns by Citi will be credited back to the payer account. The reason for the return is communicated to the payer.

B. Cash & Check Deposits Channel

Citi customers in Paraguay may receive deposits at the Citibank, N.A. Paraguay Branch. Customers may also make deposits through our network extension with which Citi has correspondent agreement . Receiving Deposits in the Extended Network

1. Customers can make deposits at the branches of our correspondent banks. These deposits can be made in cash or with local checks, either in U.S. dollars or Guaranies. Cash deposits, in both currencies, are limited to the amounts specified by each correspondent bank agency.

2. Deposits in our extended network needs to be made in the accounts provided in the deposit slip. Citi will provide the customer with the deposit slips to be used to note deposit information. The deposit slips will be used to include the details of the deposit made, which will be clearly indicated on the deposit form or cash receipt delivered as evidence of the same.

3. All information referring to the deposits made through this service may be queried by the Customer through the CitiDirect BE®.

4. The Customer needs to include the number assigned to the Customer's account in the instructions and on all other forms used to make deposits. Citi can reject or reverse a deposit that does not display the correct account number or appropriate information.

5. The availability of funds deposited at any of our correspondent banks are available as follows:

    - Cash that is deposited will be available on the same day of the date of the deposit, if the deposit was made at a correspondent agency.

    - Checks deposited in correspondent banks will be released on the second banking business day following the date of the deposit. USD checks will be released on the third banking business day following the date of the deposit.

Direct Debit Collections

A direct debit collection is a financial transaction, the Bank withdraw funds from a payer's customer, via book to book transactions.

The Customer may authorize the Bank to debit its accounts for the purpose of crediting third-party accounts (public entities, mobile entities and others) for services they provide or for periodic payments due.

The Customer needs to instruct the Bank by letter, and to instruct the third-party service provider, to suspend or terminate service for all the debits made by a third party. In all cases of activation, suspension or termination of utilities or public services handled by a third party, the instruction must be sent to the third party for processing. The Bank will proceed to stop debits only after being notified by the service provider.

Debits will not be completed if there are no sufficient funds in the account, and in such cases the Bank will promptly notify the Service Provider and the Customer.

IV. Manual Initiation of Instructions

Citi offers its Customers the ability to initiate manual instructions or Manually Initiated Funds Transfer (MIFT) in the event of a contingency or other scenarios that may involve a manual instruction, including amendment, recall or cancellation of previous instructions.

To enable this capability, the Customer must complete the Global Manual Transaction Authorization (GMTA) form, which supplements the Master Account and Service Terms (MAST), and any other applicable account terms and conditions. The GMTA form must be signed by authorized signatories as listed in the Customer's Board Resolution or equivalent.

The GMTA form identifies those individuals who are authorized to initiate and confirm instructions by manual means, on behalf of the Customer.

Customers who do not provide a GMTA form to Citi, and therefore do not have MIFT payment capability, understand that manual means of communication will not be available to them in the event they are required for contingency or other applicable scenarios that may involve manual instructions.

Additionally, Citi shares concern about operational risk related to sending physical letters to Citi offices, enabling Customers to send manual instructions via CitiDirect BE® as scanned images. To enable this capability, the Customer must request the Manual Payments solution package in CitiDirect BE® Activation Form, where it should indicate which CitiDirect BE® users will be granted this profile and how they can send manual instructions.

Manual Payments through CitiDirect BE (Pagos Manuales Virtuales)

1. The Virtual Manual Payments service allows the Customer to enter, see, and authorize instructions via images (letters) through the CitiDirect BE®, CitiDirect BE® Mobile, and CitiDirect BE® Tablet Electronic Banking system, using a secure transmission channel and following the current authentication processes (use of the Safeword Card/MobilePASS) as means of accessing and authenticating the users and processing (with preparer and approver levels previously requested and authorized by the customer).

2. The sending of instructions through the Virtual Manual Payments service is limited to the transactions that the Bank defines for this purpose.

3. Instruction images entered in the Virtual Manual Payments service must be previously signed by the Customer's authorized representatives and will follow the procedure established in the signature validation account contract.

4. The images can only be processed in two format types: PDF and JPG

Notes for Completing the GMTA Form

1. The manual instruction can be sent to Citi via either one of the following communication modes. Please select the option(s) you want to activate in the GMTA form:
   - Letter
   - Fax
   - CitiDirect BE®
2. The initiators can be made available only with Option 1 in the GMTA form.
3. Please provide at least two call-back nominees. Citi recommends that the nominees be located in the same time zone as the country where the Customer's Account is located.
4. When completing the GMTA form, the Customer should list all account numbers that are to be enabled for manual processing on the GMTA Account Information Schedule.

Processing MIFT Instructions

In the event that the Customer requires Citi to process a MIFT instruction:

1. The Customer sends a manual instruction, duly signed, to Citi via the selected communication mode. For movement of funds from the Customer's Account, Citi recommends using the Citi standard manual payment form.
2. Upon receipt of the manual instruction, Citi carries out its internal verification, including but not limited to, reviewing for completeness of the required processing details and verifying the initiators' signature(s) against those provided in the Signature Card. The Customer should take care when completing the Citi standard form for manual payment as it may be rejected if it contains erasures/white-outs.
3. Citi ~~may~~can conduct an additional control by calling back the nominees included in the GMTA form, with the exception of instructions submitted in the Pre-Defined Beneficiary List Form, once they are initially set up. The call-back nominee and the initiator cannot be the same. Confirmation by telephone may be recorded by Citi.
4. Citi processes the manual instruction once Citi determines that all the verifications are successful.

The processing of the instruction is subject to Citi's internal procedures and conditions given that there are alternative electronic channels to perform such instruction.

Updates to Authorizations

If information provided in the GMTA changes, the Customer must submit a new GMTA form which supersedes the previous form. Changes for which Citi should be informed include, but are not limited to:

- Personnel changes
- Changes to a person's name (e.g., due to change in marital status)
- New telephone numbers (e.g., new phone number, new area code, or new city code)
- New account number

Neither a GMTA form detailing just the updated alone, nor a letter or any other form of document will be accepted. This is necessary to assure the operational integrity of the manual communication process.

Deletions to Authorizations

The Customer must submit the name(s) of the nominee(s) to be removed from the GMTA form in a letter on company letterhead and signed by authorized signatories as per the Customer's Board Resolution or equivalent. Again, in the interest of operational integrity, Citi will request a new GMTA form that will supersede all the previous GMTA forms if there are several signature deletions.

V. Information Services: Data Aggregation-Infopool

A. Consolidation Service

Infopool is a single interface to accounts with Citi and third-party banks. The Infopool Service allows daily monitoring of balances and transaction of accounts maintained in different banks across borders and currencies. Thus, Infopool Services consists of consolidating the information on the Customer's bank accounts and those of its subsidiaries on the books of Citi, Citigroup banks and/or on the books of other banks (hereinafter Third Parties), through the CitiDirect BE® electronic banking system.

Citi will only consolidate the information for the accounts indicated by the Customer on the activation form, without making adjustments to the information provided by its issuer and as such Citi is not responsible for the content or preciseness of the information on the accounts.

The Customer shall authorize Group or Third Party service provider banks to provide to Citi the account information, including personal data. It likewise authorizes Citi to receive this information and to process it.

The Customer has and retains all the rights, titles and interests in the accounts information and permits Citi to consolidate such account information for querying. Given the provision of the service, Citi will only consolidate the information on accounts established by the Customer, without adjusting the information provided by the issuer.

The Customer understands that Infopool is a global service, but some countries have personal data protection laws that limit the compilation, disclosure, processing or transfer of personal data and the account information may include personal data subject to the personal data laws of one or more countries.

B. Procedure

1. The Customer warrants that for each account, regardless of the identity of the account holder, the Customer has the right and is legally authorized to access the account information. Likewise, the account holder authorizes Citi to consolidate such information.

2. For the implementation of the Data Aggregation (Infopool) service the Customer shall submit the Account Reporting Request Form and confirm the submittal of the Infopool Sample Letter to the Citi Group and/or Third Party banks on whose books the accounts to be consolidated using this service are held.

3. Infopool users will be those defined by the Customer on the CitiDirect BE® application forms with the profile enabled for queries.

VI. TTS Consolidated Security Procedures – Same (always use the last version)

As referenced in the Communications section of the Master Account and Service Terms (or other applicable account terms and conditions) ("MAST") that has been entered into between the Customer and the Bank the following is a description of the security procedures ("Procedures") used by Citi Treasury and Trade Solutions in connection with the following Services or connectivity channels.

- CitiDirect BE® (including Electronic Bank Account Management ("eBAM")), TreasuryVision®, and WordLink®)
- Interactive Voice Response ("IVR")
- Fax with the Bank excluding Manually Initiated Funds Transfer (MIFT)
- CitiConnect
- Other local electronic connectivity channels

Availability of the Services or connectivity channels will vary across local markets. These Procedures may be updated and advised to the Customer by electronic means or otherwise from time to time. Customer's continued use of any of the above noted services or connectivity channels after being advised of updated Procedures (which may include, but is not limited to, the posting of updated Procedures on CitiDirect BE®, in connection with the service or connectivity channel) shall constitute Customer's acceptance of such updated Procedures. These Procedures are to be read together with the MAST as such MAST may be amended from time to time. Capitalized terms not otherwise defined herein shall have the meanings ascribed to them in the MAST.

A. Security Manager Roles and Responsibilities*

For the applications accessible in CitiDirect BE®, the Bank requires two separate individuals to input and authorize instructions; therefore, a minimum of two Security Managers are required. Any two Security Managers, acting in concert, are able to give instructions and/or confirmations through the connectivity channels in relation to any Security Manager function or in connection with facilitating our communication via the Internet. Any such Communications, when authorized by two Security Managers, will be accepted and acted on by the Bank. The Bank recommends the designation of at least three Security Managers to ensure adequate backup. The Customer shall designate its Security Managers on the TTS Channels Onboarding Form. A Security Manager of the Customer may also act as the Security Manager for a third party entity (for instance, an affiliate of the Customer) and exercise all rights relating thereto (including the appointment of users for that third party entity's Account(s)), without any further designation, if that third party entity executes a Universal Access Authority form (or such other form of authorization acceptable to the bank) granting the Customer access to its Account(s). This only applies in relation to Account(s) covered under the relevant authorization.

*Security Manager Roles and Responsibilities may be prohibited in certain local market. Please contact your Customer Service representative for further information

The Security Manager function includes, but is not limited to:

1. Establishing and maintaining the access and entitlements of users (including the Security Managers themselves), including activities such as:

    a. creating, deleting or modifying User Profiles (including Security Manager Profiles) and entitlement rights (please note that user name must align with supporting identification documents)

    b. building access profiles that define the functions and data available to various users; and

    c. enabling and disabling user log-on credentials.

2. Creating and modifying entries in Customer maintained libraries (such as preformatted payments and beneficiary libraries) and authorizing other users to do the same

3. Modifying payment authorization flows.

4. Allocating dynamic password credentials or other system access credentials or passwords to the Customer's users

5. Notifying the Bank if there is any reason to suspect that security has been compromised.

Security Managers also assign transaction limits to users for those Bank products to which the Customer has access. These limits are not monitored or validated by the Bank; Customer should monitor these limits to ensure in compliance with Customer's internal policies and requirements, including but not limited to, those established by Customer's Board of Directors or equivalent.

Specifically related to the **eBAM Application**, the following roles are required:

The initial set-up on the eBAM Service requires the designation of three Security Officers and one Corporate Secretary. Two separate Senior Administrative Roles act in concert as maker/checker to set up and assign User function/data entitlements and Workflows. These arrangements are not monitored or validated by Bank; Workflows and User activity are monitored by the Customer to ensure compliance with Customer's (and Account Owners') internal policies, requirements, and authorization and approval levels, including but not limited to those established by the Customer's (and Account Owners') Board of Directors or equivalent governing body.

The following roles are required for the eBAM Service:

1. **Security Officer:** Fulfil the functions described in 1. a-c above within the roles of Security Managers;

2. **Corporate Secretary:** Ensures that Workflows, Users set up as Designated Authorizers, and their assignment to Workflows meet internal policies, requirements, authorization and approval levels, as established by the Customer's (and Account Owners') Board of Directors or equivalent governing authority

3. **Designated Authorisers:** Have broad, senior authority to initiate and authorise workflow activities; and

4. **Request Initiators:** are individuals authorized to perform administrative activities such as entering account and signer management requests into the eBAM system.

The Security Officers, Corporate Secretary and Designated Authorisers are responsible for:

1. defining and administering hierarchy setup and site/flow control, such as establishing Workflows and identifying Users and levels of approval;

2. creating additional Senior Administrative Roles and appointing Users thereto (who may or may not be employed by the Customer)

3. notifying Bank if there is any reason to suspect that security or confidentiality of any User (including Senior Administrative Roles) credentials has been breached or compromised; and

4. where relevant, completing, amending, approving and/or supplementing such Customer implementation forms as may be reasonably requested by Bank from time to time in connection with the provision of services and/or products to Customer

B. Authentication Methods

The Procedures include certain secure authentication methods ("Authentication Methods") which are used to uniquely identify and verify the authority of the Customer and/or any of its users typically through mechanisms such as User ID / password pairs, digital certificates, and security tokens (deployed via hardware or software) which generate a dynamic password used to access the services or connectivity channels each time the Customer or a user logs in or authenticates themselves. Please note that availability of the Authentication Methods described below varies based on local markets.

Security Managers and all users who want to (a) initiate or approve transactions (and whose User Profile permits them to do so) and/or (b) access the systems in accordance with entitlements must use the available Authentication Methods (which may be updated from time to time as described above).

The following Authentication Methods are available to access the above-noted services or connectivity channels in combination with a User ID:

Authentication Method	Description

Token: Challenge Response	Either a (i) mobile application based soft token (e.g. MobilePASS) or (ii) physical token (e.g. SafeWord Card, Vasco) which in each case is used to generate a dynamic password after authenticating with a 4 digit pin. When accessing CitiDirect BE, the system generates a challenge, and a response passcode is generated by the utilized token and entered into the system.
Token: One Time Password	Either a (i) mobile application based soft token (e.g. MobilePASS) or (ii) physical token (e.g. SafeWord Card, Vasco) which is used to generate a dynamic password after authenticating with a 4 digit pin. This dynamic password is entered into the system to gain access.
SMS One-Time-Code	A dynamic password is delivered to a user via SMS, after which the user enters the dynamic password and a secure password to gain access to the system
Voice One-Time-Code	A dynamic password is delivered to a user via an automated voice call, after which the user enters the dynamic password and a secure password to gain access to the system
MultiFactor Authentication	A dynamic password is generated via a SafeWord Card or MobilePASS token, after which such dynamic password is entered along with a secure password to gain access to the system.
Digital Certificates	A Digital Certificate issued by an approved certificate authority which is used for authentication. Digital Certificates utilize a Key Storage Mechanism and a corresponding PIN, and may be issued by IdenTrust, SWIFT (3SKey) or other agreed-upon providers.
Secure Password	A user enters their secure password to access the system. A Secure Password typically limits a user's capabilities on the system, such that information can be viewed and no transaction capabilities are enabled.
Interactive Voice Response ("IVR") & email	Users contacting the bank will be prompted to enter a PIN number or provide other information to validate authorized access over the phone or over email.
Fax	Correspondence received by the Bank, excluding MIFT requests, will be signature verified based on the information that is contained in the Customer's board resolution.
MTLS	Mandatory Transport Layer Security (MTLS) creates a secure, private email connection between Citi and the external party. An email transmitted sent using this channel is sent over the Internet through an encrypted TLS tunnel created by the connection.
Secure PDF	Encrypted emails are delivered to a regular mailbox as a PDF Document that is opened by entering a private password, both the message body and any attached files are encrypted. A private password can be set up upon receipt of the first Secure Email received.

To learn more about any of these Authentication Methods, please refer to the Login Help page on CitiDirect BE (https://portal.citidirect.com/portalservices/forms/loginHelp.pser)

For CitiConnect®

- If the Customer chooses to use a public Internet connection to connect to Citi, including HTTPS, secure FTP, and FTPs, the Bank and the Customer will exchange security certificates to ensure both the communication channel and the messages exchanged are fully encrypted and protected. The Bank will only accept Communications originating from the Customer's secured communication gateway using the exchanged security certificates, and vice versa, and the Bank will only transmit Communications to the Customer's communication gateway using the exchanged security certificates.

- If the Customer chooses to use CitiConnect via SWIFT, then for any payment orders and instructions involving SWIFT, including amending or cancelling such orders, the Procedures that will be used to authenticate that a payment order or instruction is that of the Customer and authorized by the Customer shall be those as provided for in the SWIFT Contractual Documentation (as such term is defined by SWIFT and as may be amended or

supplemented from time to time) which includes without limitation its General Terms and Conditions and FIN Service Description or as set forth in any other terms and conditions that may be established by SWIFT. The Bank is not responsible for any errors or delays in the SWIFT system. Communications to the Bank are to be provided in the format and type required and specified by SWIFT.

- If using a VPN, both the Customer and the Bank will designate a single IP address from which Communications between the Customer and Bank will be sent and/or received. The Bank will only accept Communications originating from the Customer's designated IP address, and vice versa, and the Bank will only transmit Communications to the Customer's designated IP address, and vice versa.

- The Customer and the Bank may also use a Hardware Security Module Authentication to accompany VPN Authentication. This requires the Bank and the Customer each to install a device on the servers designated for Communications between the Bank and the Customer.

- The Bank requires:

  - Customer's safeguarding of the Authentication Methods including any log-on credentials and/or security certificates associated with the Authentication Methods (collectively, the "Credentials") and ensuring that access to and distribution of the Credentials are limited only to authorized persons of the Customer. The Authentication Methods and associated Credentials are the methods by which the Bank verifies the origin of Communications issued by the Customer to the Bank.

  - The Customer should take all reasonable steps to protect the Credentials. Accordingly, the Bank strongly recommends that the Customer does not share the Credentials with any third party.

  Certain jurisdictions may require individuals (and their corresponding credentials) to be identified as compliant with applicable AML legislation requirements before granting access to perform certain functions.

  The Bank understands that the Customer may, in some cases, wish to share the Customer's Credentials with a third party entity or service provider (including without limitation any third party payroll provider) designated by the Customer to have access to the Customer's Credentials (such third party entity or service provider shall be referred to herein as an "Authorized Third Party") for the purpose of accessing and utilizing CitiConnect on the Customer's behalf. In the event that the Customer elects to share its Credentials with an Authorized Third Party, the Bank strongly recommends that the Customer takes, and ensure that any Authorized Third Party takes, all reasonable steps to protect the Credentials from being disclosed to any non-Authorized Third Party personnel. The Bank is authorized to act upon any Communication that it receives from an Authorized Third Party on behalf of the Customer in compliance with these Procedures.

C. Data Integrity and Secured Communications

- The Customer will be transmitting data to and otherwise exchanging Communications with the Bank, utilizing the Internet, email and/or fax, which are not necessarily secure communication and delivery systems. The Bank, utilizes industry leading encryption methods (as determined by the Bank), which help to ensure that information is kept confidential and that it is not changed during transit.
- If the Customer suspects or becomes aware of, a technical failure or any improper access to or use of the Bank's services, connectivity channels or the Authentication Methods by any person (whether an authorized person or not), the Customer shall promptly notify the Bank of such occurrence. In the event of improper access or use by an authorized person, the Customer should take immediate actions to terminate such authorized person's access to and use of the Bank's services or connectivity channels.
- If Customer utilizes file formatting, encryption software (whether provided by the Bank or a third party), to support the formatting and recognition of the Customer's data and instructions and acts upon Communications with Citi, then the Customer will use such software solely for the purpose for which it has been installed.

VII. Other considerations - Fees and Interest

The fees related to the services provided by the Bank are set forth pursuant to the limits established by the Central Bank of Paraguay and published monthly according to the Central Bank Regulation in a local newspaper, and also available at the website: https://www.citibank.com/icg/sa/latam/paraguay/, updated from time to time, or as agreed between the parties. The price, fees and interest may be subject to changes at Bank's discretion upon previous disclosure of the Service Fees Table according to the regulations in effect.

In saving account, the interest will be paid on a quarterly basis and in the certificate of deposits according to the tenor established.

VIII. Conclusion

Thank you for choosing Citi Treasury and Trade Solutions (TTS) for your cash management needs. Please feel free to contact your Citi relationship manager with any additional questions you have regarding TTS services.

Treasury and Trade Solutions
citi.com/tts

The information contained in these pages is not intended as legal or tax advice and we advise our readers to contact their own advisors. Not all products and services are available in all geographic areas. Any unauthorized use, duplication or disclosure is prohibited by law and may result in prosecution. Citibank, N.A. is incorporated with limited liability under the National Bank Act of the U.S.A. and has its head office at 399 Park Avenue, New York, NY 10043, U.S.A. Citibank, N.A. London branch is registered in the UK at Citigroup Centre, Canada Square, Canary Wharf, London E14 5LB, under No. BR001018, and is authorized and regulated by the Financial Conduct Authority. VAT No. GB 429 6256 29. Ultimately owned by Citi Inc., New York, U.S.A.

.

© 2017 Citibank, N.A. All rights reserved. Citi and Arc Design is a trademark and service mark of Citigroup Inc., used and registered throughout the world.
May 2017