Cash Management User Guide

Ecuador

Treasury and Trade Solutions

citi

Table of Contents

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, Citi and Bank may be used interchangeably. This Guide may be updated from time to time and any change will be communicated through our regular channels.

II. Payments Services

A. Types of Payments Services in Ecuador

- Book Transfers: Transfers of funds between Citi Accounts in Ecuador
- Domestic Funds Transfers: Transfers to accounts at other local Banks that are part of the Central Bank's Interbank Payment System (SPI). Orders may not be revoked or left incomplete by the Bank or the Customer once they have been authorized in the platform. The time at which the beneficiary receives a transaction depends on the beneficiary bank.
- Cross Border Funds Transfers: Allow Customers to transfer funds to accounts in other countries in different currencies. The process may involve the use of correspondent banks or other intermediaries and may be subject of additional charges.
- 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". The Bank, at the Customer's request, will issue books of pre-printed checks that can be used to initiate payments to the Customers' beneficiaries. Checkbooks will be enabled in the Bank's system 24 hours after being received by the Customer. The Bank will hold checkbooks for pickup for 90 days, after which the Bank will destroy them.

B. Sending a Payment

1. The Customer sends a payment instruction to Citi, formatted to market standards and as outlined at the time the payment service was implemented, via:
   - Citi e-banking channels, which include CitiDirect BE® and CitiConnect®,
   - A SWIFT interface, or
   - A manual request (refer to Section IV for details on manual transactions)

   In certain cases, instructions given outside a given schedule will be processed the following business day.

   The Bank is not obligated to overdraw the Customer's Account to comply with payments instructions, but if it does the Customer must cover the overdraft and associated charges.
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 credits the beneficiary account on a given schedule depending on the clearing cycle and type.

C. Paylink® Checks

Through the Bank's electronic banking platform, the Customer can order the issuance of customer checks or Paylink® checks to be picked up by beneficiaries, or their authorized representatives, at the Bank's tellers. If the Customer so requests, it can view the checks that have been issued and signed by beneficiaries in the Digital Library application.

Issuance and Processing of Paylink® Checks

1. The Customer communicates instructions to print and issue checks via the agreed Citi e-banking channel.
2. Citi prints the checks, drawn on the Customer's Account, with the facsimile signature(s) of Bank's officer(s). The officers whose signatures are printed on the checks are not responsible for checks' content, or for their use.
3. Citi makes the checks available for pickup by the payees as specified in the Customer's instruction. Checks that are not picked up within 90 days of the issuance date will be returned to the Customer by the Bank.
4. Checks are deposited by the payee(s) and presented to Citi via local clearing arrangements. Checks also can be presented and cashed over-the-counter at the Bank's branch or network extension locations.
5. Checks are validated and posted to the Customer's Account for settlement and the funds are then made available.
6. Citi will not make a payment if it considers a check or draft to be materially altered, forged, counterfeit or stolen, or at the request of a competent judicial, quasi-judicial, regulatory, government or supervisory authority.
7. 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. Upon the Customer's request, Citi can either issue a new check/draft or credit the Customer's Account. If the lost, misplaced, or stolen check or draft is later found, the Customer is required to deliver the original check or draft to Citi immediately.

The Customer can request to view, via the Bank's online banking platform, checks that have been issued and signed by the beneficiary.

D. Revocation and Suspension of Payments

Every payment instruction confirmed by the Customer and accepted by the Bank is final and irrevocable as of the acceptance of said instruction by the Bank. The Bank will not incur any liability to the Customer or to third parties with regard to this, whether said payment was or was not made.

Stop payment orders will be processed in the following method:

1. Before payment is made, the Customer will send a stop payment order to the Bank using the electronic banking platform provided by the Bank.
2. After payment is issued, the Customer will follow the Bank's instructions for suspension of payment in keeping with applicable laws and business practices and will send a request in writing to the Bank.

E. Receiving Direct Debits (Payments)

Citi, as the paying Bank for the Customer, supports incoming direct debit mandates received from other participating financial institutions or partner banks.

1. If the direct debit payment is in compliance with the direct debit authorization, Citi processes the instruction and debits the Customer's Account according to the Ecuadorian Central Bank procedures for direct debits (SCI-Sistema de Cobros Interbancarios).
2. Citi communicates to the collecting financial institution via the clearing system or to partner banks for positive or negative (rejects and returns) acknowledgements. In the event there are insufficient funds in the Customer's Account, Citi will not process the direct debit payment and will send the unsuccessful debit status back to the direct debit payment system.

Citi will reverse any entry passed erroneously and debit or credit the relevant Account.

F. Beneficiary Notification

Beneficiary notifications can be used to inform or notify beneficiaries of the status and details of payments to ease the reconciliation of transactions. Beneficiary notifications are emailed to the respective beneficiaries, who can access payment details through a link to the Online Payment Channel (OLPC).

The Customer, upon issuing instructions via the designated electronic banking system for payments (checks or funds transfers) to its beneficiaries, may authorize the Bank to notify beneficiaries it identifies who utilize the Online Payment Channel service of a new payment or credit on their accounts. The Bank will provide the method (check or electronic funds transfer)

and the date on which the payment will be effected. This information will be available up to 3 months from the time the payment is affected.

G. Tax Receipts and Withholdings

The Bank may make available pre-printed withholding tax receipts to be retrieved by the Customer's vendors at the Bank's tellers. The Customer must provide the Bank with all withholding tax receipts 48 hours ahead of the issuance of a Paylink® check to the vendor. The content of tax receipts and withholding slips will be instructed by the Customer to the Bank. When a payment is made via an interbank funds transfer the withholding tax receipt will be given to the Customer or made available to the beneficiary at the Bank's offices. The Customer can request to view, via the bank's online platform, payment receipts that have been signed by its beneficiaries.

III. Receivables Services

A. Receiving a Payment

1. The clearing system forwards the instruction to Citi based on the locally defined clearing cycle.
2. Citi credits the Account.

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. Direct Debit Collections

A direct debit collection is a financial transaction originated electronically by the Customer instructing the Bank to withdraw funds from a payer's bank account, whether via interbank or book to book transactions.

The Customer may authorize the Bank to debit its accounts for the purpose of crediting third-party accounts for services they provide or for periodic payments due. This authorization grants authority to such third parties for the delivery of funds as indicated.

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. The Bank will proceed to stop debits once notified by the service provider. It will take 3 business days to return the instructions and complete the process. In cases of suspension or termination of utilities or public services handled by a third party, the instruction must be sent to the third party for processing.

In the event that there are no funds in the account to make the debit(s) to the third party, the Bank will not perform the debit.

C. Interbank ACH Debit Collections

Through this service, the Customer can access the Interbank Collection System (SCI), which enables the collection of charge orders at participating financial institutions in Ecuador. The Customer can instruct to the Bank to debit the payer's account at the payer's institution. The payer must have previously authorized the Customer's debit collection orders in writing. Collection Orders confirmed by the Customer and accepted by the Bank are final and irrevocable.

The Customer will obtain, record and store written debit authorizations issued by its payers to carry out collections via SCI. If proof or copies of these authorizations are required by the Bank, the Customer must submit them within 24 hours of the request.

ACH debit collections may be reversed due to a claim by the payer, on orders of the Central Bank of Ecuador. If for any reason there are not sufficient funds in any of the Customer's accounts at the Bank at the time that said return or reversal occurs, the Customer must reimburse the costs incurred by the Bank to meet the obligation, including overdraft charges if applicable.

The Bank, according to the law, will withhold taxes at the source for each collection order that the Customer identifies on the system. Each month the Bank will provide the Customer with a withholding tax statement that includes the withholding taxes for collection order transactions executed during the month.

The payer's bank may charge the payer additional charges or expenses. .

Interbank ACH Debit Collection Process

1. The Customer will generate collection orders through the Citi e-banking channel, either by manual input or bulk files under the conditions determined by the Bank.
2. Citi validates that the transaction requests contain the information required to process them.
3. Citi communicates the ACH debit transactions to the receiving payer banks via the SCI system.
4. Citi credits the funds to the Customer's Account within the agreed time subject to the Bank's receipt of the funds.
5. The Customer will be able to view the charge or rejection in the Citi e-banking channel.

D. Identified Collections – Speed Collect

Speed Collect is a service through which the Bank accepts deposits from third parties on behalf of the Customer so that it can make transaction details, including certain information about the depositor/payer, available in the Citi e-banking channel.

The Customer shall ask the Bank's authorized vendor to issue and deliver Speed Collect deposit slips on which the details of the transaction, the depositor's/payer's information and reference number will be listed. The deposit slips, which must conform to requirements provided by the Bank, may be printed by the Customer prior to receiving authorization from the Bank, which will verify compliance with the requirements. The cost of printing the Speed Collect deposit slips will be covered directly by the Customer.

The Bank will assign up to 15 collection accounts (subaccounts) selected by the Customer for the exclusive purpose of receiving deposits. Collection accounts will not generate any additional costs for the Customer. The Bank will then concentrate funds from the subaccount(s) to the Customer's main account electronically and daily. There will not be a printed account statement for the activities of collection subaccounts. The activity is available through the Citi e-banking channel.

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. Specific country regulations may apply to MIFT.

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 the Bank, 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.

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
   - CitiDirect BE®

   Please contact your Citi representative for additional details
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 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 the Bank 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. The Customer can obtain a copy of such form by contacting the Citi Service Desk.

2. Upon receipt of the manual instruction, the bank will carry out its internal verification, including but not limited, review for completeness of the required details for processing, and verification of the authorizer signature(s) against the ones 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 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 the Bank should be informed of include, but are not limited to:

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

Neither a GMTA form detailing just the update information 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.

The Customer must submit the name(s) of 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, the Bank will request a new GMTA form that will supersede all the previous GMTA forms if there are several signature deletions.

V. Other Considerations

The use or requirement of services from the Bank, as well as services described in this manual, are subject to tariffs detailed in the general commissions catalogue of the Bank, which is available at the Bank's web page. This tariffs and applicable taxes, fees, and expenses can be debited from any of the Customer's Accounts.

The Bank will provide the Customer with a telephone support system through CitiService, our customer service, on working days between 9:00 a.m. and 5:00 p.m.

CitiDirect BE® is a secure electronic banking platform that can be accessed over the internet by users who have been authorized by the company. They can do so from IP addresses abroad, retaining the profile attributes provided at the time of their creation.

Infopool Service

Infopool is a single interface to accounts with Citi and third-party banks. The Infopool Service allows daily monitoring of the balances and transactions of accounts maintained in different banks, across borders and currencies. Thus, Infopool Services consolidates 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 information for the accounts indicated by the Customer, without making adjustments to the information provided by the issuers of the information. 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.

VI. TTS Consolidated Security Procedures

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 WorldLink®)
- Interactive Voice Response ("IVR")
- Email/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 & 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:

3. **Security Officer:** Fulfills functions described in (1) a-c above within the roles of Security Managers

4. **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

5. **Designated Authorizer:** have broad, senior authority to initiate and authorize Workflow activities

6. **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 Authorizers 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

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 the bank 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 communications 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 any of the banks electronic channels 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. 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 that you have regarding TTS services.

Treasury and Trade Solutions
citi.com/tts

October 2017