Cash Management User Guide

Uruguay

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 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., Uruguay branch, Citi and Bank may be used interchangeably. This guide may be updated from time to time and changes may be communicated through our regular channels.

II. Payment Services

A. Types of Payment Services in Uruguay

- Book to Book: Transfers between Citi accounts
- Automated Clearing House (ACH): Interbank electronic transfer payment system
- Real Time Gross Settlement (RTGS): Transfers of funds, small or large, on a real-time basis to accounts at other domestic financial institutions
- Cross Border Funds Transfer (International Transfers): Allows customers to transfer funds to accounts in other countries in different currencies using wire transfers

B. Sending a Payment

1. The Customer instructs Citi to pay the beneficiary through CitiDirect BE® or CitiConnect®, prior to the cut-off time. The instruction should be formatted according to market specifications (as outlined during the implementation).
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 should 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.

C. Beneficiary Notifications

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 (for example, vendors), who can register to access payment details through a link to the Online Payment Channel (OLPC).

Each beneficiary will receive 3 emails at approximately the same time. One email is a notification of the payment from Citi, the second email is a link to register with the Online Payment Channel (OLPC) and includes half of the alphanumeric password to use for the OLPC, and the third email will have the other half of the alphanumeric password to register for the OLPC.

D. 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 should 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 CitiDirect BE® or CitiConnect®.

E. Payable Checks

The following types of checks are available:

1. Standard checks: Negotiable instruments, which can be passed from one person/entity to another and exchanged for money. To request a new checkbook, a customer may contact Citi via a letter to the branch, authorized phone number, CCDM, or CitiService, or return the reorder slip from a previous checkbook. Once the request has been received and is processed before 4 p.m., the new checkbook(s) will be available the next business day.

   Deferred standard checks are standard checks dated for a future payment and can be made for 6 months (180 days) in advance to be kept in custody at the branch and are viewable in CitiDirect BE®.

2. Manager's checks (PayLink® Checks): Citi-issued checks where the funds are immediately debited from the Customer's account. Checks can be requested digitally through the CitiDirect BE® platform and issued by a local branch, or can be requested and issued manually at a local branch.

   Beneficiaries can pick up their payments at a local branch with either their identification number (for payments to a natural person) or the RUT and an official receipt/invoice (for company beneficiaries). Without the required identification information, payments cannot be issued for security reasons. The Bank cannot make a single receipt for several payments, even if the payer of the payment is the same. Payments are non-transferable.

3. Certified checks: Customer-issued checks that Citi guarantees and immediately debits the funds for payment. To certify a check, the Customer should provide a letter signed by an authorized signer of the Company or a Citibank Certified Check Request form with an authorized signature when the check is presented. Upon approval, the front of the check will

receive a ‘Certified’ stamp, and the back will be inscribed with the amount, currency, and Citibank N.A., Uruguay branch.

Check Validity

Checks that are issued in Uruguayan pesos (UYU) are valid for 15 business days from the date they are issued.

Checks that are issued in U.S. dollars (USD) are valid for 120 days from the date they are issued.

Stop Payment Requests on Payable Checks

The Customer or beneficiary may request that the Bank stop payment on any payable check when there is a lost or stolen check and a corresponding police report, in accordance with Bank procedures and applicable local laws. To request a stop payment:

1. The Customer or beneficiary must call and notify CitiService that a check has been lost or stolen to pause any current processing.
2. The Customer or beneficiary then needs to communicate the stop payment instructions to Citi in writing. The stop payment instructions need to specify the serial number of the check, the date of issuance, the beneficiary’s name and the amount, and enclose the corresponding 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 or beneficiary requests a replacement payable check to be issued.

F. Account Overdraft Coverage

To ensure that payments, checks, and transfers can be completed, customers may indicate accounts that can be debited to cover transactions when there are insufficient funds and the account is over-drafted. To utilize this service, customers must sign an activation form and specify the accounts that are covered and the corresponding accounts to be debited.

Unless a corresponding overdraft account is indicated, Citi cannot pay a check with funds from a different account to ensure account integrity and security. If the payment requested is in a different currency than the coverage debit account currency, Citi will convert the currency according to the bank’s exchange rate.

G. Delivery Services

Upon the Customer’s request, Citi can provide a service to deliver checkbooks, rejected checks, and manager’s checks to the Customer’s local office (as stated on the activation form) through

a third-party courier company. To utilize this service, customers must request the service through a letter, sign an activation form, and clearly state who is authorized to receive documents through the delivery service.

Upon request, a messenger will go to the Bank, pick up all requested documentation (including a documentation list of all items being delivered), and keep all items in a sealed and secure envelope until arrival to the Customer's location. Upon delivery, the messenger will require an authorized person to sign the documentation list that is included in the envelope. If the documentation list is not signed or an authorized person is not present, the documents will not be delivered.

Delivery services are available on standard business days between 12 p.m. to 4:00 p.m. (arrival times will vary).

H. Utility Payment Services

With utility payment services a customer's account is automatically debited to pay the invoices of different entities, such as utilities. To request this service, customers must request and sign the activation form. Multiple invoices can be registered at one time, and it is recommended to include a copy of an invoice for each vendor to reduce any errors while inputting account information.

The implementation timing to transition payments to the direct debit service varies with each entity. Once implemented, the Customer's invoice should state that it will be paid by Citi through direct debit.

In the case of an overdraft, the payment will be covered if there are sufficient funds in another approved account, or if there is an overdraft amount established. If there are no additional accounts and/or insufficient funds, the payment may not be made to the entity. To end this service, the Customer can send a letter to Citi to request suspension of service.

I. Tax Payment Services

To utilize the service to execute electronic tax payments from your Citi account to Banco de Previsión Social (BPS), la Dirección General Impositiva (DGI), Dirección Nacional de Aduanas (Aduana), customers must sign the activation form and indicate the individuals who are authorized to make these payments in the activation form. After the activation form has been processed, each authorized person will receive an email from Citi with a uniquely generated alphanumeric password.

To make a payment, authorized individuals should navigate to the website for the tax authority (BPS, DGI, or Aduana) and login using the credentials for the corresponding site. Once prompted to make the tax payment, choose Citi as the payment institution, which will prompt the user to provide the Citi-specific alphanumeric password (the password sent in an email from Citi). Once the password is confirmed, the payment details and reference number can be

reviewed and the payment can be confirmed. Note that the beneficiary tax identification number and the payment amount cannot be changed during the payment review.

The activation of users through the password will be considered the authorization of that user by the Customer.

J. Availability of Payments

CitiDirect BE® and CitiConnect® are available to the Customer 24 hours per day. The schedules for same day transactions are:

- Transfers between Citibank accounts: Until 4:00 p.m. the same day
- Interbank transfers: Until 4:00 p.m. for same day interbank transfers with no monetary limit in Uruguay
- Manager's checks: Available the next business day after request
- Requests made after 4:00 p.m. will be available the next business day and the beneficiary bank will credit the funds transfer before 5:30 p.m.

III. Receivables Services

A. Receiving a Payment

1. The clearing house forwards the payment 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 and the reason for the return is communicated to the payer.
3. Citi provides the name of the payer in the account statement and the corresponding reference number (for example, an invoice number).

B. Check Deposit Channels

Customers can deposit their check(s) over the counter or in the cash deposit machines (CDMs) at Citi's branches.

C. Availability of Receivables

- Local funds transfers: Until 5:30 p.m.; even if the cut-off time for a sending institution is 4 p.m., Citi will credit funds until 5:30 p.m.
- Cross border transfers: Until 4 p.m.
- Citi will not accept check deposits from other countries outside Uruguay.

D. Additional Services

Banred

Banred is a private chain of ATM networks for all banking institutions in Uruguay that can be used to make withdrawals, deposits, or both. To utilize this service for Citi accounts, customers must first sign the activation form and clearly state the authorized people for the account and their respective bank card functionality (example: withdrawals, deposits, or both).

Once the activation form has been received, Banred cards will be sent to the authorized persons or will be available for pick up at a local branch within 2-3 business days. Banred cards will be activated and available to use 1 business day after the cards are delivered.

Citicobros

Citicobros is a service whereby an independent collection company (Abitab) receives deposits from Citi customers on behalf of Citibank N.A., Uruguay branch. To use this service, customers must sign an activation form, and then Citi will provide deposit slips and order plastic cards with a bar code (Citicobros Plus) for authorized users through one of the following channels:

CitiService (by authorized users), business assistants, product managers, or by signing a letter at a branch. Alternatively, depositors can use an invoice with a bar code as an alternative to the Citicobros Plus card.

When requesting the cards, the Customer must provide Citi with the following information: Code number that the Customer wishes to assign to the cardholder, the name of the cardholder, the currency in which deposits will be made, and the number of cards requested.

Two things are required to make a deposit at a collection location: The Citicobros Plus card and a deposit slip. The Citicobros Plus card is used to access account information and the deposit slip provides payment instructions for the deposit (deposit slips are provided to customers by Citi).

Transactions can be carried out from Monday to Sunday during the days and hours respective authorized Citicobros network locations are open to the public. The transaction information will be available for 2 business days, electronically, by telephone, etc.

The collected cash funds or payable ordinary/postdated checks will be credited in 2 business days after the requested deposit. Postdated checks that are payable in less than 48 hours will be credited in 2 business days after the request. Postdated checks that are not payable yet will be kept by the Bank and upon maturity will be forwarded or credited to the recipient.

Note that Citi will credit the received funds to the account on the deposit slip, so the depositor should verify the account information is correct when making a deposit. The Citicobros Plus receipt that is created at the end of each transaction implies the Bank accepts the request.

Check Pickup Services

Citi can provide a service to pick up standard checks or deferred standard checks by a third party courier company. To utilize this service, customers can request the service through a letter and sign an activation form.

Once a check pickup is requested, the Customer organizes all documents on a completed Citi deposit slip and attaches all relevant information. A messenger will arrive with a secure envelope and secure all documents in the envelope. The messenger will request a signature from the Customer on the release ticket with a corresponding reference and envelope seal number, and the Customer will receive a copy of it.

The check pickup timeframe is from 1:00 p.m. to 4:00 p.m. Any check received before 5:00 p.m. will be processed on the same business day. Anything received after 5:00 p.m. will be processed on the following business day.

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. The GMTA form confirms 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 risks 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 the 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: Letter or CitiDirect BE® Please select the option(s) you want to activate in the GMTA form.
2. The same person who requests and signs for the MIFT can also receive and verify the callback confirmation.
3. 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 the required processing details and verifying the initiator(s)' 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 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. 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

The GTMA Form and Signature Cards are only used to register a signature. New account signers should be designated through legal documentation, such as powers of attorney, appointments of directors, or official legal documentation.

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 update alone, nor a letter nor 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. 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

Consolidation Service

Infopool is a single interface that integrates a view of accounts with Citi and third-party banks. The Infopool Service allows daily monitoring of balances and transactions 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 adjusting the information provided by its issuer. Citi is not responsible for the content or preciseness of the information on the accounts.

The Customer will authorize Group or Third Party 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 account 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.

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 will 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

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")
- Email 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 should 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 should 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	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

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.

D. Electronic Instruments

Services rendered through ATMs, Citiservice, CitiDirect or similar means that use electronic instruments such as cards, personal identification codes, or passwords should be used in the manner that they are intended. Customer agrees not to disclose their codes, passwords, or cards to unauthorized people, to keep them safe, and destroy the cards once expired. Additionally, customer agrees to modify and update the codes at the Bank's recommendation, and not to respond or utilize their card/codes in unauthorized communications or in unusual situations.

In the case that there has been a loss, theft, or forgery, customer agrees to immediately inform the Bank in accordance with the Electronic Instruments Booklet (received beforehand by the Customer), and shall be responsible for unauthorized operations carried out until the Bank is notified (or in the case of the ATM services Banred/Rias Redbanc S.A. is notified).

VII. Other Considerations

Uruguayan accounts and services are provided in adherence to the Master Account and Service Terms (MAST), as well as applicable regulations from the Central Bank of Uruguay, Confidentiality and Data Privacy Conditions, and any applicable local conditions.

Termination of Services

If the Bank decides to close a customer's account or end a service, the customer will be notified in writing at least 3 business days in advance. The customer must cancel any outstanding debts, withdraw any remaining balances, and return any relevant documents within 5 business days.

A. Current Accounts

If a customer chooses to close a current account or the customer is notified of the suspension or closure of an account, the customer must return all blank checks, pay any rejected checks, and provide evidence of payment for outstanding debts within 5 business days from the notification of the Bank. Current accounts do not accrue interest, but if they do for any time period, whenever they stop accruing interest again, the customer will be notified.

B. Price Booklet and Notifications

Customers will receive a Price Booklet that notes all charges associated with account maintenance and service, which customers are obliged to observe. Customers will be notified of any changes to the Price Booklet at least 30 days before it goes into effect. Customers will be notified of any changes to the low average commission, account maintenance commission, and/or interest rates (savings accounts, deposits, sight deposits, or time deposits) at least 5 business days before they go into effect.

C. Validity of Documentation

Citi will consider all of the documentation and information submitted by the Customer (including all corporate documentation, appointment of legal representatives, powers of attorney, domiciles, and all other personal data) as valid and enforceable until receiving an explicit notification to change it. To make a change, the Customer must notify Citi in writing and will receive an acknowledgement of receipt from Citi. All actions and documents prepared by the designated representatives (e.g.,directors or attorneys in fact) will be considered effective until Citi issues the acknowledgement to the Customer.

Citi may periodically send a summary to customers verifying the documentation/information submitted on their behalf by existing representatives. If no response is received from the customer within 48 business hours from the delivery of the email by the Bank, then Citi will consider the no response to mean the customer has no objections.

D. Informed Consent

Citi's customers may use CitiDirect BE® to pay their third-party customers, and may input their customer data into CitiDirect BE® to notify their customers of an available payment or service. Citi will utilize the information that is input by our customers to send communication notices to their third-party customers (for example, that a payment is available for pickup), and for no other purpose. Citi advises all of its customers to ensure the accuracy of the data they input into CitiDirect BE® to avoid any miscommunications.

E. Communications

For all communications, notifications, and information related to a Citi account or service, customers may directly email communications to: citiserviceuruguay@citi.com .

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

March 2018