TRUIST

Reference

Truist Treasury Manager
Security Checklist

Truist is committed to helping you keep your company's Truist online transactions safe from fraud. Because security is a key component of Truist Treasury Manager, Truist employs various security features to help you protect access to your accounts. By implementing all of the available security layers and following our recommended best practices, you can help mitigate the risk of fraud and unauthorized access. Use this checklist to assist with risk assessments and to verify that you are following our recommended security standards and best practices. We suggest that companies perform annual security evaluations, and respond promptly with additional controls where risks are identified.

Treasury Manager Standard Security Procedures

Treasury Manager provides robust security procedures to help you protect your company's online sessions, such as:

- ✓ IBM Security Trusteer Rapport* secure browsing software, which must be installed and running on every computer used to access Treasury Manager unless accessing through Truist One View, and should be installed with administrative privileges whenever possible.
- ✓ Security challenge questions which are presented in the event that the Truist risk monitoring application detects what it determines to be uncharacteristic sign-on behavior, based on the user's profile.
- ✓ A dual approval requirement, which is strongly recommended for all ACH or wire transactions entered in the service.
- ✓ Wire tokens which must be entered at approval.

Safeguarding Authorization Codes

It is your responsibility to maintain the confidentiality of your users' authorization codes used to access Treasury Manager. To help protect your users' authorization codes, please note the following recommendations:

- ✓ Create alphanumeric passwords that would be difficult for others to guess.
- ✓ Set up security challenge questions and answers that would be difficult to guess.
- ✓ Never share or divulge passwords, other sign-on credentials, wire tokens, or account information.

Security Administration

Your company's security administrator (in some cases referred to as a primary administrator) must control user access and permissions and maintain appropriate internal procedures as recommended below.

- ✓ Review system security administration User Activity and User Setup reports to audit user entitlements and activity.
- ✓ Ensure that all computers have the most recent operating system updates and current virus protection software.
- ✓ Delete user IDs when employees leave the company or change roles as part of your employee exit procedures.
- ✓ Disable online access when employees go on vacation or for those who do not sign on frequently.

- ✓ Limit user entitlements to only allow access to services and accounts based on a user's role or needs.
- ✓ Implement a dual administration requirement to help reduce the risk of an unauthorized user being added to the system or a user's permissions being changed - including granting access to additional accounts or functions - without secondary approval. With dual administration, new user setups and entitlement changes remain in a pending status for approval by another company security administrator.
- ✓ Segregate duties and ensure that the company security administrator user IDs do not have payment initiation or approval entitlements.

Payments Security

- ✓ Use a dual approval requirement to help reduce the risk of fraud and prevent keying errors. With dual approval, transactions remain in a pending status until they are approved by an alternate user.
- ✓ Import ACH and wire transfer files rather than keying them into the system. Files can be uploaded, imported or sent through secure data transmission to help protect against online fraud and reduce the risk of keying errors.
- ✓ Segregate duties between users and implement a dual approval requirement for template creation, maintenance, payment initiation and payment approval functions.
- ✓ Set approval limits at the user level, by template, or by transaction type.
- ✓ Enable Positive Pay alerts to notify users when exception items are pending.
- ✓ Limit user access to the Preferred Recipient List to help prevent ACH and wire recipients from being modified by an unauthorized user.
- ✓ Use ACH Fraud Control to review potentially unauthorized incoming ACH transactions before they post. Debit and credit blocks and filters can also be established for specific originators.
- ✓ Establish Universal Payment Identification Codes (UPIC) to collect ACH payments from your trading partners without divulging sensitive account information.

ACH Transaction Initiation

- ✓ Prenote zero dollar ACH transactions to verify the recipient routing number and account number prior to sending a live dollar transaction. Prenoting transactions can help prevent keying errors and protect against fraud.
- ✓ Designate ACH batch templates as "Confidential" so that only entitled users have access to confidential templates.
- ✓ Establish ACH Company IDs to limit user access to specific templates, accounts, or reports.
- ✓ Take advantage of intraday ACH debit alerts through Online Courier.

Wire Transfer Initiation

- ✓ Set up intraday wire alerts and wire advices through Online Courier.
- ✓ Use user-defined wire templates to reduce the risk of unauthorized changes to beneficiary routing information.
- ✓ Ensure that user limits are established on Treasury Manager.

Operating Procedures

- ✓ Reconcile accounts frequently in order to help protect your accounts against online fraud. Business accounts are subject to specific timeframes for returning or disputing potentially unauthorized transactions.
- ✓ Designate a computer(s) for online banking activities. This computer should be used exclusively for online banking, not for other activities such as email, Internet browsing, or file sharing.

- ✓ Avoid conducting online banking business activities on home computers or at publicly shared locations such as those at hotels, airports, coffee shops, or shared business centers.

Internet Browsing

- ✓ Exercise caution when using networking and account aggregation sites since they may be used to fraudulently obtain sign-on credentials and account information.
- ✓ Report any suspicion of viruses or computer performance issues to the appropriate authority at your company.
- ✓ Delete unexpected messages asking for passwords or other confidential information.

Additional Information

For more information or to report fraud, visit the **Report Fraud** page at truist.com/fraud-and-security/report-fraud.

Getting Help

Click the **User Materials** link at the top right of any page or visit the Treasury Manager page of the **Treasury Resource Center** at truist.com/treasuryresourcecenter to access reference materials.

If you need additional assistance, contact Treasury Solutions Client Services at treasuryclientservices@truist.com or **800-774-8179**. Representatives are available from 8 am to 8 pm ET, Monday through Friday on bank business days.

* Trusteer Rapport or other secure browsing software downloaded to or accessed by your computer or mobile device (the Software) is provided by IBM. You and your company agree that (i) use of the Software is subject to IBM's terms and conditions and privacy policy; (ii) Truist makes no representations or warranties of any kind related to the Software and has no responsibility for the performance, compatibility or availability of the Software, or for damages of any kind that may be caused by the Software; and (iii) protections offered by use of the Software can be achieved only when the Software is used in connection with access to specific Truist products which are designed to interact with the Software. When used with those services, the Software may make certain fraud detection information available to Truist. Truist has no obligation to provide you any notices with respect to such information.