Nacha’s Risk Management Portal

Instruction Manual for Financial Institutions

Nacha’s Risk Management Portal is the single resource to access all of our risk databases available to financial institutions and can serve as effective tools to support risk mitigation activities:

Third-Party Sender Registration Database
Direct Access Registration Database
Terminated Originator Database
Financial Institution Contact Database

The Risk Management Portal Registration Support Line is 703-349-4556.

Contents

Risk Management Portal Databases ................................................................................................................................. 2
Initial Registration ............................................................................................................................................................... 2
Field Descriptions ............................................................................................................................................................. 3
Completing the Initial Registration ................................................................................................................................ 4
How to Reset Your Password .......................................................................................................................................... 6
How to Manage Users – Administrators Only .................................................................................................................. 7
Registration Management ............................................................................................................................................... 8
Registration Confirmation .................................................................................................................................................. 9
Third-Party Sender Registration ................................................................................................................................... 11
Nacha Operating Rules Requirement ............................................................................................................................... 11
Third-Party Sender Registration in the Portal ................................................................................................................... 11
Add Third-Party Sender .................................................................................................................................................. 11
Manual Entry ................................................................................................................................................................. 11
Bulk Upload ................................................................................................................................................................... 13
Deactivating (Removing) a Third-Party Sender ............................................................................................................. 14
Direct Access Registration ............................................................................................................................................. 15
Nacha Operating Rules Requirement ............................................................................................................................... 15
Direct Access Registration Database in the Portal ............................................................................................................ 15
Registration and Updating .............................................................................................................................................. 15
Quarterly Reporting ........................................................................................................................................................ 15
Adding a New Direct Access Debit Participant Relationship .......................................................................................... 17
Terminated Originator Database (TOD) – Voluntary ....................................................................................................... 18
Contribute to the Terminated Originator Database ......................................................................................................... 18
Search the Terminated Originator Database .................................................................................................................... 18
Financial Institution Contact Database – Voluntary ...................................................................................................... 20
Enter Your Financial Institution Contacts ..................................................................................................................... 20
Search the Financial Institution Contact Database ....................................................................................................... 21
Risk Management Portal Databases

Third-Party Sender Registration Database (TPS): Each financial institution will attest as to whether it does or does not maintain third-party sender customers. If a financial institution does maintain third-party sender customers, details of each customer must be provided after registration.

Direct Access Status Registration Database (DA): Each financial institution will need to attest (or re-attest) as to whether it does or does not have maintain direct access debit participant relationships. If a financial institution does maintain direct access debit participant relationships, details of each relationship must be provided after registration.

Terminated Originator Database (TOD): Participation in the TOD is voluntary. If your financial institution decides to participate in the TOD, you will have to agree to the Terms of Use. The Terms of Use will only appear if you select to participate.

Financial Institution Contact Database (FI Contact): Participation in the Financial Institution Contact Database is voluntary.

Each ODFI must attest to their Third-Party Sender and Direct Access Debit Participant relationships, and opt in or out of each optional database. Financial institutions that are RDFIs only will not have the option to register for the Third-Party Sender Registration Database or the Direct Access Registration Database.

If you have questions about registration, please contact your local Payments Association or Nacha.

Initial Registration

1. Registering for the Risk Management Portal begins at https://riskmanagementportal.nacha.org/. Registration should be completed by an “Administrator” or someone with knowledge, information and authority to make decisions about your financial institution’s relationships with Third-Parties and use of risk mitigation services.

2. Select “Financial Institution Registration.” Financial institutions that originate ACH transactions will need to select “Originating Depository Financial Institution (ODFI)” in subsequent screen and click on Register. Financial Institutions that receive ACH transactions, but do not originate ACH transactions will select “Receiving Depository Financial Institution (RDFI)” in subsequent screen and click on register. i.e., ODFIs are also RDFIs (and would register as an ODFI), but an RDFI does not have to be an ODFI (and would register as an RDFI).

Please note that many of the references and graphics in this instruction manual refer to “ODFIs.” For financial institutions using the Risk Management Portal as a Receiving Depository Financial Institution only, the “ODFI” references will appear as “RDFI” within the Portal. The instruction manual outlines the Risk Management Portal instructions specific to “ODFIs” to generally describe the Portal registration for all financial institutions, as it is essentially identical for ODFIs and RDFIs.
3. Do not enter your email address and password for the Nacha website on the Risk Management Portal Login page. This is a distinct and different log in, and your credentials will be established after you complete the Financial Institution Registration portion.

3. You are now at the Financial Institution Registration Page. All fields marked with * are required to be completed. After completing the fields, your financial institution must attest to whether or not your institution maintains Third-Party Sender or Direct Access Debit Participant relationships (for ODFIs), and/or opt in to participating in the Terminated Originator Database and/or Financial Institution Contact Database. Note: Participation in the Terminated Originator Database (TOD) and Financial Institution Contact Database is voluntary and can be updated at any time.

✓ Please double-check all email addresses for accuracy before you submit your registration. Any error in the email address will render the Administrator or User unable to log in to the Risk Management Portal. You will not be able to edit the Administrator or User emails after submission. (See the Managing Users portion of this document on how to deactivate a User entered with an incorrect email.)

Field Descriptions:

**Primary RTN** - Each financial institution must register once using its primary RTN, or RTN with which it originates all or most of its transactions. Once registered, additional RTNs can be assigned to financial institutions based on additional relationships or Risk Management Portal databases utilized by the financial institution.

✓ The Primary RTN field cannot be changed after registration.

**ODFI or RDFI Name**: This field will auto-populate based on the RTN selected. This field is editable.

**Administrator Details**: Administrators oversee management of the Risk Management Portal for their organization, and can access, add, modify, and remove Users and/or contacts of the Portal. Each financial institution is required to have an Administrator. Each financial institution will have only one administrator.

✓ The Administrator’s email address cannot be the same email address as any User.

**User Details**: Users can access, add, and modify organization details and records in the Risk Management Portal databases utilized by the organization. Users are not required and can be added or modified by the Administrator at any time after registration. Each financial institution can have up to four Users.

✓ Any User’s email address cannot be the same as the Administrator’s email address.

**Contact Person Details**: An Administrator or a User can also be the contact person, but does not have to be. The contact person will be contacted by Nacha in the event of questions or issues related to organization information or records in the Risk Management Portal databases utilized by the organization.

✓ This contact can be the same as the Administrator, any User, or a separate contact. (The Contact Person does not have log-in capabilities.)
4. Click Register to submit your registration.

Completing the Initial Registration

1. Once Nacha has accepted your registration, the Administrator and any Users added at registration will receive a welcome email with a temporary password. Use the link provided in the email to log in for the first time and create a new password. The new password should be between 10 and 50 characters and contain one capital letter, one number, and one special character.
If you do not receive the welcome email, please check your spam and junk folders, and ensure internal email servers are configured to white-list nacha.org.

Emails are automatically and immediately generated from the Database. Delivery to your mailbox may be delayed by your internal email system.

Once your password has been changed from the initial password provided in the welcome email, you will be redirected to the login page again. Enter your email address and your new password. At this time, an email will be sent to you containing a One-Time Authentication (OTA) Code.

If you do not receive the OTA email, please check your spam and junk folders, and ensure internal email servers are configured to white-list nacha.org.

Emails are automatically and immediately generated from the Database. Delivery to your mailbox may be delayed by your internal email system.

Hi Jordan Bennett,

Below is your One-Time Authentication Code. Please return to the authentication screen and enter this code to access NACHA’s Risk Management Portal.

One-Time Authentication Code: 7ba3e5

For security, this code will expire in 180 hours. Please do not share your authentication code with anyone.

For questions, please reply to this email.

Regards,
NACHA Help Desk

2. You will then be prompted to enter the One-Time Authentication Code received in the email. This form of multifactor authentication is required every time you log in to the Risk Management Portal.

It is important that you do not hit the ‘back’ button or leave the OTA page until you have received and entered the OTA Code.
3. Once the OTA Code is entered, you are now logged in to Nacha’s Risk Management Portal and should see the Registrations and Control Menu tabs. If you attested to having Third-Party Sender customers or Direct Access Debit Participant relationships, these tabs will be available. The TOD and FI Contact tabs are also available for the financial institutions that choose to participate in these databases.

✓ The Risk Management Portal will log the User out after five minutes of inactivity. You will be required to log back in and submit another One-Time Authentication Code every time you are logged out.

How to Reset Your Password

1. There are two ways to reset your password. Select “Forgot Password” from the Risk Management Portal login screen, or if you are a User, ask your financial institution’s Administrator to reset your password.

2. You will receive an email with a temporary password. Use the link provided in the email to log in and create a new password. The new password must be between 10 and 50 characters and contain one capital letter, one number, and one special character.

3. Once your password has been changed, you will be redirected to the login page again. Enter your email address and your new password. At this time, an email will be sent to you containing a One-Authentication Code.

✓ If you do not receive the OTA email, please check your spam and junk folders, and ensure internal email servers are configured to white-list nacha.org.

✓ Emails are automatically and immediately generated from the Database. Delivery to your mailbox may be delayed by your internal email system.
4. You will then be prompted to enter the One-Time Authentication Code received in the email. This form of multi-factor authentication is required every time you log in to the Risk Management Portal.

How to Manage Users – Administrators Only

1. Select the “ODFI Users” item from Control Menu Tab to manage Users for your financial institution. Each financial institution must have one Administrator. Each financial institution can optionally have up to four additional Users. It is recommended that each financial institution have at least one User.

2. Select “Create New User” to add a new User. A pop up will appear.

3. Fill in each box with the new User’s information and select “save” to add the new User. Once added, the new User will receive a welcome notice with temporary password. Instruct the new User to follow the steps for initial login.

4. Editing a User: Scroll to the extreme right to the Actions column, select the “Edit User” icon to change the information about the User.

   □ The Administrator cannot change the email address of a User. If the email address was entered incorrectly during the initial registration, the User must be deactivated (see Section 7 below) and entered again using ‘Create New User’ (see Section 2 above).

5. Select the “Reset Password” icon from the actions column to reset the password for a User.
6. Deactivate a User: Scroll to the extreme right to the Actions column, select the “deactivate” icon to eliminate access for the User. You will receive a pop-up confirming your selection. Click “yes.” The row of the deactivated User will turn pink to indicate the User has been deactivated.

7. Reactivate a User: Scroll to the extreme right to the Actions column, select the “reactivate” icon to restore access for the User. A pop-up will appear. Confirm that you would like to reactivate the User. You should receive notice that the User is active and their row will turn back to white indicating they are active.

Registration Management

The Registrations menu is where you can find and edit information about your financial institution or organization. This tab allows you to manage your financial institution details and allows your financial institution the option to select which Nacha databases to join. Confirmation of registration along with the date the financial institution was registered is presented in this area. This table is exportable. Individual Third-Party Sender or Direct Access Debit Participant registrations are available for viewing in the TPS and DA tabs.

1. Select “ODFI Management” from the Registrations dropdown menu. You should now see the information about your ODFI as it was entered at registration.
2. Scroll to the extreme right to view your financial institution’s registrations in the actions column.

3. The “Edit” icon (see illustration ‘A’) will let you edit any of the information submitted at registration with the exception of Primary RTN. The “Deactivate” icon (see illustration ‘B’) will deactivate the financial institution along with all Users, all registered Third-Party Senders, all Direct Access Debit Participant relationships, and any FI contacts associated with the financial institution. The remaining icons are quick navigation icons that take you directly to your financial institution’s registered Third-Party Sender customers, registered Direct Access Debit Participant relationships, TOD contributions, FI Contact management.

Registration Confirmation

✓ Pop-up blockers must be disabled before you perform Step 1 below. Otherwise, you will be logged out of the Portal.

1. Click on the “Registration Confirmation” button to print your financial institution’s registration summary. Print the registration confirmation after all Third-Party Sender Customers and Direct Access Debit Participants have been added.
2. A one page summary will appear in a new window. Use your browser's print option to print and/or save the one-page registration confirmation.

This confirmation page is typically what an auditor will need in order to confirm your registration with Nacha.

**Registration Summary Report**

BANK OF NACHA, Primary RTN 061000101, 400, 2550 Wasser Terrace, Herndon, VA has successfully registered with NACHA.

REGISTRATION STATUS: Active

DATE OF INITIAL REGISTRATION: 11-03-2017

AS OF 11-08-2017, BANK OF NACHA HAS ATTESTED TO THE FOLLOWING:

**THIRD-PARTY SENDER REGISTRATION**
The financial institution *does* currently maintain Third-Party Sender customers. The financial institution maintains 3 Third-Party Sender customer(s).

**DIRECT ACCESS REGISTRATION**
The financial institution *does* currently maintain Direct Access Debit Participant relationships. The financial institution maintains 1 Direct Access Debit Participant relationship(s).


Third-Party Sender Registration

Nacha Operating Rules Requirement
The Nacha Operating Rules require that the ODFI must register the Third-Party Sender within the later of 30 days of transmitting the first entry on behalf of the Third-Party Sender, or within 10 days of becoming aware that an unregistered customer for which the ODFI transmits entries is actually a Third-Party Sender.

Additionally, the ODFI must update the registration information on the Third-Party Sender within 45 days following any change to the information previously provided, including termination of the Third-Party Sender. (Nacha Operating Rules, Subsection 2.17.3, Third-Party Sender Registration)

✓ The ODFI does not need to re-register annually. The initial registration stands until or unless there is a change to the information provided to Nacha, including termination of the Third-Party Sender(s).

Third-Party Sender Registration in the Portal
The Third-Party Sender (TPS) menu is home to the Third-Party Sender Registration Database. Adding, editing, viewing, and exporting all of your Third-Party Sender customers can be completed from this tab. This tab is only enabled for financial institutions that attest to currently maintaining Third-Party Sender customers.

Add Third-Party Sender
1. Select “TPS DB Management” from the TPS tab dropdown menu.

Manual Entry
1. Select the blue “Manual Entry” button. A pop-up will appear. Complete the form for each Third-Party Sender customer. All fields marked with an * need to be completed. Click “Submit” to save. Each Administrator and User will receive an email confirming the new TPS.
The ODFI Routing Number is the routing number used by Third-Party Sender customer being registered. Begin typing and the selection box will auto complete using the routing numbers associated with your Primary RTN.

If multiple Company IDs are used for a single Third-Party Sender, only enter the Third-Party Sender once and enter one (1) of the associated Company IDs (at the ODFI’s discretion). Do not enter any one Third-Party Sender more than once.

Only register the TPS Company ID of the Third-Party Sender and not the company names and IDs of every Originator. The Nacha Operating Rules do not require the Company ID for every Originator associated with the Third-Party Sender.

2. Each entry, originally submitted via the manual or bulk upload process, can be manually edited using the “Edit TPS” icon (A) in the actions column. The red “Deactivate TPS” icon (B) will deactivate the selected TPS.

Export TPS Entries
All registered Third-Party Sender customers can be exported in multiple formats.
1. Select the desired format and “Export.” The exported file will appear in a pop-up window. Make sure your web browser’s pop-up blocker is disabled. The Excel, CSV, and XML export options export in the bulk upload format. The
TPS Table will export the entries in Excel exactly as shown in the TPS table. The TPS table format includes the date registered, date modified, and modified by fields that are not part of the bulk upload formats.

2. Save the file. The Excel, CSV, and XML files can now be modified and uploaded using the bulk upload process. The TPS Table file can be stored and maintained for audit purposes.

Bulk Upload
1. Select “Bulk Upload” from the TPS drop down menu.

2. Select a template from the download templates available. You can also modify a previously exported file. See the “Export TPS Entries” section of this document for instructions on exporting TPS customers from the Third-Party Sender Registration Database. Add or modify TPS customer information and save your file.

3. For reference, the Excel, CSV, and XML templates and the reference key for each field are attached below.

4. Choose the file using the “Choose File” button and then select “Upload.” The Risk Management Portal will perform validation and move the file into the file processing queue. Successful files will receive the message, “Files have been successfully placed in the file processing queue.” Error messages will alert Users to files that do not pass the validation. **All files are processed at midnight on the date of upload and are available to view on the following day.**
5. Monitor the process of submitted files using the “Bulk Upload History” selection under the TPS tab. Files will remain in "Pending" status until after midnight on the date the file was received. The Risk Management Portal completes a rule validation on each row of all imported files and can process a file in whole or in part. Error messages will appear in the actions column letting the User know which row(s) failed and why.

Deactivating (Removing) a Third-Party Sender
If your financial institution no longer processes for a Third-Party Sender, follow these steps to deactivate the Third-Party Sender:

1. Go to TPS, then TPS DB Management, scroll to the extreme right to the Actions column, and click the “Deactivate” icon (see illustration ‘B’).

2. If you are deactivating all TPSs, you must also go to the ODFI Management section, and change the TPS question from a ‘Yes’ response to a ‘No’ response by going to the ODFI Management page, scroll to the extreme right to the Actions column, and click the “Edit ODFI” icon (see illustration ‘A’) and submit.
Direct Access Registration

Nacha Operating Rules Requirement
An ODFI that has one or more Direct Access Debit Participants must register each relationship with Nacha prior to originating entries for the Direct Access Debit Participant(s). The ODFI must provide updated information following any change to the information previously provided, including termination of the Direct Access Debit Participant. (Nacha Operating Rules, Subsection 2.17.1, Direct Access Registration)

✓ The ODFI does not need to re-register annually. The initial registration stands until or unless there is a change to the information provided to Nacha, including termination of the Direct Access Debit Participant(s).

Direct Access Registration Database in the Portal
The Direct Access (DA) menu is home to the Direct Access Registration Database. Adding, editing, viewing, and exporting all Direct Access Debit Participant relationships can be completed from this tab. This tab is only enabled for financial institutions that attest to currently maintaining Direct Access Debit Participant relationships.

Registration and Updating
1. If the financial institution attests to having a Direct Access Debit Participant relationship, Nacha Risk staff will contact the financial institution to confirm the Direct Access Debit Participant relationship and complete the registration with the financial institution.
2. Direct Access Debit Participant relationships can be deactivated by scrolling to the extreme right to the Actions column, then click the ‘deactivate’ icon.

Quarterly Reporting
All financial institutions with one or more Direct Access Debit Participant relationships must provide the following data on a quarterly basis for each relationship in total and by Standard Entry Class (SEC) Code:
   a. average daily debit Entry origination volume;
   b. average daily debit Entry origination dollar value;
   c. average daily debit Entry return volume;
   d. average daily debit Entry return dollar value; and
   e. average daily rates of return.

1. Select “Quarterly Debit Participants” from the DA dropdown menu.
2. Select “Submit Quarterly Reporting” to add new quarterly reporting.

3. Select the Tax ID, reporting year, and reporting quarter for each submission. Use the + icon to add additional SEC codes. All fields must be completed prior to submission.

4. After submission, a new record will appear in the Quarterly Direct Access Debit Participant Submissions table. This table tracks all reporting by the financial institution. Each record is viewable by clicking on the “view” icon in the actions column.
Adding a New Direct Access Debit Participant Relationship

Financial institutions that have already attested to currently maintaining Direct Access Debit Participant relationships will see the “Request New DA” button in the DA DB Management view. Upon clicking this button, the user will see the following message. Nacha staff will contact the submitting financial institution within 24 hours to obtain all required information for the Direct Access Debit Participant.
Terminated Originator Database (TOD) – Voluntary

ODFIs and Third Parties that register for the Terminated Originator Database (TOD) will be able to perform part of their due diligence for KYC (“Know Your Customer”) by being able to add information on, investigate new and periodically verify Originators and Third-Party Senders.

Inclusion in the TOD, after being terminated for cause by an ODFI, does not mean an Originator or Third-Party Sender is prohibited from working with another ODFI. However, it allows educated business decisions about onboarding Originators or Third-Party Senders.

Contribute to the Terminated Originator Database

1. Select “TOD DB Management” from the TOD dropdown menu. This is where you will contribute new submissions and manage all TOD contributions.

2. To add a new TOD contribution, select “Contribute to TOD.” This will take you to a new screen. To contribute a new terminated Originator or Third-Party Sender, all fields marked with an * need to be completed.

Search the Terminated Originator Database

1. Select “Search TOD” from the TOD dropdown menu. Searches can be done on the complete legal name, Tax ID or Doing Business as Name (DBA). Only an exact match will return a result. No partial names or wildcards can be used to search the TOD.
2. All contributed information will be displayed if an exact match is found. Multiple records indicate that Originator or Third-Party Sender has been terminated by multiple sources.
Financial Institution Contact Database – Voluntary

Financial institutions (FIs) face increasingly sophisticated fraud schemes, such as data breaches, business email compromise, and other interrupters, e.g., distributed denial of service attacks (‘DDoS attacks’). FIs respond by investing considerable resources in cyber protection technologies.

Nacha provides the Financial Institution Contact Database as a means to enable communication between financial institutions during an event as described above. FIs can share pertinent contact information to mitigate the impact an event can have on day-to-day operations.

This database is designed to include contact information for multiple key FI personnel. Typically, FIs contribute operations and processing contacts; however, FIs should consider adding internal IT, security, or risk personnel as contacts. A variety of contacts greatly increases the value of the Financial Institution Contact Database.

Financial institutions must opt-in in the Portal in order to contribute to or search the Financial Institution Contact Database.

Enter Your Financial Institution Contacts

1. Select “FIC DB Management” from the FI Contact menu tab to manage the contacts representing your financial institution. Select “Add New FI contact.”

2. Complete each field for the contact. Each financial institution can have a total of 4 Primary Contacts and 4 Secondary Contacts (in addition to the financial institution’s Administrator). Use the blue + to associate the RTN(s) to this contact. All fields marked with an * must be completed.
3. Updating the Contact: Scroll to the extreme right to the Actions column. The “Edit” icon (see illustration ‘A’) will let you change or update the contact information. The “Deactivate” icon (see illustration ‘B’) will deactivate the contact.

Search the Financial Institution Contact Database

√ Each financial institution must contribute at least one Primary Contact to the FI Contact Database to enable searching for other financial institution’s contacts.

1. Select “FIC Contact Search” from the FI Contact menu tab to search for a financial institution’s contacts in the FI Contact Database.

2. The database can be searched by Routing Number or FI Name.