IMPORTANT NOTICE

National Securities Clearing Corporation

DTCC The Depository Trust & Clearing Corporation

A#6481
P&S #6051
DATE: **July 25, 2007**
TO: **ALL PARTICIPANTS**

ATTENTION: **MANAGER MUTUAL FUNDS OPERATIONS, MANAGER DATA PROCESSING, MANAGER CASHIERS, MANAGER P&S DEPARTMENT**
FROM: **WEALTH MANAGEMENT SERVICES - MUTUAL FUNDS**
SUBJECT: **MUTUAL FUND SECURITY PROFILE SERVICE REDESIGN - HELPFUL HINTS AND COMMONLY ASKED QUESTIONS**

NSCC has reengineered the Security Issue database component of Mutual Fund Profile Service as stated in Important Notice A#6374, P&S#5944 dated January 5, 2007, Important Notice A#6405, P&S 5975 dated February 20, 2007, Important Notice A#6450, P&S# 6020 dated May 15, 2007 and Important Notice A#6475, P&S#6045 dated July 3, 2007.

I. Profile Effective Date

As stated in Important Notice A#6475, P&S#6045 dated July 3, 2007 the Profile Security Issue Database Redesign conversion period for funds has been **extended to September 17, 2007**.

On June 2nd, existing data was converted to the new database with a future Profile Effective Date of July 16, 2007. This converted data became the "current" data on the new database on Monday July 16, 2007.

Funds that participated in the spreadsheet conversion process or that directly input data via the new DTCC WebDirect screens must send DTCC an authorizing email to have their data released. Once funds have completed reviewing and updating their data they must send Rita Gribben at rgribben@dtcc.com and their Relationship Manager the confirming email by **Thursday, September 13, 2007, 5:00PM ET for their data to be sent to firms for the first time on Friday September 14, 2007.**

Please note funds are encouraged to send their confirming email to DTCC as early as possible so their status of completion is known. The new live production date for funds and for firms to receive standard input and output from the new database in production is Monday, September 17, 2007. There is <u>no output to firms in production</u> from the new database during this extended review and scrubbing period.

Funds must continue to update the old Profile Security database and the new Profile Security database in Production to keep both databases in sync until the new Profile database is launched on September 17, 2007. Funds must continue this process until the September 13th deadline.

NSCC will send the full data file to firms with any data that has effective dates of September 17th or earlier. If funds input or change data prior to September 17th using a future effective date of September 18th or later, that data will also be in the file sent to firms on Friday night September 14th. As today when these "future" dates become current" dates, NSCC will send the data to firms in the normal output schedule thereafter. Please refer to Section III. Output to Firms in this Important Notice for additional details.

At the close of business on Friday September 14, 2007 the old database in PROD and PSE (test region) including the old PC WebDirect functionality will be disabled. The new Security Profile goes live in PROD on September 17, 2007.

Helpful Hint:

When a fund overrides or edits their hierarchal default values for "current" effective data via the DTCC WebDirect screens, the override indicator "O" will appear when the fund views the changed data.

When a fund overrides data that has a "future" Profile Effective Date, the "O" indicator will not appear until the future effective date becomes the current date.

II. Timeline

START DATE	END DATE	ACTIVITY
June 4, 2007	September 13, 2007	---Participants use new functions in new database in PROD ---No Firm output available in PROD during this period ---Funds and firms can use new Profile functions in PSE test region ---This is the scrubbing period for funds ---Funds must email NSCC authorization to release data for PROD in New Profile
	September 14, 2007	---Friday night after 8:30PM is the first time firms receive data file of entire new security issue

		database
	September 17, 2007	---New Profile live in PROD ---Standard input and output files begin to go out from New Profile ---Old Profile disabled in PROD

III. Output to Firms

The first output to firms from the new production security issue database will be sent on **Friday night September 14, 2007 sometime after 8:30PM** This one-time data file of complete current and future data on the new database will be sent out via AutoRoute 02110824 (Global Security) for this instance only. All the records will be marked with the Action Code /indicator value of "A" for ADD. The indicator of ADD is needed because firms are starting with a clean database and will have to ADD all the new Profile Security records. **Funds' data that has not been authorized to be released will not be sent to firms.**

Firms should contact their Relationship Manager to ensure that they are properly set up to receive this output file and also AutoRoute 02110825 (Specific Security).

The current standard input/output schedule will apply to the new Profile Security Issue database thereafter for both funds and firms.

IV. Additional Information on Profile Security Issue Database Redesign for DataScrubbing

A. Conversion Methodology

Information on DTCC's conversion methodology is provided below to help funds better understand the process that was used to convert existing data from the current Profile Security Issue database to the new Security Issue redesigned hierarchy database.

Funds participating in the Conversion Process were asked to complete spreadsheets with information to create the unique links that would allow the data to relate and flow between the four hierarchy levels. This information was required to:

- establish the data storage and management hierarchies for the new structure,
- allow NSCC to ascertain specific default data necessary for the new and updated data elements (fields), and
- establish the source data for default information and values used in populating the data in the hierarchies.

The fund instructed NSCC as to which Security Issue ID's data should be used to populate each level of the data hierarchy. This was accomplished by the fund selecting an "M", "S" or "P" indicator in the appropriate columns designating a specific Security Issue ID they wished to be used to populate the Management Company Level Hierarchy

Default information, the Share Class Level Hierarchy Default information, and the Fund Portfolio Hierarchy Default information.

If data existed in the old Profile Security Issue database, these values were converted to the new database at a Security Issue Level, without any changes being made to this data from the default data selected for the Hierarchy. All unique data took precedence over what was filtering down from the default Security Issue ID. The premise was that fund's data in the old database for a Security Issue ID was scrubbed and correct, and therefore would not be overridden by the hierarchy default values as defined in the spreadsheets.

Next, default values were applied (for new fields and blank fields that were not previously available in the Old Profile). The "Recommended Default Value" column in the Data dictionary provides information on how default values were applied.

B. How to Delete Data at the Security Issue Level to Apply Hierarchy Defaults

The new database was designed so that hierarchy default information established at the hierarchy levels would filter down to the Security Issue ID level. Hierarchal default data will transcend down to the Security Issue ID level if there was no data for that Security Issue ID or the data was the same (not different than the hierarchy default information).

Helpful Hint:

If a fund wants to delete unique data that was converted and apply hierarchy default information to a Security Issue ID, go to the Security Issue ID Level, select Delete Security Issue ID in the navigation bar to the left of the screen, expand the levels, and delete the data at the Management Company level, Share Class Level, Fund Portfolio Level and Security Issue ID level. (Hint: Do not try to blank out or delete individual fields. Click on the "Delete" button and all data will be removed automatically.) Then go to View the Security Issue ID at the Security Issue ID level. The default data will now appear that the fund established at the hierarchy levels. The hierarchy default data will filter down to the Security Issue ID level because the data was deleted for that Security Issue ID. Remember: there can only be one Security Issue ID attached to one Fund Portfolio name and one Share Class Name.

C. How to Delete All Data Transactions and Hierarchy Default Transactions and Start Over

A fund may want to change their hierarchy default data and start over. They can do this by going to the Data Management Transaction navigation bar and select Delete Security Issue Profile. Select Delete at each of the hierarchy levels - Management, Share Class, Fund Portfolio and Security Issue ID. Please refer to the Profile Security Issue Redesign WebDirect User Guide at http://funds.dtcc.com for more detailed information.

WARNING: The above action will remove all data in the database for your participant number. Please be certain you want to remove all data before taking this action.

Helpful Hint:

Before Share Class Name or Fund Portfolio name can be updated in the Hierarchy transaction screen, data that has already been created for a specific Share Class or Fund Portfolio must first be deleted.

Important Note: Security Issue IDs, Share Class names, and Fund Portfolio names cannot be deleted. These are key data fields. Only data associated with them can be deleted. A Security Issue ID, Share Class name and Fund Portfolio name together with the NSCC participant number creates the unique hierarchy links in the database so that data can be properly applied in the hierarchal structure in the database. If there is a need to delete a Security Issue ID, Share Class Name or Fund Portfolio Name, please contact your Relationship Manager for assistance.

D. Short Term Redemption Fee Data

Short Term Redemption (STR) Fee default hierarchy data is created at the Fund Portfolio Level. STR data will be applied to Security Issue IDs for those Fund Portfolios that have STR fees. STR data fields can be overridden at the Security Issue ID level. However, a fund cannot at the Security Issue ID level delete the entire STR default value fields since the system was designed for hierarchy default information to transcend down to the Security Issue ID level.

E. New Reject Codes

To better describe error message 0382, NSCC redefined this error message and created two additional reject codes. This change is in production and the complete Mutual Fund Profile Service Reject Code list is on our website http://funds.dtcc.com.

Reject Code	Old Error Message	New Reject Code	New Error Message
0382	Submitting Participant Invalid for Security Issue (MFP Security Master)	0382	Security Issue ID belongs to another Fund number
		0660	Another Security Issue ID exists with the same Fund number and Class name and Portfolio name
		0661	Security Issue ID exists with different Fund number, or Class name or Portfolio name

V. Technical Manuals and User Guides

The DTCC Security Profile WebDirect Users Guide and Profile Security Best Practices Guide are in the process of being updated. Copies of these revised documents will be available on our website next week at http://funds.dtrcc.com.

The following are common or frequently asked questions and their answers about the redesigned Profile Security Issue database:

Frequently Asked Questions

Question	**Answer**
Because the conversion and scrubbing period has been extended to September 17, 2007, do funds need to change the Profile Effective Date of their data on the system?	Funds do not need to change the Profile Effective Date from July 16, 2007 to September 17, 2007. All current and future effective data (input by September 17 or earlier) will be sent to firms on Friday night September 14th.
There is a new data field "Number of Eligible Social Codes" and its business definition is "The number of social codes eligible to purchase this fund". What is this?	Security Profile now has a table of Social Codes that are valid for a particular Security Issue ID. Social Code Eligibility is completed at the Share Class level. If you have a class that has no restrictions on what type of account can be opened, then you would list every single NSCC Social Code as valid for purchase. On the other hand, if you have a class that is only eligible for retirement business, you would only list these applicable social codes as being valid for purchase. The list of valid NSCC Social Codes can be found at http://funds.dtcc.com Social code eligibility hierarchy default data fields can be overridden at the Security Issue level. However, the default values established at the Class level cannot be completely deleted at the Security Issue ID level. Currently the Social Code field is a key data field. This is currently under review as a future enhancement to add flexibility to allow changing or removing social codes at the Security Issue ID level.

Why can't a fund change the name of a Share Class or Fund Portfolio?	Because these are key data fields. Once a fund creates a Share Class Name or a Fund Portfolio Name in the "Hierarchy Transactions" screens, and then proceeds to the" Data Transactions" screens and Creates/adds data for these names (key data fields), a fund cannot change the name of that Share Class or that Fund Portfolio in the "Data Hierarchy transactions" screens. The only way to change names at that point is to **delete all the data associated with that Share Class or Fund Portfolio.** Then go to the "Hierarchy Transactions" screens and either do a Create / Add or an Update/change Share Class Name or Create / Add or Update/change Fund Portfolio Name.
What does the error message " Errors: Unknown mainframe error code = "1111111" received" mean?	This error message means that a fund must first delete all data associated with this Share Class or Fund Portfolio. This Error Message will be changed to "Cannot Change Share Class Name or Fund Portfolio Name" Must first delete data associated with this Share Class or Fund Portfolio."
I participated in the spreadsheet conversion process. I have now made numerous changes to some "higher" hierarchal fields, such as at the Share Class Level, however, I am not seeing those changes filter down to the lower level Security Issue IDs. Is the trickle-down an auto feature, or is there something I am not doing right?	When you submitted your spreadsheet, you chose a default Security Issue ID at the Share Class Level. This Security Issue ID was designated by an "S" on the spreadsheet. Upon conversion, NSCC went to the old database and took those values and made it the DEFAULT Security Issue ID in the new database. The result was that every Security Issue ID you grouped on the spreadsheet (under that Share Class) would contain those same values. If there was no data in the old database for

	that Security Issue ID, NSCC allowed the DEFAULT data to flow down from the Share Class to the Security Issue ID Level. If there was data for that Security Issue ID in the old database, NSCC compared it to the DEFAULT data and if it differed, that Security Issue ID data was determined to be "unique." In other words, the Security Issue ID did not agree with the Default Security issue ID data and the unique data took precedence over what was filtering down from above. This means that Security Issue ID data in the old database overrode the default data in the new database at the Security Issue ID Level. If the Security Issue data in the old database agreed with the DEFAULT data then the DEFAULT data from above (Share Class) filtered down to the Security Issue ID Level. Therefore, when you changed the Share Class data, only the Security Issue IDs under that DEFAULT Security Issue ID will receive the changes. The fact that the Security Issue ID Level contains different information than the Share Class means you had data that was different in the old database. If you want all your Security Issue IDs to have the exact same characteristics of the DEFAULT Security Issue ID, then delete the data for those Security Issue IDs at the Security Issue ID Level. That will allow the Share Class info to flow down to all your Security issue IDs. Then when you make any changes at the Share Class Level all your Security Issue IDs will reflect it.

When I try to download my CSV report (User File Request) from the WebDirect screen I get the error message, "Selected Report Does Not Belong to The Selected Participant Number". Why is this happening?	You are receiving this error because you are not selecting the report that you want to download from the drop down menu. After entering your participant number, click on the refresh CSV File link. After that select the report you want to download.
Why can't I delete a Security Issue ID from the database?	Security Issue ID is a key data element. Security Issue IDs cannot be deleted. The data that is attached to the Security Issue IDs can be deleted. If a Security Issue ID has been erroneously associated with an incorrect Share Class name or Fund Portfolio name, please contact your Relationship Manager to discuss available options to make such corrections.
If we change something at the Share Class level (Breakpoint Schedules), it should populate down from the Share Class level to all Fund Portfolios and Security Issue IDs for that Share Class, but it only updated our default Fund Portfolio and Security Issue ID. All the other Fund Portfolio and Security Issue IDs still show the old information. Is this a bug?	There was information in the old database that was different from what you chose as the Security Issue ID used at the Share Class level default on your spreadsheet. Therefore, no matter what you change on the Share Class Level Breakpoint, that data will only flow to the Security Issue Id(s) that used the default data. You need to delete the specific Breakpoint data in the Security Issue level in order for the default data from up above to filter down and populate those Security IDs.
I submitted a User File Request in PSE and PROD using the WebDirect screens and then tried to download the Reports and no reports are available? What should I do?	Please contact your Relationship Manager. You may not be set up in PSE or PROD with the new AutoRoute ID numbers to receive the reports. You need to be set up in PROD with 02110157 for the MRO report or 02110161 for the CSV report. To receive the reports from PSE you need 02980157 for the MRO report or 02110161 for the CSV report.