

# The Depository Trust Company

# IMPORTANT

**B#:** 1092

**DATE:** December 11, 2000

**TO:** All Participants

**CATEGORY:** Executive Notices

**FROM:** DTCC Corporate Information Security

**ATTENTION:** PTS Users

**SUBJECT:** PTS Modernization Efforts Affecting Access Security

With DTCC's focus on delivering its services via Internet based technologies, the integration of Internet initiatives is being accelerated. PTS applications are in the process of being modernized with some functions becoming available in the first quarter of 2001. With our new services being developed for delivery via web-enabled technologies, at some future time new applications and service offerings may only be available via web-enabled technology. In order to participate in the upcoming implementation of PTS Modernization, individual PTS user IDs must be migrated to DTCC's new standard. This effort, announced in August, 2000, is now being expanded and is expected to be completed by mid-year 2001.

The steps leading up to the migration necessitate that each Participant formally establish one or more designated Access Coordinators, who will be responsible for "authenticating" those employees able to access DTCC's services. This user control over authentication will give Participants and other users helpful flexibility in using their staff resources; it also clarifies that the Participant is fully responsible for the process of identifying its employees who are able to access DTC or NSCC services.

As part of this conversion (and as described in Important Notices #Z99-001, dated November 16, 1999 and #0410 dated August 4, 2000), we intend to build on the "access coordinator" structure that was implemented for the PCWeb products. Documentation which provides more information on our migration effort is available from your Relationship Manager.

The first step for each Participant will be to formally identify its Access Coordinator(s) and execute the appropriate Access Coordinator form(s). Access Coordinators will be responsible for "authenticating" those

employees able to access our services. In granting access privileges to a Participant employee, the Participant is responsible (1) for ensuring that the employee appropriately protects those privileges (e.g., by safeguarding passwords), (2) for what that employee does with those privileges, and (3) for ensuring that those privileges are modified or revoked when necessary (e.g., if the employee changes jobs or leaves). As part of the process of granting access privileges, personal/confidential information about each employee - his or her name and business address, as well as a confidential PIN number and security pass phrase and the month and day of his/her birth - must be provided to DTCC, so that the identity of the user can be verified in the event that he or she requires support from DTCC's Customer Support Center. A new PTS update function "PSWD" is now available to all PTS users for the purpose of collecting this information.

Once a Participant's Access Coordinator(s) has been formally designed by an appropriately authorized individual, DTCC representatives will work with the Access Coordinator(s) to plan the migration of the organization's PTS user IDs to an industry-standard security package. This will permit users to select their own passwords (in accordance with system rules). It will also require that each user have his or her own individual sign-on. With the migration to the new access control system, users will be systematically required to change their passwords every 90 days and users that have not been signed-on within a thirty-day period will be prevented from accessing the system.

Any questions or comments may be directed to your Relationship Manager, Stash Jarocki, Chief Information Security Officer/Vice President at (212) 855-8831 or Diana King, Systems Security Director at (212) 855-3313.