SECURING CREDIT CARD/400™

The Administrator must take steps to insure the confidentially of their customer's information. This includes protecting Credit Card/400 from unwanted access on the AS/400. As shipped from BDS, the Credit Card/400 objects are not secured and the public can access them. Below are some security scenarios the administrator may consider when protecting Credit Card/400.

Credit Card/400 is shipped with *PUBLIC having *CHANGE authority to all objects in libraries BRODERICK and BDSDATA. Thus the strategies below remove varying amounts of authority to user profiles.

Note: These changes to authority will need to be re-applied after updating to a new release of Credit Card/400.

Minimal Security

This scenario is applicable when other measures are in place that will provide acceptable protection against unwanted access to Credit Card/400 information. An example would be a single application system with a limited number of users, all of which are blocked to menu options only. In this example, no changes to BDS objects are necessary.

Moderate Security

This scenario is applicable to most AS/400 systems. Reasonable security procedures are already in place but due to the size and complexity of the AS/400, some minor additional protection is recommended. The following procedure is recommended:

1) Determine and classify users. Three classifications are suggested:

Administrator	Can do everything
Operator	Start/Stop Remote Hosts, Build DC (Settlement) Batches
User	Process Credit Transactions

2) Revoke *PUBLIC authority to key Credit Card/400 objects. The following objects are needed to access the function shown. All shown objects should have their authority revoked from *PUBLIC and *CHANGE authority granted to the individual users.

Process Credit Cards:

BCCSNDRH	*PGM
CRDUSR	*CMD

System Operations:

Library BRODERICK

BCCBLDDC	*PGM
STRCCRMTH	*CMD
ENDCCRMTH	*CMD

Administrator:

BCCSETUP	*CMD
CRDADM	*CMD

You may consider your user classes as a hierarchy; Operations can do all User tasks plus theirs and Administrators can do all.

3) Review the programs that adopt their owner's authority. The list is provided below. Please note that for minimal and moderate security, BDS considers the programs in the list an acceptable security risk.

Maximum Security

This scenario is applicable to AS/400 systems with high security needs. The moderate security procedures above are recommended, with the following additions:

1) Revoke *PUBLIC authority (RVKOBJAUT cmd) from all Credit Card/400 objects (BCC* and the commands listed above) in libraries BRODERICK and BDSDATA.

2) For each user identified above, grant *CHANGE authority to the Credit Card/400 objects in library BDSDATA and *USE authority for objects in library BRODERICK.

3) Set up a special user profile for Remote Host tasks. The initial program for this user can be *SIGNOFF. As shipped from BDS, QSYSOPR is used. Grant this user authority to all Credit Card/400 objects (except the key objects listed in the moderate procedures) because it must be able to execute the Remote Host programs and access all data files. Change the Job Description BCCRMTH, user profile keyword, to the new user profile.

4) Change the programs that adopt authority to *USER. See below for the list. Implement the alternative listed for each program.

For questions implementing additional security measures, contact BDS technical support.

SECURING CREDIT CARD/400™

*Programs that Adopt *OWNER Authority*

Below is a list of programs that are created with the USRPRF(*OWNER) attribute. Because all objects are owned by QSECOFR, the programs have no authority limitations during execution. A brief description of the program describing the reason for the adopt and possible alternatives are given.

Note: Historically, Broderick Data Systems has only used adopt on CL programs. The source of most of these can be retrieved. The administrator may wish to inspect the programs.

BCC036. This program issues a submit job command using job description BCCRMTH, which specifies user QSYSOPR. Since most users do not have authority to QSYSOPR, the submit job will receive a function check if no adopt is used. The administrator may consider limiting the command to users and granting them authority to QSYSOPR.