Chapter 305 Appendix C

Examiner's Guide to Open Door

Introduction

Open Door is a web-based application that interfaces with the Corporate Credit Union Network (CCUN) and is used by corporate and member credit unions to enter and retrieve account information, initiate wire transfer requests, check share, loan, and investment rates, and transfer funds between accounts.

Modules

Open Door has several modules. For example, the web pages that support wire transfers make up a module. Other modules include Accounts, Transfers, Directory of Services, and Coin and Currency. Various functions may be performed within each module. An example is the Accounts module with three related functions: view account balance information, future dated transaction inquiry, and view selected history.

Corporate Credit Union Users and Member Credit Union Users

Two levels of Open Door users are recognized, corporate credit union users and member credit union users. Corporate users see all modules and menu options in Open Door including all security administrative functions. Member credit unions see a subset of menu options and have limited access to security administration functions with member credit union users restricted to changing their PIN and passwords. All other system administration is handled at the corporate user level.

Users and User IDs and Contacts

All users requiring access to Open Door are assigned a user ID. This user ID includes a user ID profile containing the authorization codes, dollar limits, and PIN information assigned to that user. Open Door also defines individual contacts, each representing a specific member credit union. A user ID is associated with one or more contacts, relating each user ID to a specific credit union or credit unions.

Each user holds a password, allowing access to the functions to which that user has been assigned permissions. A first time user must change the temporary password issued by the system administrator immediately upon logging on to the Open Door application. Future password changes are the responsibility of the user. A PIN number is assigned to the user if access to the wire transfer module is permitted.

Dual Controls

Open Door imposes dual control on both (1) security administrative activity and (2) initiation and release of wire transfer requests. An example of security administrative change using dual controls is when a corporate user with security administration access enters or updates someone’s authorization codes. A different corporate user with security administration access must approve the entry or change. Dual controls on wire transfer initiation and release are also imposed by Open Door as well. One authorized individual must initiate the wire transfer request and a second authorized party must approve or release the request.

Verification Bypass Authorization

Corporate users may be assigned a bypass verification authorization code for use in member credit union wire transfer request processing. This allows corporate users to bypass verification of member wires when no employee at the credit union is available to verify the wire request. Dual control is still maintained; however, a credit union and a corporate employee are now acting on the wire for two party approval rather than two member credit union employees.

PIN Security

PIN security is an option for some functions such as credit union pre-authorized wire requests. PIN security options are available both at the credit union level and the corporate credit union level. PIN security may be switched off; however, an alternative validation method must be indicated if PIN security is removed from member to member transfers, or wire transfers.

Summary

In wide use by corporates and member credit unions, Open Door provides the means to establish generally acceptable security options and controls on critical activities and transactions. The combinations, permutations, and unique application possibilities presented by the program preclude explicit instructions touching on all potential pitfalls. However, the following guidance is provided as a risk-based approach to examination of Open Door.

Examination Goals

The examination goal is to verify sound segregation of duties and to ensure appropriate controls are imposed on funds transfer activity.

There are three essential areas to review:

1. Sound Segregation of Duties. Segregation of duties is controlled by the Open Door system administrators at each corporate. Examination procedures should include review of the corporate's controls on adding new users, both corporate and credit union, changing user authorities, and deleting inactive or expired users;
2. Transaction Controls. The corporate system administrators impose these controls by assigning various functions to each user ID along with assigning any dollar limits associated with that user ID. Examination procedures should include a general review of the functions assigned to corporate employees within each module in Open Door, looking for inappropriate access assignments. Additionally, a specific review of the functions assigned to corporate employees with access to the wire transfer module should be completed to verify restricted access to wire transfer applications, ensure appropriate dollar limits are assigned to wire room employees, and verify that sound segregation of duties is maintained within the wire transfer application; and
3. Open Door Wire Processing Rules. The corporate system administrator selects certain wire processing rules that effect the combinations of individuals allowed to create and send a wire transfer as well as wire transfer dollar amounts requiring second party verification. A corporate may hold to a standard application of control setting or, may vary the control settings based on the needs or desires of the member credit union.

Examination procedures need to determine:

a) PIN security is "on" for sensitive transactions;
b) Wire option amount settings are appropriate; and
c) The "Verify Bypass" function is allowed only when other risk mitigation measures are present.

Examination Guidance

Request Items:
Related Policy
Related Procedures
Related Contracts & Agreements
Employee Listing with Job Titles
Open Door Report – Member Listing
Open Door Report – Update Member Profile
Open Door Report – OD900 Operator Authority Report
Open Door Report – Authorization Code Maintenance
Open Door Report – Update Corporate Authorization Codes
Open Door Report – OD040 Non-Financial Transactions
Open Door Report – OD002 Security Violations

Security Administration

The function of the security administrator within Open Door is similar to the Local Security Administrator (LA) in Fedline. Therefore, Open Door examination procedures are similar to reviewing the Fedline LA function. The same questions should be asked. Who are the administrators? Are there more than two employees assigned this function? Is a formal process in place to add, change, or delete user authorities? How is a new credit union user added? How is a new corporate user added? What happens if a credit union user loses a password? How often are passwords changed? How often are PIN numbers changed?

Transaction Controls

Wire transfers are the most critical funds transfer feature of Open Door. Other account transactions are possible; however, only a wire transfer moves funds out of the CCUN. Open door imposes strict dual controls on all wire transfers. Action on the part of two users must occur to (1) initiate and (2) release a wire transfer. However, the combination of employees providing that dual control is variable. Two credit union employees may initiate and verify a wire, a credit union employee and a corporate employee may complete these actions, or two corporate employees may provide the necessary parties. Clearly not all combinations of personnel would be appropriate in all situations, even though dual controls are present. A number of other questions should be investigated as well. Are all of the authorized wire requesters assigned appropriate dollar limits? Do surrogates have access to credit union IDs and authorities that don’t have dollar limits? What occasion would result in a physical callback? What dollar amount requires a physical callback? Are controls in general sufficient to minimize both the corporate’s and the credit unions’ risk?

Wire Processing Rules

Within each Member Profile Module there are dollar amount settings specifying the minimum dollar amount of a wire transaction requiring second party verification. In addition, dollar limits are allowed for new wires, pre-authorized wires, intra-network wires, and international wires. A setting of “0” requires all wire entries to be verified and a setting of 99,999,999 meaning no second-party verification is required unless the transaction is greater than 99,999,999.

The examiner needs to verify dollar limits and verification settings are established to provide adequate control of transactional risk. If the corporate or credit union has selected amounts greater than the default value of “0”, is the new amount supportable? Does the corporate request the credit union to establish dollar limits for each of its employees? Are corporate users’ dollar limits appropriate? Are credit union user limits frequently set at 99,999,999 rather than more realistic defaults? Is verification inappropriately bypassed for new wires or new templates? This review is most easily accomplished by reviewing (1) Open Door member profile screens (perhaps on a sample basis), (2) the corporate’s own settings for internal transactions, and (3) settings for large dollar participants.

There are also settings for pre-authorized wire template creation allowing establishment of a dollar limit on template creation and a choice for second-party verification to establish a new template. Default settings are “0” and “verification required”. Again, has the corporate deviated from the default settings and if so, are its actions supportable?

PIN security is another feature of Open Door allowing a selection of “on” or “off” for certain transactions. This is another member profile option setting and must also be reviewed on screen, from screen prints. Is PIN security turned off for any participant, and if so, why?

Unfortunately, as of this date, the member profile module does not support a printed report of wire option settings. They must be viewed on screen for each participating credit union and corporate or a query may be run and printed by the corporate. Sampling may suffice if corporate policy and procedures are strong.

OFAC Compliance

OFAC compliance is not a part of the Open Door system. Corporates are responsible for OFAC compliance for all wires processed through the system. Corporates cannot pass the responsibility to the member credit union, U.S. Central, or corresponding bank. Examiners must ensure that the corporate has developed a procedure to monitor all funds transactions by this system either by software or physical review of each transaction.

Contingency Plans

The corporate should have a written contingency plan that addresses the movement of funds should Open Door not be available. The plan should include how the request will be taken from the member credit union and alternative PIN numbers for emergency use. This can be accomplished by telephoning in wire requests and establishing emergency PIN numbers assigned and maintained by both parties.

Further Information

U.S. Central Credit Union has developed an Open Door Training Manual for program participants. This manual is available for reference at participating corporate credit unions and member credit unions and offers an in depth discussion of Open Door’s features and controls.