Appendix 306A

EXAMINER'S GUIDE TO APEX SECURITY SETTINGS

Introduction

APEX is U.S. Central Federal Credit Union's (USC) Internet based Automated Clearing House (ACH) processing system. This system allows participating corporate and natural person credit unions to submit ACH files to the Federal Reserve through USC using any PC with an Internet connection.

The participant, not USC, is responsible for establishing the system's various control features. This guide is intended to allow an examiner to determine whether or not the settings in use by the participant are appropriate and meet basic safety and soundness standards. It is not intended to be a complete review of ACH operations.

What to Ask For:

The examiner should request printouts of the following two screens or view the screens on the participant's PC:

1. ACH Options Screen
2. ACH Security Settings Screen

The ACH Options Screen provides a summary report that will allow the examiner to determine whether the exposure limits settings, dual controls features, and permitted transaction settings are "on" or "off".

The ACH Security Settings Screen provides a summary report of terminal control settings including password standards and password change intervals.

What to Look For:

A representation of each screen, an explanation of the settings, and recommended settings necessary to activate critical internal control features of APEX are provided in this guide.

By comparing the settings displayed on the participant's screens with the commentary and recommendations, the examiner can determine if the settings, as established by the participant, provide the basis for sound internal controls on APEX system access and ACH file creation.

APEX Credit Union Definition Screens

ACH Options

Should ACH risk management be performed? ○ Yes ○ No

Third Party ACH Operator? ○ Yes ○ No

Must batches be reviewed? ○ Yes ○ No

Must templates by reviewed? ○ Yes ○ No

Are PPD payments permitted? ○ Yes ○ No

Are CCD payments permitted? ○ Yes ○ No

Are TAX payments permitted? ○ Yes ○ No

Are CTX payments permitted? ○ Yes ○ No

Are ENR payments permitted? ○ Yes ○ No

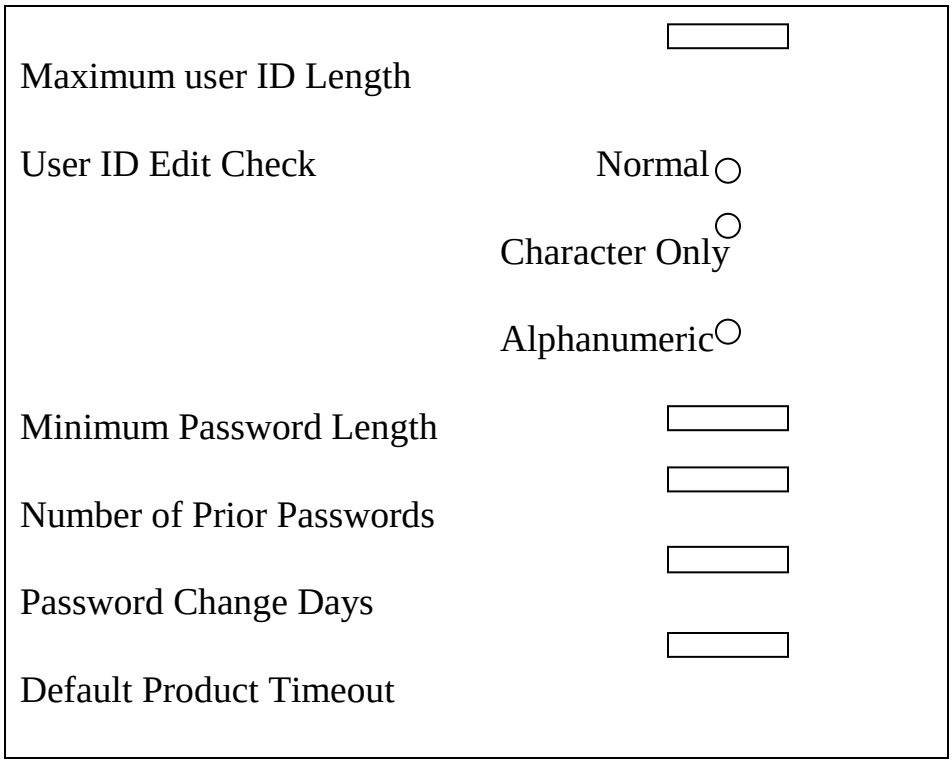
Are XCK payments permitted? ○ Yes ○ No

Security Parameters

Must users be approved? ○ Yes ○ No

Number of invalid logons ☐

Minimum user ID Length ☐


Maximum user ID Length
User ID Edit Check
Normal
Character Only
Alphanumeric
Minimum Password Length
Number of Prior Passwords
Password Change Days
Default Product Timeout

ACH Options Settings

Should ACH risk management be performed?

A "yes" setting requires an exposure dollar limit to be established. The exposure limit establishes the maximum dollar amount allowed for a single file or a cumulative maximum dollar amount allowed for one day's transactions. Any credit union originating ACH debit or credit entries should have an exposure limit set, both for its own internal applications and for any ACH customers transmitting ACH files through the credit union (such as a sponsor or payroll processor). **A "no" setting is a material internal control weakness for an Originating Depository Financial Institution (ODFI) and exception should be taken.**

If PPD payment or CCD entries are permitted (see description of these settings below), the setting should be "yes" with a maximum allowable dollar amount established for each type of entry. A no setting would only be appropriate if the credit union's origination activity is limited to returns and non-financial ACH entries.

Third Party ACH Operator?

A "yes" setting allows the credit union to create ACH files for multiple companies or entities such as small employee groups (SEG). A "no" setting means files may be created for only one entity, usually the credit union itself. Neither setting is critical to internal controls. Either a "yes" or "no" is acceptable; however the setting should reflect actual operations.

Must batches be reviewed?

This setting establishes dual controls on ACH file creation. The preferred setting is "yes". **A "no" setting is a material internal control weakness for a credit union sending PPD or CCD entries (see description of these settings below) since it would allow an individual to create and send an ACH file without second party review.**

Must templates be reviewed?

This setting establishes dual controls on ACH template creation. Templates reduce the entry time required for recurring files by pre-formatting some of the necessary information. The preferred setting is "yes". **A "no" setting is a material internal control weakness since it would allow someone to create a fictitious template without second party review.**

Are PPD payments permitted?

A "yes" setting allows consumer ACH debit and credit transactions to be entered. If ACH activity is to be limited to only ACH returns and non-financial transactions, the setting should be "no".

Are CCD payments permitted?

A "yes" setting allows corporate cash concentration entries to be created. This activity is generally undertaken for businesses and potentially involves high dollar amounts. A credit union involved with only consumer ACH transactions does not need this authority and the setting should be set at "no".

Are TAX payments permitted?

ACH activity involving a member's tax payments holds significant risk. A "yes" setting for ACH tax activity should be carefully considered by the examiner. Management should demonstrate that it understands the risks associated with this type of activity.

Are CTX payments permitted?

This ACH application is for corporate trade exchange entries. This will rarely be applicable to credit union ACH operations and for most users the setting should be "no."

Are ENR payments permitted?

ENR ACH entries are automated enrollment entries to sign a member up for government electronic benefits payments such as social security or other pension programs. Even a small credit union that is not involved in ACH financial entries will likely want this setting to be "yes". Since ENR entries are non-financial and do not involve the actual payments themselves, a "yes" setting represents minimal risk.

Are XCK payments permitted?

XCK entries involve destroyed checks. Having this setting at "yes" would rarely be necessary for a credit union; although, a "yes" setting in itself holds minimal risk.

APEX Security Parameter Settings

Must users be approved?

This setting enables required second party approval for adding a new user or changing an existing user's authorities. **A "no" setting is a material internal control weakness and exception should be taken since a no setting allows changes to user authorities without second party review.**

Number of invalid logons?

An appropriate number of invalid logon attempts is 3. A setting greater than 3 holds increased risk. If the setting is significantly higher than 3, exception should be taken.

Minimum user ID Length?

The default setting is 4. Exception should be taken if this setting is less than 3 since a shorter ID holds a higher risk that the ID could be chanced upon or compromised.

Maximum user ID Length?

APEX allows user IDs to be up to 16 characters in length. The higher the number assigned, the lower the risk of a compromised ID. Industry security practices recommend minimum user ID lengths of 7 or more characters. ID lengths of 4 or 6 characters are common. However, examiners should encourage credit unions to adhere to industry best practices.

User ID Edit Check?

User IDs may be letters, numbers, or a combination of both. The best security is provided by a combination of letters and numbers including both upper and lower case characters.

Minimum Password Length?

Passwords should be no less than four characters in length. However, industry best security practices encourage passwords of 7 or more characters. Examiners should encourage credit unions to adhere to industry best practices.

Number of Prior Passwords?

Password changes should require at least three change intervals before a password can be reused. (See Password Change Days)

Password Change Days?

The recommended password change interval is no less than 30 days.

Default Product Timeout?

This setting invokes a screen saver (blank screen) after the established time period of inactivity. A setting of 10 minutes or less is recommended as an industry best security practice; although the APEX default value is 15 minutes.