

---

# Privacy Controls

## Controlling Access to Member Accounts

### INTRODUCTION

More and more, credit unions have become concerned about securing members' personal data – as well as the access to that information. CU\*BASE Privacy Controls allow credit unions to heighten the controls placed on this data, through masking, as well as requiring the entry of information to access member accounts.

### CONTENTS

WHAT IS PRIVACY CONTROLS?.....	2
PRIVACY CONTROLS CONFIGURATION.....	3
PRIVACY CONTROL CONFIGURATION SCREEN	3
MASKING DATA USING PRIVACY CONTROLS.....	6
WHAT A PERSON ACCESSING THE ACCOUNT MIGHT SEE	7
CODE WORD.....	8
RULES FOR ACCESS	9
WHAT A PERSON ACCESSING THE ACCOUNT MIGHT SEE	9
OUT-OF-WALLET AUTHENTICATION	10
RULES FOR ACCESS	11
WHAT A PERSON ACCESSING THE ACCOUNT MIGHT SEE	11
SECURITY CONTROLS.....	13
OVERRIDE OF LOCKED ACCOUNT	13
REPORTING ON ACCESS TO ACCOUNTS/OVERRIDE OF LOCKED ACCOUNTS	14

Revision date: March 16, 2012

For an updated copy of this booklet, check out the Reference Materials page of our website:  
[http://www.cuanswers.com/client\\_reference.php](http://www.cuanswers.com/client_reference.php)  
CU\*BASE® is a registered trademark of CU\*Answers, Inc.

---

## WHAT IS PRIVACY CONTROLS?

In a nutshell, Privacy Controls allows credit union control over who sees members' personal data in Teller, Phone Operator and Inquiry screens. A credit union might decide, for example, to use Privacy Controls configuration to mask all but the last four digits of the member's social security number. When this configuration is in place, an outside person assisting one of their members will see asterisks in place of the social security number (\*\*\*-\*\*-1234).

Privacy Controls also allows the credit union to require that a code word be entered or out-of-wallet question be answered to access a member's account. This ensures that when an outside person assists the member, they will be required to ask for this information.

Privacy Controls configuration has separate configurations for internal staff versus outside people who might assist members. Because of this, credit unions can even use Privacy Controls on their own staff members to ensure that authentication practices are followed internally as well. For example, credit unions can use this feature to ensure that their own staff always asks for a member's code word before entering the member's account.

# PRIVACY CONTROLS CONFIGURATION

## PRIVACY CONTROL CONFIGURATION SCREEN

### MNCNFC #27-Privacy Controls Configuration

Data Element	Display for CU Staff	Display for Other Staff
SSN/TIN	<input checked="" type="checkbox"/> 9 characters	<input checked="" type="checkbox"/> 9 characters
Driver's license (blank-all)	<input checked="" type="checkbox"/> 20 characters	<input checked="" type="checkbox"/> 20 characters
	<input checked="" type="checkbox"/> Phone #	<input checked="" type="checkbox"/> Phone #
	<input checked="" type="checkbox"/> Birth date	<input checked="" type="checkbox"/> Birth date
	<input checked="" type="checkbox"/> Birth year	<input checked="" type="checkbox"/> Birth year
	<input checked="" type="checkbox"/> Mother's maiden name	<input checked="" type="checkbox"/> Mother's maiden name
	<input checked="" type="checkbox"/> Address	<input checked="" type="checkbox"/> Address
	<input checked="" type="checkbox"/> City/state/ZIP	<input checked="" type="checkbox"/> City/state/ZIP
	<input checked="" type="checkbox"/> Code word	<input checked="" type="checkbox"/> Code word
	<input checked="" type="checkbox"/> eMail address	<input checked="" type="checkbox"/> eMail address

Teller confirmation questions

Display pop-up window if code word exists     Display pop-up window if code word exists

Ask other questions from database elements     Ask other questions from database elements

Phone Op confirmation questions

Display pop-up window if code word exists     Display pop-up window if code word exists

Ask other questions from database elements     Ask other questions from database elements

The screen allows credit unions to differentiate between what will be visible to their credit union employees (Display for CU Staff) versus what shared branching tellers or Xtend call center staff see (Display for Other Staff).

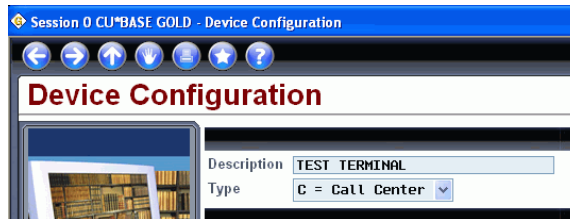
Using the top section of the screen, credit union can decide to mask private information they deem important. For example, a credit union may choose to mask all but the last 4 digits of a member's SSN/TIN whenever the Teller, Phone Operator or Inquiry screens are used by someone other than their own staff.

The bottom section of the screen determines which individuals are required to enter the members code word and/or answer an out-of-wallet question in order to access a member's account via Phone Operator, Teller or both.

## What Determines if a person is considered "Other Staff"

A person is considered "Other Staff" when:

- The person enters your shared branching ID on the Teller posting screen
- The person does not have a workstation configured for your credit union
- The person has a workstation configuration with a Type of C=Call Center



## How Does this Affect Call Centers and Working with Client Services?

Call Centers will be considered "Other Staff" and will have the restrictions placed on the configurations for this setting because they will have a workstation configuration Type of "C-Call Center." Client Service Representatives may also be restricted, depending on their configuration.

## Special Restrictions Placed on "Other Staff"

Restrictions are placed on people accessing your accounts based on whether they are considered "Staff" or "Other."

- If a person is defined as an "Other Staff", this person will not have access to certain function key and buttons, such as the Household Statistics button on Verify ID, Teller and Phone Operator screens, since this gives access to personal information that is not subject to the Privacy Controls configuration.

## HOW TO DETERMINE THAT PRIVACY CONTROLS ARE "ON" FOR A USER

When a user is configured to have Privacy Controls activated, the user will be notified of this condition when he or she accesses Inquiry, Phone Operator and Teller. If access is restricted a conditional badge will appear on the entry screen.

This user is configured to have Privacy Controls turned on. "Masking" indicates that items will be masked on the Inquiry, Teller and Phone Operator screens. "Questions" indicates that either Code Word or Security Questions (or both) will be required for entry.

Session 0 CU\*BASE GOLD - Phone Operator Member Lookup

Network Links

### Phone Operator Member Lookup

Employee ID  Password   
Account base

**Privacy controls are ON**  
 Masking  Questions  
This workstation is Call Center

Search Criteria

Last name  First name   
Employee #  Credit card   
Reference  SSN  (Enter 3 digits)

Account #	Member Name	SSN/TIN	Employee #	Reference

Cancel F7

FR (394) 7/28/11 16:12:19 [Learn About This Feature](#)

# MASKING DATA USING PRIVACY CONTROLS

Using the Privacy Controls configuration, credit unions can select to mask private data on selected screens. If configured to be masked, the selected items will be appear as asterisks when the person (according to role) accesses screens via Inquiry, Phone Operator or Teller.

Data Element	Display for CU Staff	Display for Other Staff
SSN/TIN	<input type="checkbox"/> characters	<input type="checkbox"/> characters
Driver's license (blank=all)	<input type="checkbox"/> characters	<input type="checkbox"/> characters
	<input checked="" type="checkbox"/> Phone #	<input type="checkbox"/> Phone #
	<input checked="" type="checkbox"/> Birth date	<input checked="" type="checkbox"/> Birth date
	<input checked="" type="checkbox"/> Birth year	<input checked="" type="checkbox"/> Birth year
	<input checked="" type="checkbox"/> Mother's maiden name	<input checked="" type="checkbox"/> Mother's maiden name
	<input checked="" type="checkbox"/> Address	<input type="checkbox"/> Address
	<input checked="" type="checkbox"/> City/state/ZIP	<input type="checkbox"/> City/state/ZIP
	<input checked="" type="checkbox"/> Code word	<input type="checkbox"/> Code word
	<input type="checkbox"/> eMail address	<input checked="" type="checkbox"/> eMail address

Items that can be masked are shown above and include the following:

- Number of characters of SSN (to display)
- Number of characters of license number (to display)
- Phone #
- Birth date
- Birth year
- Mothers' maiden name
- Address
- City/State/Zip
- Code word
- e-Mail address

Items that are *unchecked*, will show as asterisks. If you choose to mask certain digits in the social security number or driver's license, the masked numbers will show as asterisks (for example \*\*\*-\*\*-1234 in place of a Social Security Number). If there is no data, such as no email address, the area will remain blank on the screen and no asterisks will appear, indicating that there is nothing to show on the screen.

- NOTE: If your credit union masks any part of the address, the Print Envelope icon will not appear on the Verify ID, Inquiry and Phone Operator screens, since this could give access to the address.

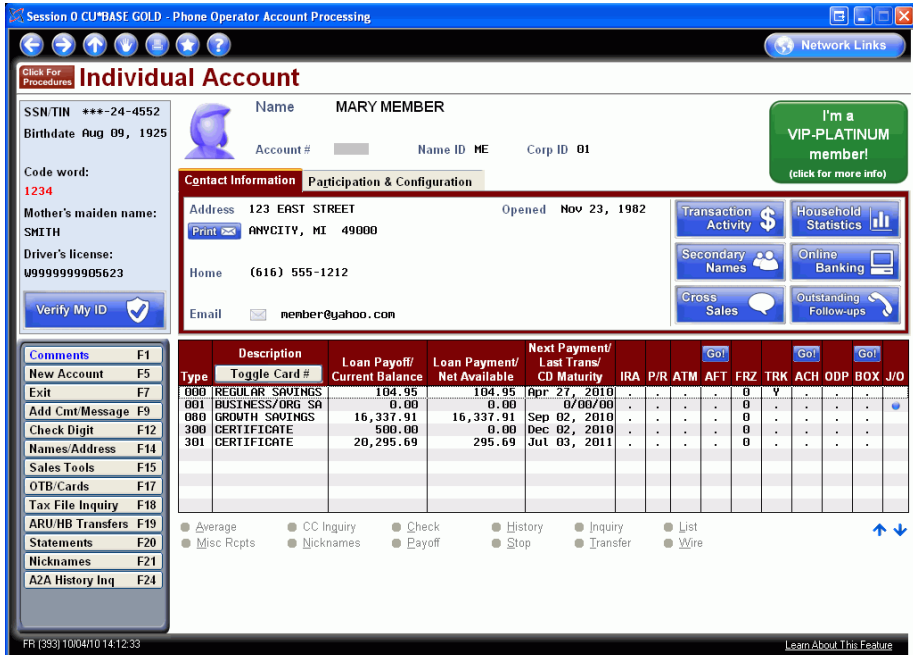
# WHAT A PERSON ACCESSING THE ACCOUNT MIGHT SEE

## Example of Phone Operator Screen with Masking



In the example above, the person accessing the account was configured as “Other Staff.” Everything was masked by the credit union for this type of person, except for the last four digits of the social security number and the last five digits of the license number.

## Example of Same Screen without Masking (except for SSN)



In the example above, the person accessing the account was configured as “CU Staff.” Nothing was masked except for the last four digits of the SSN.

# CODE WORD

Members give the credit union a code word with the expectation that they will be asked for it prior to an employee accessing their account (especially when they are serviced on the phone since they are not present to provide identification).

Using Privacy Controls, a credit union can require that people categorized as “Other Staff” are required to enter the member’s code word in a pop-up screen before accessing the member’s account. Credit unions can also configure this setting for their own staff to ensure that they ask for it as well. If the code word pop-up screen appears and the code word is not entered correctly, the person will not be able to access the account.

- NOTE: The pop-up screen will not appear if the member does not have a code word for his or her membership.

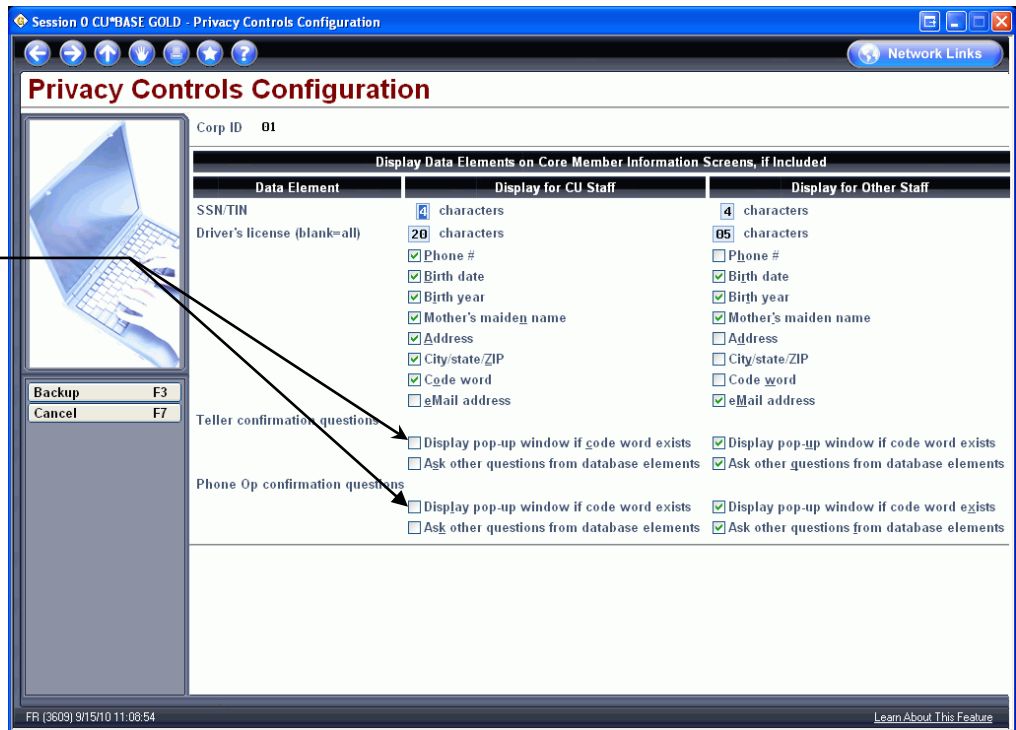
Separate controls allow credit unions to select that this feature be active in Teller or Phone Operator or both. This can be used in conjunction with Out-of-Wallet questions or not (see following section), depending on the credit union’s preference.

## Code Word Configuration Control

Display pop-up window if code word exists

## Privacy Controls Screen

Separate controls are available for “CU Staff” and “Other Staff.” There are separate Teller and Phone Operator, as well.



## RULES FOR ACCESS

If code word is activated, you will not be able to enter the account until you enter the correct code word. After three incorrect code entries, the account will lock and you will not be able to access the account until the lock is overridden by an employee using the Override feature at the *member* credit union.

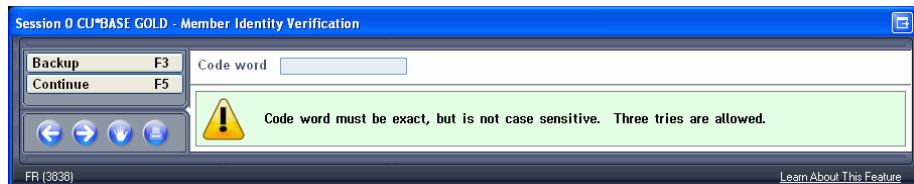
Retries Exceeded



## WHAT A PERSON ACCESSING THE ACCOUNT MIGHT SEE

If a person accessing an account is required to enter the code word *and the member has one*, the person will be presented with the following screen:

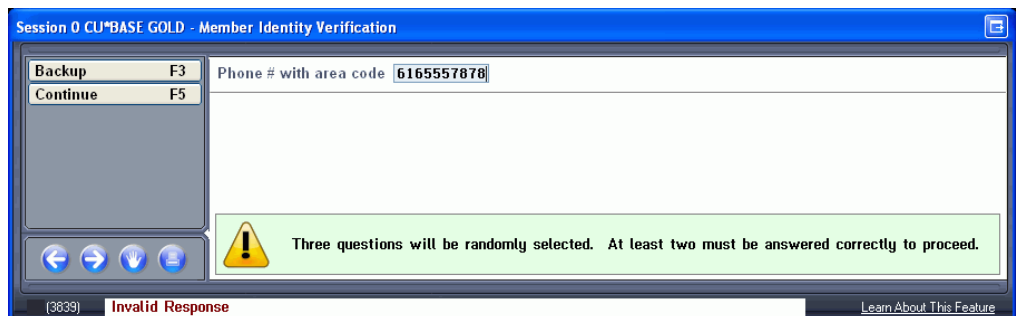
Code Word Pop-Up Screen



After entering the code word, the person uses F5-Continue to enter the account. If the correct code word is entered, the person will either access the account (viewing the Verify Member screen and/or any other comment window first), or move on to the Out-of-Wallet question screens.

If an incorrect answer is entered, messaging will appear alerting the person of this condition.

Code Word Pop-Up Screen - Invalid Entry



## OUT-OF-WALLET AUTHENTICATION

When a credit union activates Out-of-Wallet questions, the person accessing the account is required to correctly answer three questions (from data found in the MASTER file) before the person can access the account. Separate pop-up screens appear, each with a different question that must be answered.

Questions for individuals include:

- Last four digits of SSN
- Birth date (mmddccyy)
- Phone number with area code (home, work, or other will work, as long as the number is a complete number with area code and all numbers are not the same)
- Zip code (first five digits only)
- Mother's maiden name (if exists on the system)

(For organizations the last four digits of the TIN, charter date, phone number with area code and zip code are used.)

As with the code word configuration, separate controls allow credit unions to select that this feature be active for "CU Staff" or "Other Staff" (or both). Additionally, there are different configurations for Teller or Phone Operator. This can be used in conjunction with code word or not, depending on the credit union's preference.

Code Word Configuration Control

Ask other questions from database elements

Privacy Controls Screen

Separate controls are available for "CU Staff" and "Other Staff." There are separate Teller and Phone Operator, as well.

Session 0 CU\*BASE GOLD - Privacy Controls Configuration

Privacy Controls Configuration

Corp ID 01

Display Data Elements on Core Member Information Screens, if Included		
Data Element	Display for CU Staff	Display for Other Staff
SSN/TIN	<input checked="" type="checkbox"/> 4 characters	<input type="checkbox"/> 4 characters
Driver's license (blank=all)	<input type="checkbox"/> 20 characters	<input type="checkbox"/> 05 characters
	<input checked="" type="checkbox"/> Phone #	<input type="checkbox"/> Phone #
	<input checked="" type="checkbox"/> Birth date	<input type="checkbox"/> Birth date
	<input checked="" type="checkbox"/> Birth year	<input type="checkbox"/> Birth year
	<input checked="" type="checkbox"/> Mother's maiden name	<input type="checkbox"/> Mother's maiden name
	<input checked="" type="checkbox"/> Address	<input type="checkbox"/> Address
	<input checked="" type="checkbox"/> City/state/ZIP	<input type="checkbox"/> City/state/ZIP
	<input checked="" type="checkbox"/> Code word	<input type="checkbox"/> Code word
	<input type="checkbox"/> eMail address	<input checked="" type="checkbox"/> eMail address
Teller confirmation questions		
	<input type="checkbox"/> Display pop-up window if code word exists	<input checked="" type="checkbox"/> Display pop-up window if code word exists
	<input type="checkbox"/> Ask other questions from database elements	<input checked="" type="checkbox"/> Ask other questions from database elements
Phone Op confirmation questions		
	<input type="checkbox"/> Display pop-up window if code word exists	<input checked="" type="checkbox"/> Display pop-up window if code word exists
	<input type="checkbox"/> Ask other questions from database elements	<input checked="" type="checkbox"/> Ask other questions from database elements

Backup F3  
Cancel F7

FR (3609) 9/15/10 11:08:54 [Learn About This Feature](#)

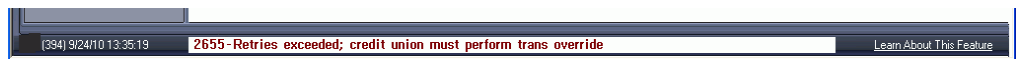
## RULES FOR ACCESS

The entry of two correct answers are required to advance to the account. If at least four answers exist in the database, the person can use F10-Next Question to advance to the next question. (This option can only be taken one time. Once it is selected, F10 disappears from the next popup screen.) Once an answer is typed in the field, the person uses F5-Continue to advance to the next question (pressing Enter does nothing).

A person can enter two incorrect answers; on the third wrong answer, the account is locked and the person will not be able to access the account until the lock is overridden by an employee using the Override feature at the member credit union.

- NOTE: Two incorrect answers for the same questions count as two wrong answers, for example if two wrong phone numbers are entered, the next wrong answer will lock the account.

Three Incorrect Entries



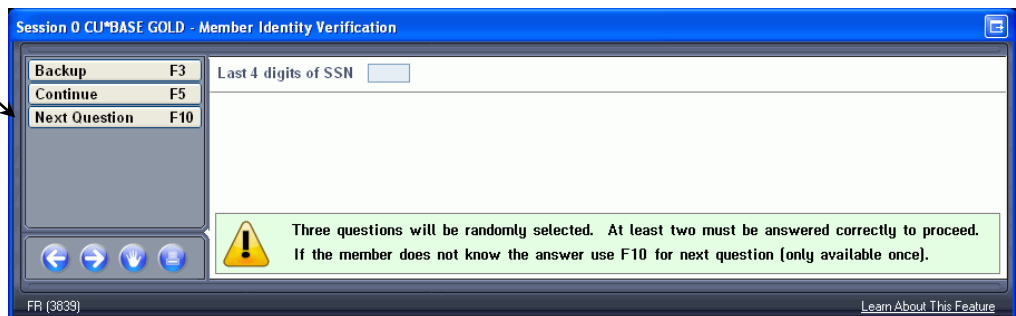
## WHAT A PERSON ACCESSING THE ACCOUNT MIGHT SEE

Here is an example of what a first Out-of-Wallet question might look like. (A list of possible questions is listed on the previous page.) This screen will either appear after the Code Word Pop-up screen (if this is activated), or directly after the person enters the account number (and Shared Branch ID if required).

If a correct answer is entered, the person entering the account may use F5-Continue to advance to the next question. After two correct answers, the person is able to access the account, after first viewing the Verify Member and/or any other comment screens.

Sample First Out-of-Wallet Question

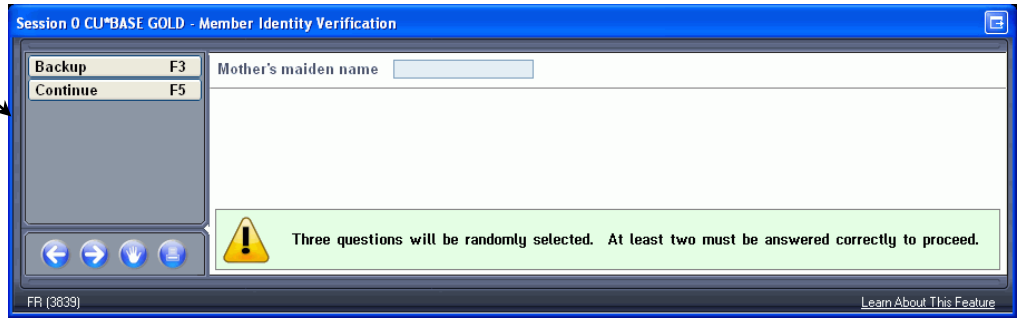
If there are at least four answers in the database, F10-Next Question appears on the screen. You will be able to select this option one time.



If there are at least four answers in the database, F10-Next Question appears on the screen. You will be able to select this option one time.

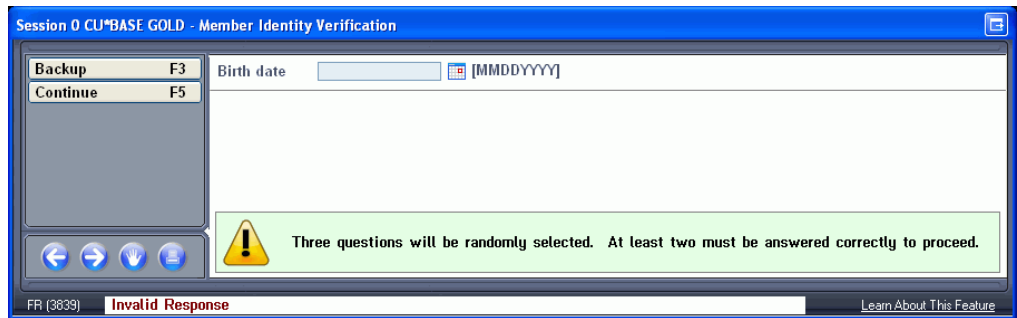
### Sample Out-of-Wallet Question Once F10-Next Question is Selected

Here we see that F10-Next Question was selected. This option no longer appears.



If the wrong answer is entered and F5-Continue is selected, messaging will appear showing that an invalid response was entered. This will be counted as one invalid response. (On the third invalid response, the account is locked.)

### Sample Out-of-Wallet Question With Invalid Response



# SECURITY CONTROLS


## OVERRIDE OF LOCKED ACCOUNT

Once the account is locked (either by three invalid code word or out-of-wallet question answer), it cannot be accessed until the lock is overridden by an employee with override privileges at the *member* credit union.

The override feature can be accessed via F2-Trans Override on the Main Teller Posting, MNADJ #19-Perform Transaction Override or via #7-Supervisor transaction override on the Time Out Window.

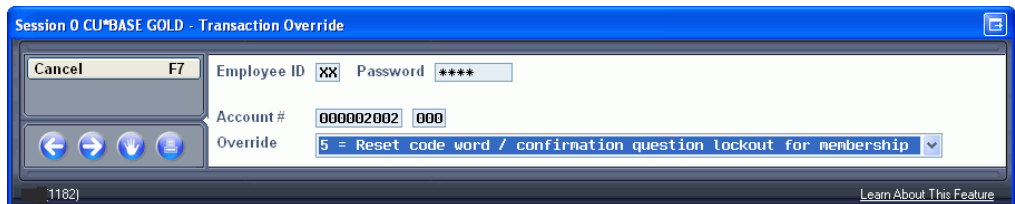
All access points will bring you to the same screen:

Override Screen



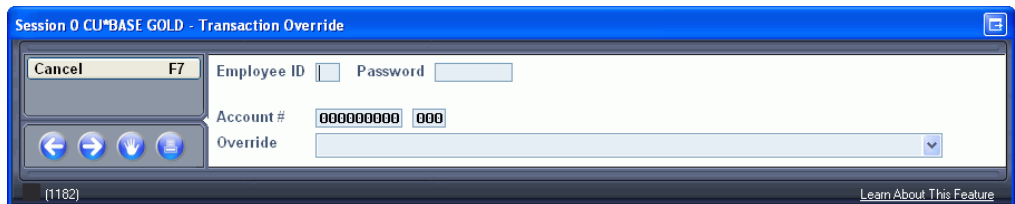
Enter your employee ID and password (if required) and the base account. Select #5 – Reset code word / confirmation question lockout for membership from the drop-down menu.

Override Screen – Selection Made



Press Enter on the screen shown below to remove the lock on access to the selected account.

Lock Removed



# REPORTING ON ACCESS TO ACCOUNTS/OVERRIDE OF LOCKED ACCOUNTS

## SECAUD File and Query

Each time a code word or out-of-wallet answer is entered, this entry is recorded in the SECAUD file. The Access Granted column shows if this entry resulted in access toward entering the account (Y) or in a locked account (N). A canned Query of this file can be accessed via the Report Builder 1 menu (MNQUERY) #26-SECAUD-Employee Activity. Each entry (each code word and out-of-wallet answer) is recorded in a separate line in the file.

SECAUD File - Security Question and Code Word Access

Line	DATE	Emp ID	Employee Name	Account Number	Access Granted	Program	User	Work Station	Time (HHMMSS)	CU#	
000019	09/16/2010	Y	MEYERS	2002	Y	DNFIRM	QST	R	IM	14:31:23	112
000020	09/21/2010	Y	MEYERS	1075	N	DNFIRM	QST	R	IM	11:18:49	112
000021	09/21/2010	Y	MEYERS	2002	N	DNFIRM	QST	R	IM	11:22:25	112
000022	08/03/2010	Y	MEYERS	2002	Y	CODE WORD	R	IM	12:01:52	112	
000023	08/03/2010	Y	MEYERS	2002	Y	CODE WORD	R	IM	14:28:02	112	
000024	08/03/2010	Y	MEYERS	2002	Y	CODE WORD	R	IM	11:47:34	112	

## Member Transaction Override Report

The Transaction Override Report allows you to review the number of times the lock on an account was overridden. Using the Code Word/Confirm Quest in the Override Type drop-down menu option will result in a report recording the overrides of this type.

MNADJ #27-Member Transaction Override Rpt

**Override Transaction Register**

**Report Options**

- Application type: [ ]
- Override type: [ ]
- File type: [ ]
- Date of file: [ ]
- Member branch #: [ ]
- Transaction branch #: [ ]
- General ledger account #: [ ] Optional
- Date type: [ ]
- Account base: [ ] Optional
- Transaction code/type (01-99, 01-99): [ ] [ ] Optional

**Response**

- ALL
- ALL
- U = Code word/Confirm Quest**
- F = Frozen
- P = Par value
- S = Secured
- U = Uncollected

**Job queue**

- Job queue
- Copies: [ 1 ]
- Printer: [ P1 ]

Cancel F7

FR (918) 10/04/10 14:22:49 [Learn About This Feature](#)

## Insider/Due Diligence Report

For reporting on Insiders, use the Account Security access/security audit selection on the Insider/Due Diligence Report. The report has two sections: one with each time a code word or out-of-wallet question was entered and one with the times that access was denied. If you check the “List only if access not granted” box, only the report that lists the times that access was denied will be printed.

### MNAUDT #17-Insider Due Diligence Report

Date	EMP ID	Employee Name	User ID	Work Station	Time (HHMMSS)	CU#	Program	Acct Number	Access Granted
10/04/10 15:16:38 BETA TESTING CREDIT UNION LACCSAUD PAGE 1 Insider/Employee Audit Report - ACCOUNT ACCESS/SECURITY AUDIT USER ALYCIAM For the Period 9/27/2010 to 10/04/2010 Member/Employee Type: 1									
09/30/10	-9	MARY EMPLOYEE	MARYV	MARYVG0	151957	112	CNFIRM QST	1111	N
09/30/10 15:16:38 BETA TESTING CREDIT UNION LACCSAUD PAGE 2 Insider/Employee Audit Report - ACCOUNT ACCESS/SECURITY AUDIT USER ALYCIAM For the Period 9/27/2010 to 10/04/2010 Member/Employee Type: 1									
09/30/10	-9	MARY EMPLOYEE	MARYV	MARYVG0	152846	112	CNFIRM QST	1111	N
09/30/10	-9	MARY EMPLOYEE	MARYV	MARYVG0	154032	112	CNFIRM QST	1111	Y
10/01/10	-9	MARY EMPLOYEE	MARYV	MARYVG0	83711	112	CNFIRM QST	1111	N
10/01/10	-9	MARY EMPLOYEE	MARYV	MARYVG0	134142	112	CNFIRM QST	1111	Y
***END OF REPORT***									

- The first page lists the accounts where access was denied. The second page lists all access attempts on the account.