



**WELCOME TO THE**  
**9TH ANNUAL CONVERSATIONS ON**  
**COMPLIANCE**

**MAY 15, 2024**

# AuditLink

CU\*ANSWERS Management Services

# AuditLink

CU\*ANSWERS Management Services

# NASCUS

The National Association of State Credit Union Supervisors

LET'S TAKE A 15-MINUTE  
BREAK!

# AuditLink

CU\*ANSWERS Management Services



Lillie  
Resource Group



# CU\* Answers Conversations on Compliance

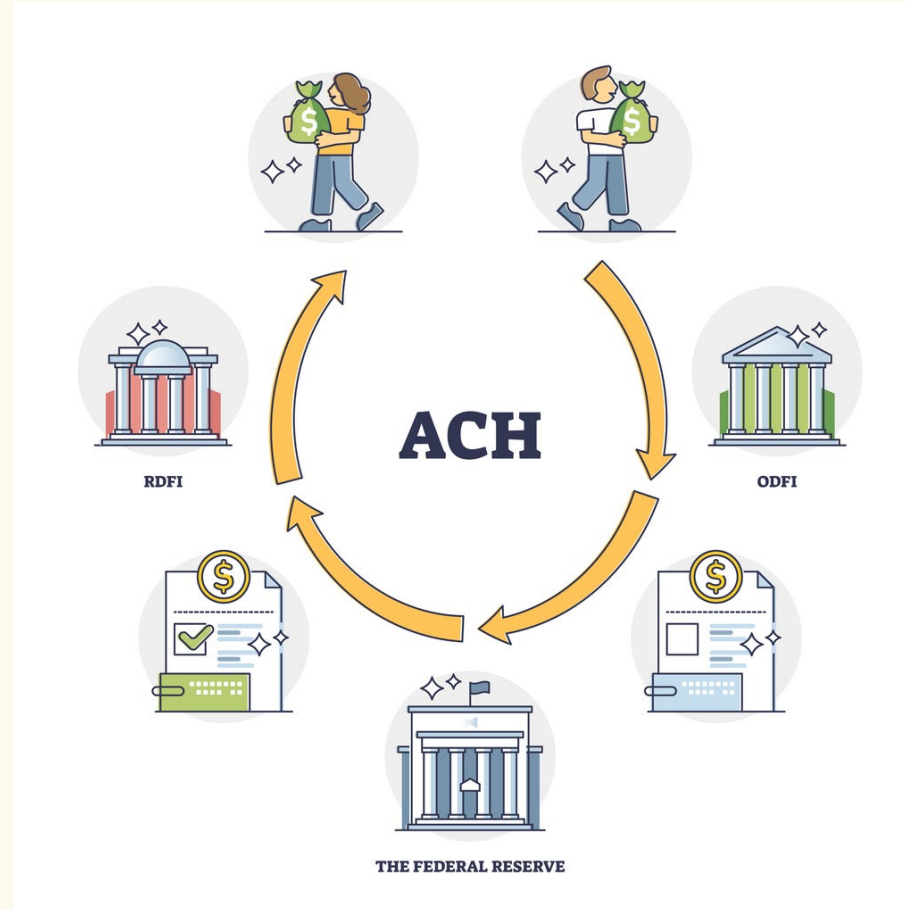
May 15<sup>th</sup>, 2024



Lillie

Resource Group

# ACH Common Findings



# Consumer Statement Requirements

Nacha Rules state consumer statements are required to contain specific language for standard entry classification codes (SEC Codes). Some CUs do not populate the required information on the statements.

Specific SEC Codes that need to show detailed information on the statements include:

- » ARC, BOC, POP
- » IAT
- » TEL
- » WEB DB & CR
- » PPD/CCD
- » RCK
- » POS



# Same Day ACH Posting Requirements

There are 3 windows for posting same day ACH credits.

Processing Window	ODFI Deadline	RDFI Receipt Time	Settlement	Credit Funds Availability Requirement
First Same Day ACH Window	10:30 a.m. ET	12 noon ET	1:00 p.m. ET	1:30 p.m. RDFI Local Time
Second Same Day ACH Window	2:45 p.m. ET	4:00 p.m. ET	5:00 p.m. ET	5:00 p.m. RDFI Local Time
Third Same Day ACH Window	4:45 p.m. ET	5:30 p.m. ET	6:00 p.m. ET	End Of Processing Day

Same day ACH debits must be posted by the end of the settlement date.

Non-same day credit entries have the following posting requirements:

- Entries received by 5pm local time the day before the settlement date must be made available to the receiver for withdrawal no later than 9am local time on the settlement date.
- Entries received after 5pm local time the day before the settlement date must be made available to the receiver for withdrawal no later than the end of the settlement date

# Return Reason Codes and Unauthorized Debits

Be sure the correct return reason codes are used for unauthorized debits.

Return Reason Code	Use
• R-05*	• Unauthorized Debit to a consumer account bearing Corp SEC Code
• R-07*	• Authorization Revoked
• R-10*	• Unauthorized
• R-11*	• Not in accordance with the authorization
• R-37*	• ARC and POP Source Document and ACH Post
• R-38	• ARC Stop Payment
• R-51*	• Unauthorized RCK
• R-52	• Stop Payment on RCK
• R-53*	• Check and ACH Paid

Some returned debits require a Written Statement of Unauthorized Debit (WSUD). These WSUDs must be retained for a period of 1 year from the settlement date of the extended return entry to which the form relates.

Be sure to retain WSUDs as required.

\*WSUDs with these codes must be signed and dated on or after the settlement date of the entry, obtained from the Receiver prior to initiating an adjustment, and must contain the required language (authorized signer or authority to act, and the information is true and correct). A copy must be given to the ODFI within 10 banking days.

# Notifications of Change (NOCs)

Notification of Change entries may be received by the ODFI when an entry that was originated has incorrect information and the RDFI is asking for it to be corrected.

Be sure the NOC reports are reviewed daily, and appropriate corrections are made.

\*This is the most common Nacha Rules violation in the Northeast.

# BSA Common Findings



# Risk Assessment Updates

A common misconception is that Risk Assessments need to be reviewed and updated only once a year.

Risk Assessments are “living documents” and should remain evergreen/dynamic and ready for updates whenever a change in the program, risk, products, geography, FOM, membership, etc. occurs.

## Things to include in Risk Assessments include:

- » Recent exam or independent testing findings
- » Lack of CDD for indirect memberships
- » AMLA-related national priorities
- » Staffing changes, including significant turnover, senior leadership changes, or newly appointed BSA/AML Officer or staff
- » 3<sup>rd</sup> party vendor risks
- » OFAC risks
- » Qualitative and quantitative information

# Beneficial Ownership Information

- Triggering events
  - Triggering events are often forgotten about. The BOI must be either recertified or collected again during triggering events, such as a new share, new loan, new signer. (This is not an exhaustive list.)
- Incomplete Information
  - Often, the significant controlling authority is not completed since it is the same information as the person opening the account and the BO.
  - Another issue is the lack of BO information when the business is a sole-member LLC. This is often confused with a sole-proprietorship.
- Incorrect information
  - It is not uncommon to see BOI listed in the ownership section when the business is either an unincorporated association or a business that does not qualify under the “ownership prong” of the certification (cub scouts, churches, non-profits, etc.).

# Monitoring Concerns

- CUs are responsible to review all types of activities for potentially suspicious transactions. This includes wire transfers, ACH transactions, fraud charge-offs, requests for information, subpoenas, and alerts from core reports or monitoring programs.
- If the CU uses an automated process for identifying suspicious transactions, be sure to conduct rule-tuning. If the CU operates manual review processes, be sure to utilize all the tools CU Answers provides. Leveraging the available tools will help reduce the burden of missing suspicious activity.
- Fully document the review of alerts. Use clear, concise language to indicate what was observed and what determinations were made.
- Don't forget MSBs, CRBs, and CVCs. Just because a CU may decide not to service these businesses, doesn't mean they don't sneak through. If the CU unknowingly services these types of businesses, significant regulatory consequences may be imposed.

# Member Due Diligence (CDD)

- Ensure that CDD collection is sufficient. Do you ask for PEP status, citizenship, expected activity, etc.?
- CDD often gets collected and forgotten about. When the member's activity becomes concerning, look at the CDD collected. If the information doesn't match what the member stated, this is a great time to collect updated CDD and chat with the member. Don't be afraid to go back to the CDD information during review of member activity.
- If the member is disgruntled with answering questions, this should be considered a red flag. This may be a time to consider if the CU wants to continue the relationship with the member. This may also be a great time to consider if a SAR is appropriate, when the totality of the circumstances is considered.
- Don't be afraid to verify the information and conduct research. CDD should segue into Enhanced Due Diligence (EDD) for high-risk members. Utilize open-source intelligence (OSINT) tools such as Google, LinkedIn, social media, court records, news sources, etc. to gain an understanding of these members. If needed, consider utilizing subscription intelligence services, such as Accurint, Clear, etc. to cast a wider net for information gathering.



# Bank Secrecy Act Considerations



# Corporate Transparency Act

Congress passed the CTA on January 1, 2021. With the CTA came a new section to the Bank Secrecy Act (31 U.S.C. 5336) that requires small businesses, including corporations, limited liability companies, limited liability partnerships, business trusts, and most limited partnerships, in the United States (called reporting companies) to report information about their beneficial owners to a central database that will be implemented by FinCEN (Financial Crimes Enforcement Network).

The Access Rule only permits FIs to request BOI from FinCEN for purposes of complying with CDD requirements under applicable law and only with the consent of the reporting company to which the BOI pertains. The FI is responsible for obtaining a reporting company's documented consent. In preparation for access to BOI from the national database, we recommend that the Credit Union start thinking about (and drafting) procedure and policy requirements and updates. It will be imperative that you continue to refer to FinCEN's BOI FAQ page.

# CTA Questions to Consider:

- How will you safeguard information you receive from the BOI?
- How will you collect and retain consent from your customer / member? Will new or revised account agreements need to be developed?
- How will handle an account whose owner has not registered in the BOI system? Will you require proof of registration?
- Who will have access to the database?
- In what circumstances will you access the database?
- Be sure to include the use of the database in your risk assessment. There are penalties for misuse of the database.

# CTA Resource

- [https://www.fincen.gov/sites/default/files/shared/BOI\\_Informational\\_Brochure\\_508C.pdf](https://www.fincen.gov/sites/default/files/shared/BOI_Informational_Brochure_508C.pdf)

# USA Patriot Act – Section 311

Section 311 of the USA PATRIOT Act added 31 USC 5318A to the BSA, which authorizes the Secretary of the Treasury to require domestic financial institutions and domestic financial agencies to take certain special measures against ***certain foreign jurisdictions, foreign financial institutions, classes of international transactions, or types of accounts that are of primary money laundering concern.***

These special measures are not against ALL foreign jurisdictions, institutions, classes of transactions, or types of accounts. Nor do they remain the same. The Secretary of the Treasury periodically amends or rescinds the orders.

## Regulation 311 and Special Measures

# 311 Special Measures

1

**Recordkeeping and Reporting** of Certain Financial Transactions

2

Information Relating to **Beneficial Ownership**

3

Information Relating to Certain **Payable-Through Accounts**

4

Information Relating to Certain **Correspondent Accounts**

5

**Prohibitions or Conditions** on Opening or Maintaining Certain Correspondent or Payable-Through Accounts

# Accounts Affected

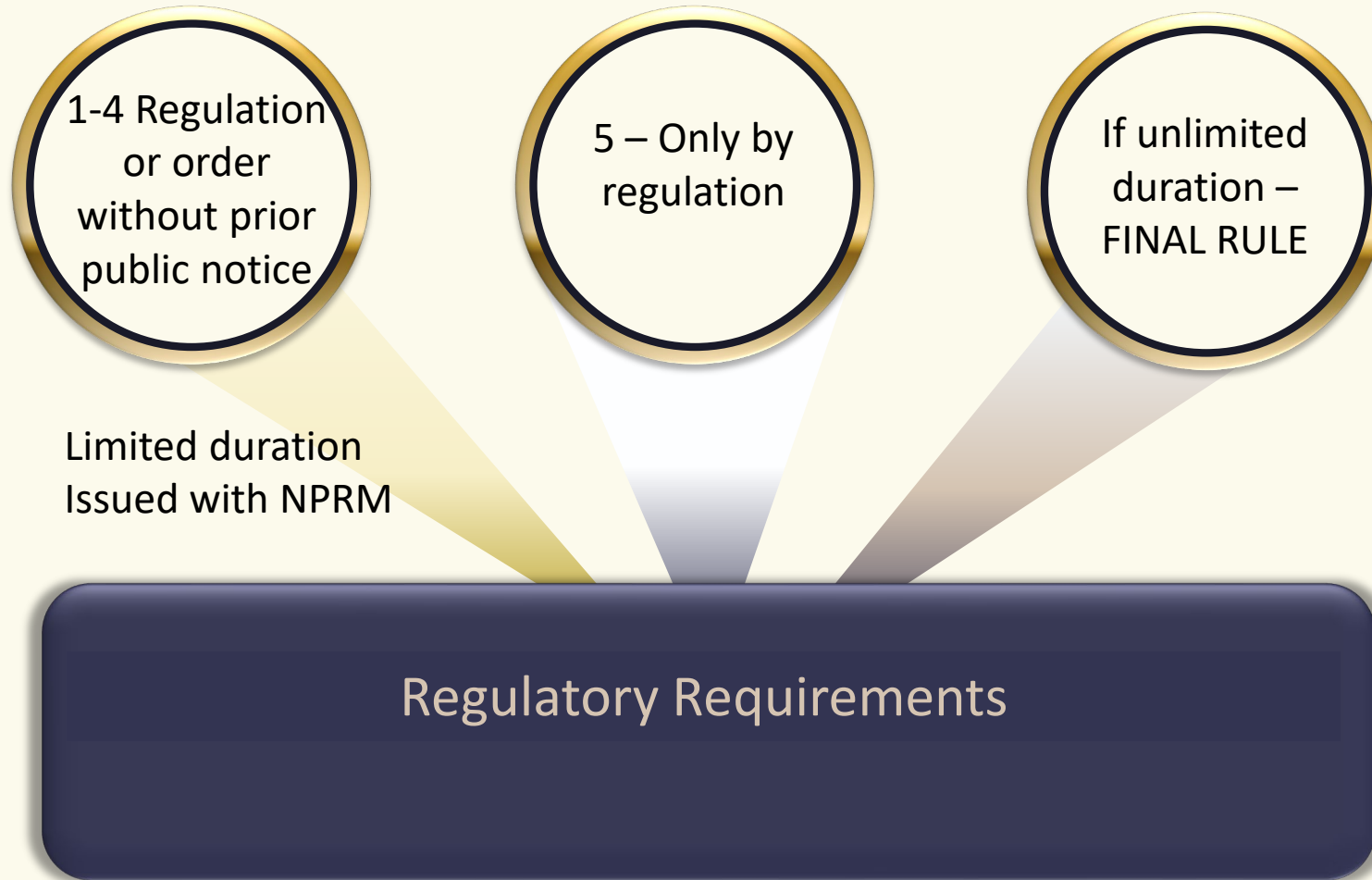
## Payable through Account

- A payable-through account (PTA) is a demand deposit account through which banking agencies located in the United States extend privileges to the customers of other institutions, **often foreign banks**.
- PTA accounts are a concern to bank regulators because the banks or agencies providing the accounts may not be subject to the end customers to the same level of scrutiny as they would their own customers.

## Correspondent Account

- A correspondent account is an account established by a financial institution to receive deposits from, make payments on behalf of, or handle other financial transactions for another financial institution. Correspondent accounts are established through bilateral agreements between the two banks.
- Most commonly accounts of **foreign banks** that require the ability to pay and receive the domestic currency.

# How Imposed





# Take-Aways



**Between Banks / FIs**

**Specific Accounts**

**Almost certainly foreign**

# 311 Resources

- [Special Measures Narrative and Exam Pro.pdf](#) (ffiec.gov)
- <https://bsaaml.ffiec.gov/manual/AssessingComplianceWithBSARegulatoryRequirements/15>

# AML Systems

**Your Question: Are there any BSL/AML system weaknesses identified?**

- Customer Due Diligence Flows / Core vs. Manual
- Staff Risks:
  - Not understanding configurations and what transactions alert
  - Not having proper governance
  - Not having time to properly research alerts
  - Not understanding importance of, and risk of, tuning
  - Lack of ongoing training on the system
- Examiners and auditors not understanding the systems and inadvertently creating more confusion for the institution
- Not considering risk / threat in their risk assessment

# What Else?



## Contact Information:

- [www.lrg.com](http://www.lrg.com)
- Keri Lillie,  
[klillie@lillierg.com](mailto:klillie@lillierg.com)
- Heather Williams,  
[hwilliams@lillierg.com](mailto:hwilliams@lillierg.com)

TIME FOR LUNCH!

# AuditLink

CU\*ANSWERS Management Services



# OPEN BANKING DODD FRANK 1033 CONSUMERS RIGHTS TO ACCESS INFORMATION

Jim Vilker, NCCO, CAMS  
AuditLink VP of Profession Services CU\*Answers

## **AuditLink**



# WHAT IS THIS

*IN 35 YEARS OF REVIEWING PROPOSED REGULATIONS THIS IS THE WORST THOUGHT OUT REGULATION I HAVE EVER SEEN*

(a) IN GENERAL.—Subject to rules prescribed by the Bureau, a covered person shall make available to a consumer, upon request, information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person, including information relating to any transaction, series of transactions, or to the account including costs, charges and usage data. The information shall be made available in an electronic form usable by consumers.

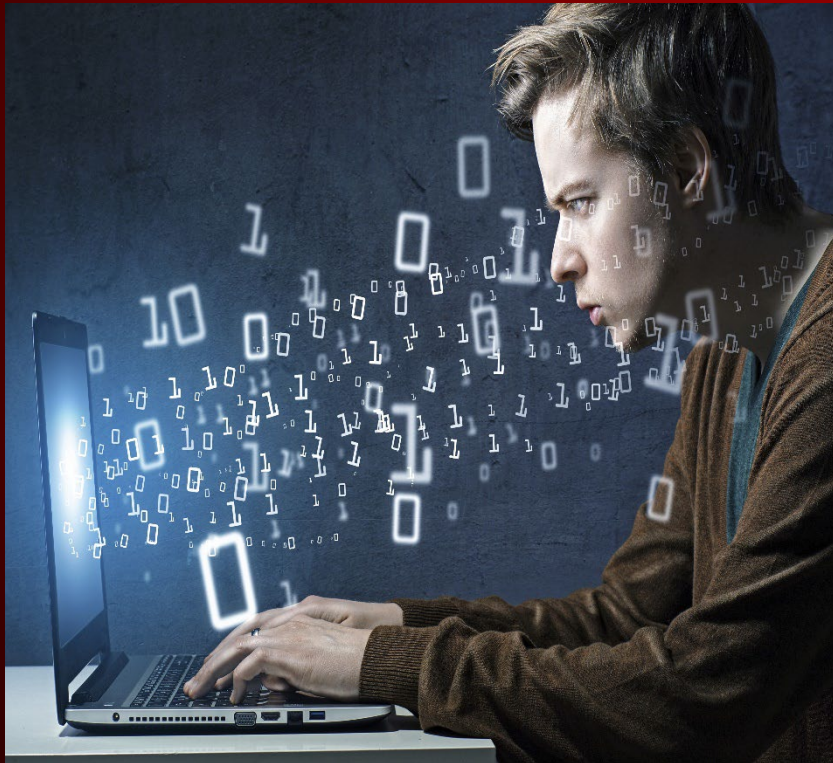
# TIMELINES FOR ADOPTION FROM DATE OF PUBLICATION

- 6 months for F/I's greater than \$500 billion
- 1 year for F/I's \$50 to \$500 billion
- 2.5 years for F/I's \$850 million to \$50 billion
- 4 years for all others

# WHAT INFORMATON

- Transactions or series of transactions for last 24 months including pending transactions, merchant name, rewards credits, fees and finance charges
- Account balance
- Information to initiate payment to or from a Reg E account (ACH)
- Terms and conditions including fee schedule, APR and APY, rewards program terms, has the consumer opted into overdraft coverage, has the consumer entered into an arbitration agreement

# WHAT INFORMATION



- Upcoming scheduled bill payment information and any upcoming payments due your member
- Basic account verification information
  - How many vendors are involved here
  - What if this information is buried in an account agreement
  - What is the purpose of this data
  - Standards for data were not prescribed and CFPB is requiring the industry to establish those

# RESPONDING TO REQUESTS



- Machine readable files
- Fees prohibited
- MFA or consumer credentials cannot be used for the developer interface
- Available in a industry standard format or widely used by other developer interfaces
- Meet performance standards. 99.5% response rate that must be tracked and made publicly available annually. Responses must be made in less than 3,500 milliseconds.



# HERE'S THE RUB

- CFPB was required to consult with prudential regulators..... No mention of that discussion in the commentary
  - Credit unions will need to expand their vendor management program to complete due diligence on all FinTech's prior to them accessing member data
  - Did not take into consideration that 1,631 credit unions are under \$25 in assets and have an average staff of 3 people
  - CFPB mentioned creating an accreditation process but this was not found in the proposal

# AN MORE BURDENS

- Creating portals for the consumer and developers
  - No fees can be charge
  - Small business entity (SER) group estimated that costs could be as high as \$500,000 and the CFPB grossly underestimated the cost
    - 1,451 credit unions made less than \$50,000 in 2023
  - SER stated this could cause the closure or rural community banks that could not absorb the costs
  - CFPB spoke to “A” developer's portal
    - Credit unions are required to vet the third party and limit the data they can have based upon needs and security. Each FinTech will have a custom portal.

# DEVELOPERS DILEMMA

- Proposal requires developers to use a qualified industry standard
  - Recognized that one does not exist
  - Asking the industry to develop one
  - Is not in line with the Dodd Frank ACT
  - Lack of standards will have developers potentially having to recreate portals if deemed not to meet industry standards

*(d) STANDARDIZED FORMATS FOR DATA:* The Bureau, by rule, shall prescribe standards applicable to covered persons to promote the development and use of standardized formats for information, including through the use of machine readable files, to be made available to consumers under this section.

Currently this was pointed out in comments from CU\*Answers and may be the one item taking them back to the drawing board.



NOT TO  
MENTION  
SECURITY.... OR  
LACK THERE OF

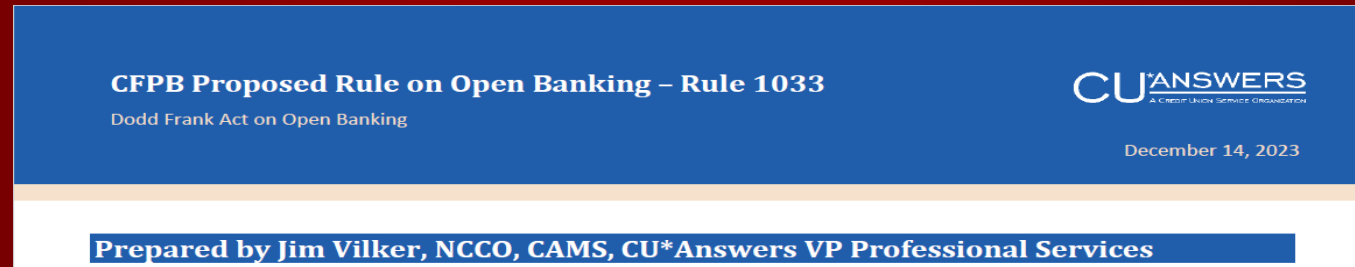


- Third party access without the use of MFA or credentials will
  - SER's stated
    - It will increase liability and fraud losses
    - Stated insurance costs will go up
    - Create increase reputational risks
    - Unclear which party would be liable in the event of a breach
  - CFPB has stated they can fine institutions for UDAAP relating to securing non-public information while creating a target risk environment for bad actors in open banking
  - Proposals mention GLBA Safeguard framework which states institutions should implement MFA for accessing non-public information
  - Did not take into consideration guidance by the NCUA, OCC, or FDIC

So who did they consult with????? Definitely not regulatory bodies or their own SER (required by Dodd Frank)

# LET'S SEE THE COMMENTARY FROM CU\*ANSWERS

Please share this with your Executive Team, Board Members, and Congressmen.



<https://www.regulations.gov/comment/CFPB-2023-0052-0622>

And read a synopsis in CUSO Mag



<https://cusomag.com/2024/02/07/cfpb-and-open-banking-searching-for-a-solution-while-creating-new-problems/>

**AuditLink**

CU\*ANSWERS Management Services

# CU\*BASE Releases That Matter to You

RECENT AUDIT AND COMPLIANCE RELEASES

Brought to you by **AuditLink**

# Speakers



AJ Schalk, AVP-  
AuditLink



# Releases We Will Discuss

CU\*BASE Release 23.05  
May, 2022

CU\*BASE Release 23.10  
October, 2022

CU\*BASE Release 24.05  
May, 2023



# CU\*BASE Release

## 23.05

MAY-2023

# Release 23.05 May-2023

## Enhancements to Wire Transfer Tracking

- Wire Transfer Tracking (Tool #981) has been updated to sort the most recent wires first. And like so many dashboards, the columns are now sortable.

Posted to Member						
Done	Date	Time	Account	Name	Amount	In/Out
1	Apr 28, 2023	10:36:09	53854-000	STABLER, ELLIOTT J	100.00	I
1	Feb 21, 2023	13:42:42	53641-000	MILNE, CHRISTOPHER R	100.00	I
1	Feb 16, 2023	14:43:14	53644-000	BOXER, TRINIDAD	500.00	I
1	Dec 05, 2022	11:53:58	11020-000	MOUSE, MICKEY	750.00	I
1	Nov 09, 2022	16:55:05	53365-012	AMITAF, FATIMA	200.00	I
1	Nov 09, 2022	14:02:46	53365-000	AMITAF, FATIMA	300.00	I
1	Aug 12, 2022	15:18:54	1234-000	MEMBER, MARY A	2,000.00	I
1	Aug 12, 2022	15:16:12	1234-000	MEMBER, MARY A	2,000.00	O
1	Jul 11, 2022	11:25:52	987258-012	MINION, BOB B	1,000.00	I
1	Jul 11, 2022	11:13:01	86456-000	RATIO, CHUCK L	10,000.00	I
1	Jul 11, 2022	11:03:36	9291-013	MINAJ, NIKKI	10,000.00	I
1	Jul 11, 2022	11:01:59	9291-012	MINAJ, NIKKI	9,999.00	I
1	Jul 11, 2022	10:59:46	9291-000	MINAJ, NIKKI	1,000.00	I
1	Jun 24, 2022	10:09:45	789456-000	SMITH, AMBER C	100.00	I
1	Jun 23, 2022	16:14:24	52703-010	BLOW, JOE E	450.00	I

Change

Delete

View

Member Inquiry

↑↓



# Release 23.05- May 2023

## Tool #569- Online/Mobile/Text Banking VMS Configuration

- Allow maintenance of personal information by member (online)

New option added to allow Direct Update with two factor (text/email)

Will use phone numbers and email on file for member

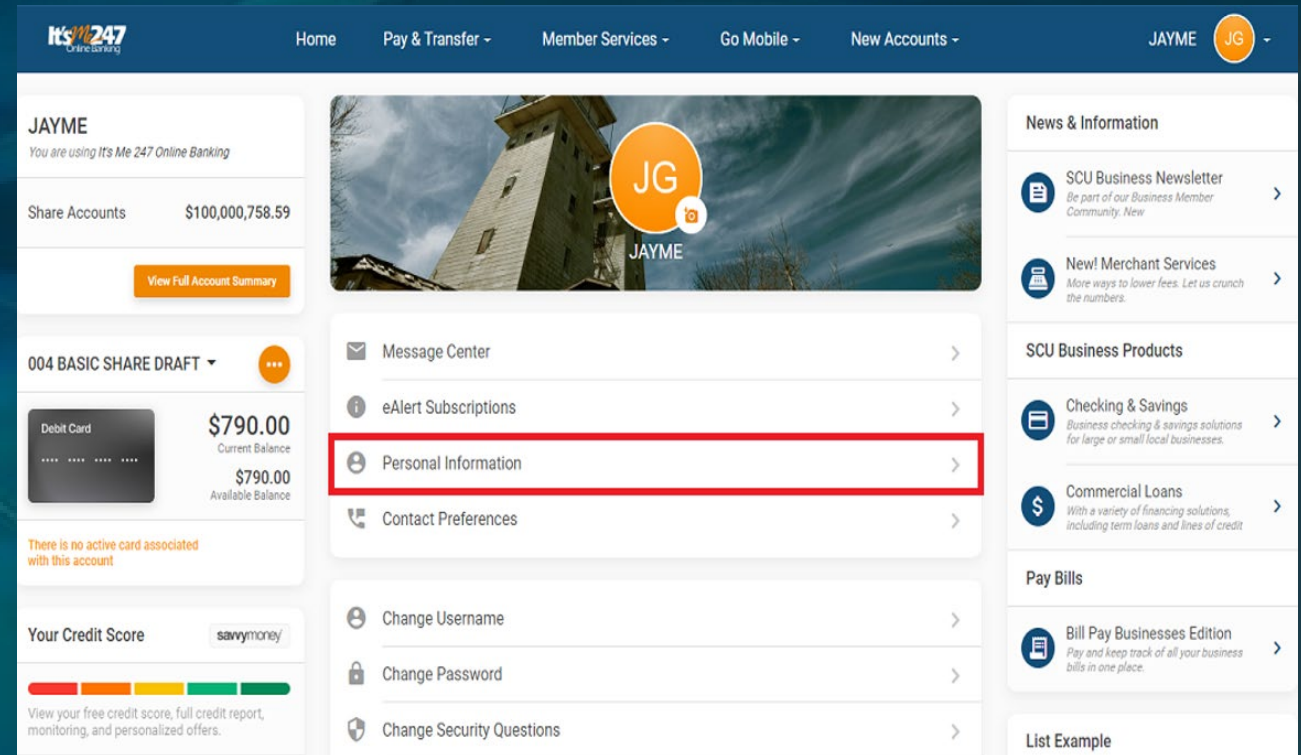
Member must use Two-Factor Authentication to access personal information page with Online Banking, not just update

The screenshot shows the 'Update Credit Union Online Banking Settings' window. The 'Corp ID' is 01. The 'Allow new membership application online' section is checked, with 'Apply membership application fee' also checked and 'Dividend application to be used' set to SH. The 'Activate savings rate board', 'Activate certificate rate board', and 'Activate loan rate board' are all checked, each with a 'Member Instructions' button. The 'Require co-applicant if marital status is Married' is unchecked. The 'Allow maint of personal info by member (online)' section has three radio buttons: 'Direct update (no approval)', 'Reviewed update (approval required)', and 'Direct update with two factor (text/email)'. The third option is selected and highlighted with a red rectangle. The 'Allow member to enter account nicknames' is checked. The 'Default setting when setting up transfer control list' has 'All sub-accounts' selected. The 'Allow member to change Reg E Opt In/Out choice' is unchecked, with a 'Member Instructions' button. The 'Show who was served (either a jump guest or via Teller Currently Serving) in transaction history' is checked. At the bottom, there are 'Update' and 'Instructions' buttons, and a navigation bar with icons for back, forward, up, down, print, link, info, help, and search.

# Release 23.05- May 2023

## Two-Factor Authentication Module from a member's perspective

- When Navigating to access personal information from the profile menu the member will be presented with a Two-Factor Authentication module
- If you use First-Time User activation this process works the same.



# Release 23.05- May 2023

## Two-Factor Authentication Module from a member's perspective

- Once selecting Personal Information, the member will be presented with the new Two-Factor Authentication module to gain access
- The member must select either a phone number that has text availability or an email to receive the one-time access code

### Let's Verify Your Identity

Since protecting your information is our top priority, we need to verify it's you in order to access & update your personal information. Select a contact method to receive a one-time verification code to continue.

- ☐ Text Code to (\*\*\*) \*\*\*-0742
- ☐ Text Code to (\*\*\*) \*\*\*-1877
- ☐ Text Code to (\*\*\*) \*\*\*-7693
- ☐ Email Code to jas\*\*\*\*\*u@cuanswers.com

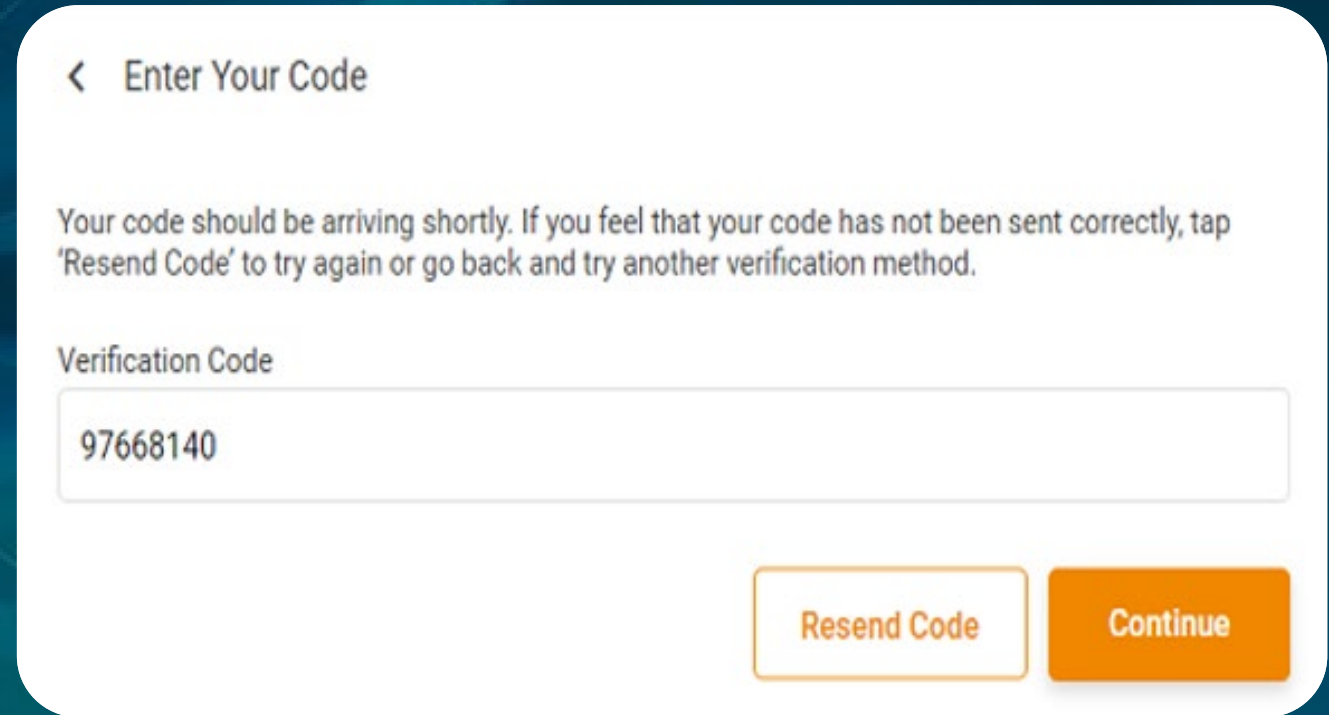
Send Code

Send Code

# Release 23.05- May 2023

## Two-Factor Authentication Module from a member's perspective

- A code will be sent to the member via the channel they selected (text/email)
- Once the member receives the code, they must then enter it within the module and continue into the Personal Information module



The screenshot shows a mobile app interface for two-factor authentication. At the top, there is a back arrow and the title 'Enter Your Code'. Below this, a message states: 'Your code should be arriving shortly. If you feel that your code has not been sent correctly, tap 'Resend Code' to try again or go back and try another verification method.' Underneath the message is a label 'Verification Code' followed by a text input field containing the code '97668140'. At the bottom right, there are two buttons: 'Resend Code' with an orange border and 'Continue' with a solid orange background.

< Enter Your Code

Your code should be arriving shortly. If you feel that your code has not been sent correctly, tap 'Resend Code' to try again or go back and try another verification method.

Verification Code

97668140

Resend Code Continue



# Release 23.05- May 2023

## Two-Factor Authentication Module from a member's perspective

- Once successfully completed Two-Factor Authentication process, the member will then have access to their personal information.
- The member now can view and edit their Personal Information. This update will be the same as a **Direct Update**. No review option is available.

### Personal Information

This is your primary membership address. If you receive mail from the credit union at another mailing address, please contact the credit union to update that address, if necessary.

#### Address

6000 28TH ST SE  
GRAND RAPIDS, MI 49546

#### Email

jason.lareau@cuanswers.com

#### Phone Number

HOME  
(555) 339-0742

MOBILE  
(555) 351-1877

WORK  
(555) 332-7693

Your Code Word ?

Edit Personal Information

Edit Personal Information

# CU\*BASE Release

## 23.10

OCTOBER-2023

# Release 23.10- October 2023

## Multi-Factor Authentication for P2P

### Tool #569- Online/Mobile/Text Banking VMS Configuration

- For integrated P2P solutions
- Prompts members to enter a confirmation code via text or email
- Applies when accessing to enroll or send a P2P, grants access until they log off online banking

**Update Credit Union Online Banking Settings**

Corp ID 01

☐ Allow new membership application online  
☐ Apply membership application fee  
Dividend application to be used ☐

☒ Activate savings rate board  
☒ Activate certificate rate board  
☒ Activate loan rate board  
☒ Require co-applicant if marital status is Married

Allow maint of personal info by member (online) ☒ Direct update (no approval) ☐ Reviewed update (approval required) ☐ No  
☐ Direct update with two factor (text/email)

☒ Allow member to enter account nicknames

Default setting when setting up transfer control list ☒ All sub-accounts ☐ Owned sub-accounts only ☐ Specify

☒ Allow member to change Reg E Opt In/Out choice  
☒ Show who was served (either a jump quest or via Teller Currently Serving) in transaction history  
☐ Apply two factor authentication to P2P

**Member Instructions**  
**Member Instructions**  
**Member Instructions**  
**Member Instructions**

**Update**  
**Instructions**

# Multi-Factor Authentication In Future Releases

Watch for more use of this feature coming in future releases. Next on the docket is optional multi-factor authentication for logging into home banking and password resets.

To find out more visit our kitchen page.

[Authentication Enhancements for Online/Mobile Banking | CU\\*Answers \(cuanswers.com\)](#)





# Release 23.10-October 2023



## BSA Watch Analysis Dashboard Update (Tool #984)

### Member Tracker Entry

Account # 10829-000 DON J HULIO

Memo type   Bank Sec Verifi

Speaking to  Conversations 51

[Save/Continue](#) Page Up/Down  

[Phone Inquiry](#)[Save/Continue](#)[Contact](#)[Previous](#)[Filter](#)[First](#)[Last](#)[Next](#)[Household](#)[Additional Signers](#)[Conversations](#)[Print Notice](#)

Date

Time

Memo type

Created by

Need group



Task


Assigned

Contact

Follow up

Complete

Shift + Page Up/Down  

 Conversations are ordered newest (First) to oldest (Last).

# Release 23.10-October 2023

## Search Fraud Incident Maintenance Dashboard (Tool #1715)

**Fraud Incident Maintenance**UPDATE

Jump to account

Fraud type

Fraud status

# Fraud Incidents 14

Account #	SSN/TIN	Fraud Description	Type	Status	Change Date	Chg By
1234	013-45-6780	MEMBER DISPUTED CHARGES	DEBIT CARD FRAU	RESOLVED WITH LOSS	11/10/22	/0
	192-83-7665	SUBMITTED FRAUDULENT LOAN APPL	LOAN FRAUD	RESOLVED NO LOSS	09/14/22	/0
123456789	123-45-6789	MEMBER SERVED AS A MONEY MULE	UNEEMPLOYMENT SC	RESOLVED NO LOSS	11/12/20	/0
15857	543-21-9857	MEMBER SERVED AS MONEY MULE IN	UNEEMPLOYMENT SC	RESOLVED NO LOSS	08/26/20	/0
123456789	123-45-6789	MEMBER SERVED AS MONEY MULE IN	UNEEMPLOYMENT FR	RESOLVED WITH LOSS	05/28/20	/0
22649	123-45-0673	TESTR	FRAUDULENT CHEC	RESOLVED NO LOSS	12/06/19	.K
6399	12-3076454	PURCHASES USING REPLACEMENT C	CREDIT CARD FRA	RESOLVED WITH LOSS	07/30/19	/0
444445	333-33-8888	LOGIN VIA ONLINE BNK ATTEMPT T	ACCOUNT TAKE OV	RESOLVED NO LOSS	07/30/19	/0
40410	095-32-1672	STRAW BUYER IN FLIPPING SCAM	REVERSE MORTGAG	IN LEGAL PROCEEDINGS	07/30/19	/0
10924	000-11-1212	LOC PROCEEDS WIRED TO PERP FOR	ADVANCE FEE SCH	RESOLVED WITH LOSS	07/30/19	/0

- Added ability to easily search by Fraud Type, Fraud Status, as well as jump to a specific account number.

# CU\*BASE Release 24.05

MAY-2024

# Release 24.05-May 2024

## Credit Card Overpayment Limit

- New feature allows your credit union to define the maximum percentage a member can overpay their credit card.
- Limits are set at the loan category level in Tool #458, applicable only to credit card loans.
- If a member initiates a transfer to their credit card that surpasses configured limit the payment will fail to post.
- Helpful in preventing fraud due to excessive overpayments above CU's approved disbursement limits.

[24-24-05-Release-Summary.pdf \(cuanswers.com\)](#)

# **Release 24.05-May 2024**

## **New Online Banking Login Dashboard**

- Tool #1044 OLD Logins by Account Base/IP Address
- Help your staff review member logins to online banking
- Contains login date, start time, IP address, and session ID.
- Prevents having to query AUDICC table.
- Useful for fraud research

# Previous Releases Recap

- Updates to Wire Transfer Tracking Tool
- Multi Factor Authentication for Personal Information and P2P
- Enhancements to Tool #984 BSA Dashboard
- Upgrades to Search Fraud Incident Maintenance Tool
- Credit Card Overpayment Limit
- New Online Banking Login Dashboard

[23-23-05-Release-Summary.pdf \(cuanswers.com\)](#)

[23-23.10-Release-Summary-.pdf \(cuanswers.com\)](#)

# Practical Use of Enhanced Due Diligence Features

BEST PRACTICES

# Due Diligence Codes

## *Examples of Due Diligence Codes*

DD Code	Description
0	DUE DILIGENCE CODE 0
1	MED RISK
2	LOW RISK
3	HIGH RISK
4	OCCUPATIONAL
5	RESIDENT NON-ALIEN
6	NEW ONLINE MEMBERSHIP
7	DUE DILIGENCE CODE 7
8	DUE DILIGENCE CODE 8
9	DUE DILIGENCE CODE 9

Update



## Why High, Medium, and Low?

- Allows you to monitor accounts at separate intervals
- Saves the credit union staff valuable time while staying compliant
- Creates the ability for members to rehabilitate their status

## Tool #402

Gives you the ability to efficiently pull reports on high-risk accounts

### Print Special Account Audit Report

Generate report for ☒ Insider/Employees ☐ Members with due diligence flag

Employee type code  Optional

#### Reports to Print

☒ Teller audit key review

Include data from   To   [MMDDYYYY]

(Remember that data is retained for 90 days)

Audit keys  Optional

Flag transactions greater than or equal to  (whole \$) Optional

☒ Transaction activity review

Pull data from ☒ Current month ☐ Prior month range

Dates to include   To   [MMDDYYYY]

☒ File maintenance review

Pull data from ☒ Current month ☐ Prior month

Range of days in that month  to  (such as 03 to 10 for the 3rd through the 10th)

☒ Negative balance/Delinquent accounts review

(No date selections available; will be as of today)

☒ Account list only

(No date selections available; will be as of today)

# Under Utilized Tools

TOOLS YOU SHOULD ALL HAVE ACCESS TO

# Under Utilized or Unknown Tools You Should All Have Access To

- Tool 559 – OFAC scan history
- Tool 951 – View employee security
- Tool 159 – Critical field monitoring
- Tool 247 – Due diligence codes
- Tool 537 – Abnormal Activity Monitoring / Pattern Recognition
- Tool 402 – Insider audit/high risk accounts
- Tool 565 – Online Banking Stats

# Under Utilized or Unknown Tools You Should All Have Access To

- Tool 565 – Online banking stats
- Tool 546 – Overpaid credit cards
- Tool 664 – Print member trackers – OFAC overrides
- Tool 260 – Configure memo types
- Tool 1892 – View Fraud Alert/Block Persons List



Questions?

**AuditLink**

CU\*ANSWERS Management Services

Thank you for coming!