October 2025

Risk Management and Operational Strategy

AJ Schalk
AVP-AuditLink
CU*ANSWERS

AuditLink
CU*ANSWERS Management Services

SPEAKER

AJ Schalk began working at CU*Answers in 2021 as a Client Service Representative. In this role, AJ developed fundamental knowledge of the functionality of the CU*BASE software suite, as well as a growing passion for assisting clients. These skills quickly moved AJ to serve as an Account Executive on the Cards & Payments team, where he managed intricate projects for bill pay and debit card data conversions. Along with project management and ongoing specialized client support, AJ honed his skills to gain a greater understanding of the risk assessment necessary within the world of EFT. In 2023, AJ became a NAFCU Certified Compliance Officer (NCCO) and joined the AuditLink Team as AVP. As the leader of AuditLink, AJ manages business operations and utilizes his regulatory skill set to assist credit unions in alleviating the regulatory mandates that they face daily, as well as preparing credit unions for auditor visits and requests. As an effective and dynamic communicator, AJ prides himself in his ability to train credit unions on BSA and high-risk management with the CU*BASE software suite to ensure that credit unions understand the dept of the software and remain in compliance.

Legal Disclaimer

*The information contained in this document does not constitute legal advice. We make no claims, promises or guarantees about the accuracy, completeness, or adequacy of the information contained in this email. You should retain and rely on your own legal counsel, and nothing herein should be considered a substitute for the advice of competent legal counsel. These materials are intended, but not promised or guaranteed to be current, complete, or up-to-date and should in no way be taken as an indication of future results. All information is provided "as is", with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this information, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, merchantability and fitness for a particular purpose. In no event will CU*Answers, its related partnerships or corporations, or the partners, agents or employees thereof be liable to you or anyone else for any decision made or action taken in reliance on the information provided or for any consequential, special or similar damages, even if advised of the possibility of such damages.*

AGENDA

KEY ITEMS

Agenda

NCUA Letter to Credit Unions

NACHA Rules 2026

Fraud Monitoring

Internal Controls

NCUA Letter To Credit Unions 2024

NCUA Letter To Credit Unions

Who Remembers Junk Fees!?

NCUA published a letter to credit unions in December of 2024 titled “Consumer Harm Stemming from Certain Overdraft and Non-Sufficient Funds Fee Practices”

Executive Summary

- Include policies and procedures designed to manage consumer compliance and reputation risk.
- Mitigation strategies should include discontinuing policies related to charging overdraft, NSF, and other related fees that your members cannot reasonably anticipate and avoid.
- Analysis should identify and reimburse members who have been negatively impacted by any assessment of these fees.

NCUA’s Supervisory Approach

The NCUA does not expect credit unions to cease offering overdraft programs designed to assist their members in managing their cash flow needs. However, the NCUA will continue to review overdraft programs to ensure credit unions are effectively managing the heightened risk of certain fee practices and will expect credit unions to properly mitigate such risks, including by ceasing unanticipated fee practices.

If examiners identify violations of laws or regulations due to unanticipated fee practices, the NCUA will evaluate appropriate supervisory or enforcement actions, including restitution to harmed members.

The NCUA will also recognize your credit union’s proactive efforts to self-identify and correct violations. Examiners will generally not cite and the NCUA will generally not pursue enforcement action under the FTC Act nor the CFPA for violations that have been self-identified and fully corrected prior to the start of an examination. In addition, in determining the scope of any restitution, the NCUA will consider the likelihood of substantial consumer harm as well as a credit union’s risk-management processes to identify and correct violations.

The NCUA encourages credit unions to review their overdraft and NSF program practices to ensure compliance with Section 5 of the FTC Act, Sections 1031 and 1036 of the CFPA, and other applicable laws and regulations.

NCUA Letter To Credit Unions

What is Considered "Unanticipated"?

NCUA published a letter to credit unions in December of 2024 titled "Consumer Harm Stemming from Certain Overdraft and Non-Sufficient Funds Fee Practices"

Unanticipated Overdraft Fees

Unanticipated overdraft fees occur when a credit union assesses overdraft fees on transactions that a member would not reasonably expect would give rise to such fees. Though credit unions are required to provide disclosures related to their transaction processing and overdraft fee policies, these processes and policies can be complex. Research published by the Consumer Financial Protection Bureau suggests that, despite such disclosures, customers and members of depository institutions, including credit unions, face uncertainty about when transactions will be posted to their account and whether they will incur overdraft fees.

- Authorize Positive/ Settle Negative (APSN)
- Multiple NSF Representment Fees
- Transaction Ordering
- NSF/Overdraft Fees

Who remembers Junk Fees!?

Authorize Positive Settle Negative

- Major concern of regulatory agencies (as well as class action lawsuits).
- Debit card transactions that authorize when a member's account has a sufficient available balance to cover transaction but, due to one or more intervening transactions, has an insufficient balance to cover transaction at the time it settles.
- Members cannot reasonably anticipate when overdraft fees will be assessed.

Multiple ACH Representment Fees

- Consumers receiving fees for returned ACH transactions, as the consumer has no control when the ACH transaction is re-presented for payment.
- **Example:** John Member authorizes PayPal to debit their account $40. The member has insufficient funds and incurs a fee. Two hours later PayPal sends another request for the same authorization and the member receives a second fee.

Who remembers Junk Fees!?

Transaction Ordering

So-called “high-to-low” transaction processing order can result in more fees being addressed by a consumer.

Such practices result in higher costs to the member with no countervailing benefit and are likely unfair under both FTC Act and the CFPA.

Ensure you understand how transactions are posting through your CORE.

NSF/Overdraft Fees

Expectation is that you are not using fees in a “predatory way”.

Setting up guard rails to prove you are protecting your members to a reasonable degree. Such as having a minimum transaction amount to have a fee applied. **EXAMPLE**: Not charging a $30 fee for a $5 cup of coffee.

Consider a Risk Assessment

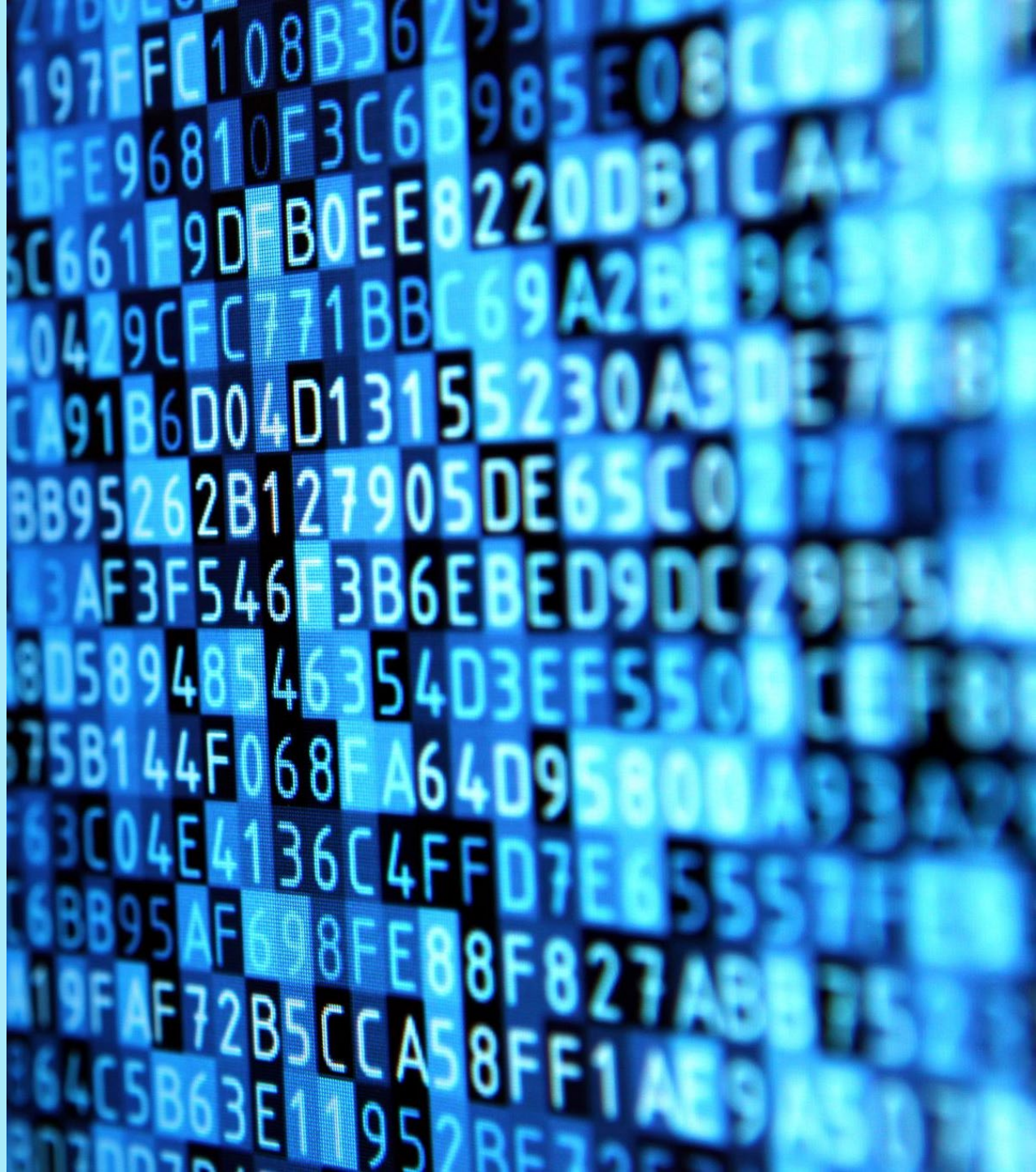
NCUA Letter To Credit Unions

Risk	Threat
Concentration/Liquidity Risk	Credit Union has overreliance on fee income
Reputation Risk	Credit Union is failing to manage consumer expectations
Strategic and Transaction Risk	Credit Union is failing to manage its overdraft and NSF program
Compliance and Legal Risk	Credit Union is not in compliance with laws and is not managing its membership disclosures.

NACHA Rules 2026

Risk Management Topics- (Fraud Monitoring Phase 1 &2)

- Eliminates use of “commercially reasonable” as a standard.
- Replaces “detection system” with “processes and procedures.”
- Provides a next level description of requirements – i.e., “reasonably intended to identify…”
- Provides that the requirements apply “to the extent relevant to the role the entity plays.”
- Allows an ODFI to expressly consider steps that other participants in origination are taking to monitor for fraud in designing its own processes and procedures.
- Clarifies that monitoring is not required pre-processing.
- Requires a review of processes and procedures “at least annually.”



Importance of Risk-Based Approach

In the Rule Amendment, Nacha sets forth a definition and some examples, but it still allows for a credit union's interpretation. Due to the lack of direction, there is no specific set of standards.

- A risk-based approach to fraud monitoring enables RDFIs to apply resources based on risk assessment for various types of transactions.
- A risk-based approach to fraud monitoring enables financial institutions, Originators, and other parties to apply resources based on a risk assessment for various types of transactions. A party might take extra measures to detect fraud in transactions in which it has determined risks to be elevated; take basic precautions where it has determined that risks are lower, and exempt transactions or activities that it determines involve very low risk.
- A risk-based approach should not be used, however, to conclude that no monitoring is necessary at all. At a minimum, an entity applying a risk-based approach should conduct a risk assessment to identify and differentiate higher-risk from lower-risk transactions.

Implementation Dates

Phase 1

Fraud Monitoring by Originators, TPSPs, and ODFIs

- **Effective Date:** March 20, 2026
- **Applies To:** All ODFIs, non-consumer originators, TPSPs, and TPSs with annual ACH origination volume of 6 million or greater in 2023.

RDFI ACH Credit Monitoring

- **Effective Date:** March 20, 2026
- **Applies To:** All RDFIs with annual ACH receipt volume of 10 million or greater in 2023

Phase 2

Fraud Monitoring by Originators, TPSPs, and ODFIs

- **Effective Date:** June 19, 2026
- **Applies To:** All other non-consumer originators, TPSP, and TPS.

RDFI ACH Credit Monitoring

- **Effective Date:** June 19, 2026
- **Applies To:** All other RDFIs.

Fraud Monitoring

With Decrease in Regulation, Fraud Is Still in Play

Fraud Monitoring

- New Memberships
- High Risk Accounts
- Social Engineering/Account Takeovers
- Elderly Exploitation

With Decrease in Regulation, Fraud Is Still in Play

Fraud Monitoring

New Memberships

- Are we allowing opening/funding of accounts online?
- How are we monitoring these new accounts? (Nature and purpose)
- Verifying identity
- How are we monitoring for abnormal activity?

High Risk Memberships

- How are we parsing out our levels of risk? High risk only? High, Med, Low?
- What tools to we have to flag these accounts in the CORE?
- What are our procedures for following up on these accounts?
- What tools are available to complete this enhanced due diligence?
- Can we limits services?

With Decrease in Regulation, Fraud Is Still in Play

Social Engineering/Account Takeovers

- Continuing to educate members on what type of information will not be requested via text/phone call
- Reviewing account activity to look for cash being brought in followed by wires or ACH to purchase crypto currency
- Asking questions or verifying identity before making transfers via phone call.
- Reviewing file maintenance and home banking logins
- When in doubt contact your financial institution

Elderly Exploitation

- When reviewing cash logs always paying attention to age
- Ensuring tools are available to review activity outside of cash for elderly members
- Paying attention to who is conducting activity on the membership via teller line. Is this a J/O?
- Appearance and emotional state of member

Internal Controls

Recent News Headlines

Source:https://www.cutimes.com/fraud-enforcement/

August 22, 2025

Former Massachusetts Loan Officer Faces Sentencing for $900,000 HELOC Fraud

Brian Socha uses coworkers' computers to increase credit limits and lower interest rates on his loan.

August 06, 2025

Former Indiana Credit Union Branch Manager Accused of Stealing More Than $350K

Teresa Palmer exploited elderly members who were unable to regularly monitor their accounts, federal prosecutors allege.

August 08, 2025

Former Indiana Credit Union CEO to Be Sentenced in $300K Fraud Case

Daniel Johnson admits to submitting fake loan applications and misusing funds to buy a house and pay debts.

What Do These Have In Common?

- Employee was in a trusted position
- Segregation of duties and dual control was not considered
- In some cases, file maintenance not being reviewed
- Financial statement configs and G/L suspense not tested or reviewed
- Employee account reviews not being completed
- Lifestyle was not taken into consideration
- Reconciliation of corporate account not being completed or tested

Basic Internal Controls

Financial Statements

- **Second set of books**
  - Evaluate Financial statement configs and verify against member trial balance with supporting documentation
- **Hidden Accounts**
  - Review reconciliation of trial balance to control accounts by someone not responsible for daily reconciliation on surprise basis
- **Undetected usage of G/L Accounts**
  - Review if G/L accounts have been suspended from printing on financial statements if they have zero balance

Cash

- Review G/L postings to all cash related accounts prior to and after the surprise cash counts
- Verify entries to cash in transit and received
- Do not develop a routine for cash counts
- Teller reversals

Dormancy

- Review activity on dormant accounts. Consider age and type of activity before activating the membership
- Create segregation of duty around who conducts the transaction and who is responsible for reviewing activity

File Maintenance

The Key To Most Events

- What are the credit union procedures for reviewing file maintenance? Daily, Weekly, Monthly?
- File maintenance review may be critical after uncovering a separate loose thread
- Sifting through what the system did vs employees
- Evaluating critical fields
- Understanding what to do based on findings
- Documenting review

Basic Internal Controls

Insider Account Reviews

- Are we keeping track of insider accounts?
- How do we flag them?
- What are we monitoring?
  - Teller activity
  - Status of account
  - File Maintenance
  - System access

Segregation of Duty

- How is system access audited and maintained?
- Are we creating job duties where only required access is granted?
- Thinking logically about what access in combination could be high risk (example teller line access and reactivating dormant memberships)
- We are small segregation of duties is difficult… what do we do?
  - Invest in training your supervisory committee
  - Invest in internal training, perception of detection and who is looking at what
  - Utilize system controls

Thank You For Your Time!
Questions?