# REGCORNER

October 21st, 2025 | Volume 1 | Issue 20

For MCUL Compliance, Advocacy and other news, check out the **MILeague Minute**!

## Hello & Headlines! Start Here, Stay Informed

**Hi Compliance Comrades,**

The regulatory radar is lighting up this week—and we've got plenty to track. From comment calls that could reshape supervisory standards to fresh guidance on suspicious activity reporting, the compliance conversation is moving fast.

The **CFPB's proposed rule on Supervisory Designation Standards** is open for comment until **October 26**. This rule could impact how entities are designated for supervision and what legal standards apply—so if your credit union is watching supervisory thresholds, now's the time to weigh in.

Also worth noting: **FinCEN released updated SAR FAQs** earlier this month, offering clarity on structuring, continuing activity, and documentation expectations. It's a welcome move toward streamlining reporting and reducing unnecessary burdens.

And for those navigating **CDFI certification**, the final reapplication window is now open through **December 31**. With federal staffing shifts and funding questions in play, many credit unions are watching closely to ensure continued access to capital and community investment tools.

As always, we're here to help you cut through the noise and focus on what matters most for your credit union. So grab your coffee, settle in, and let's dive into this week's headlines, comment calls, and compliance events.

—JaMille

## The Fine Print Files: What's New in Reg Land

***Some headlines you might have missed:***

***America's Credit Unions***:

- Stablecoin framework should support credit union involvement (Click to Read)
- This week: Shutdown enters week four (Click to Read)
- FinCEN Issues Frequently Asked Questions to Clarify SAR Requirements (Click to Read)
- What's Going on With the CFPB? (Click to Read)

***Credit Union Times***:

- Credit Union Leaders Urge Treasury to Reinstate CDFI Fund Staff (Click to Read)
- Senate NDAA Deal Delivers Major Wins for Credit Unions (Click to Read)
- Scott Simpson's New Chapter (Click to Read)

## "What's Happening in Compliance (Besides Everything): Compliance Events

**MCUL Compliance Office Hours**

Formerly SAS Compliance Office Hours, the group has been expanded to all credit unions in MI, regardless of size. Join us each month where we'll discuss recent compliance and regulatory updates, work through your compliance challenges, and have the opportunity to share resources, insights and other information with peers. We will also be looking for opportunities to include some elements from Cheers! to Compliance. You definitely don't want to miss these calls!

**When:** 1st Friday of every month, unless otherwise noted
**Time:** 9:00 am

Join us for the next session, scheduled for **Friday, November 7th.**

REGISTER HERE

**2026 Compliance Office Hours:** REGISTER HERE

## Ctrl+Alt+Deceit: Fraud in the Digital Age

*Fraud may be the bane of our regulatory existence, but let's be honest—it keeps our inboxes full and our careers thriving. Below are some industry fraud trends and sources with more information.*

### Emerging Fraud Trends for Credit Unions (Late 2025)

**1. AI-Driven Social Engineering & Deepfakes**
Fraudsters are using **AI-generated voice and video deepfakes** to impersonate executives or trusted staff, tricking employees into authorizing wire transfers or sharing sensitive data. These attacks are highly convincing and often bypass traditional verification methods. Read Me!

**2. Interactive Teller Machine (ITM) & ATM Jackpotting**
Credit unions are reporting **jackpotting attacks**, where malware forces ATMs to dispense all cash in the canisters. ITMs are also being targeted outside business hours using counterfeit debit cards. One CU had **7 of 10 ITMs emptied in hours**. Read Me!

**3. AI-Generated Check Fraud**
Check fraud is resurging with a tech twist: criminals use **AI tools to create realistic counterfeit checks** that mimic handwriting and security features. Remote deposit capture is a key vulnerability, and stolen check images are sold on the dark web. Read Me!

**4. SIM-Swap & eSIM Fraud**
Fraudsters hijack mobile numbers by swapping SIMs or transferring eSIM profiles, gaining access to **multi-factor authentication codes,** and locking members out of their digital lives. Once inside, they drain accounts and compromise fintech and brokerage platforms. Read Me!

**5. Loan & Application Fraud**
Organized fraud rings are using **synthetic identities** and stolen data to apply for loans they never intend to repay. These schemes often slip past traditional verification systems, creating long-term losses for credit unions. Read Me!

**6. Card Skimming & POS Attacks**

Skimming devices on ATMs and point-of-sale terminals remain a growing threat. Fraudsters steal card data and PINs, often combining this with social engineering to bypass security. Read Me!

**7. Behavioral Exploits & Insider Risks**
Fraudsters are shifting from pure tech attacks to **behavioral manipulation**, exploiting trust between staff and members. Insider fraud and weak internal controls remain a major vulnerability for smaller credit unions. Read Me!

## CU Learning in Motion: Upcoming MCUL Trainings & Events

Make sure you check out our MCUL Education master calendar to find all the latest information on the wonderful events our team is hosting!

Link to MCUL Education Calendar

INFOSIGHT360

## Around the InfoSight: Highlights Worth a 360° Look

***New FAQs Related to Suspicious Activity Reporting***
On October 9th, the Financial Crimes Enforcement Network (FinCEN) along with the joint agencies, including the National Credit Union Administration (NCUA), issued four frequently asked questions related to SAR filing. The FAQs, available here, are summarized below:

- A credit union is not required to file a SAR simply because a transaction (or series of transactions) is at or near the CTR reporting threshold of $10,000. A SAR is only required if the institution knows, suspects, or has reason to suspect that the transaction(s) are designed to evade the CTR reporting requirement.
- A credit union is not required to conduct a separate review after the filing of each SAR to determine whether the suspicious activity is continuing. Instead, it can rely on its policies, procedures, and internal controls to monitor for ongoing suspicious activity.
- For ongoing suspicious activity, any subsequent SAR filing should include a full 90-day review period. For example, the credit union identifies suspicious activity on day 0. It has until day 30 to file a SAR. A full 90-day review period from the filing of the previous SAR would end on day 120. The credit union would then have until day 150 to file a subsequent SAR for the continuing suspicious activity.
- Documenting a credit union's decision not to file a SAR is not a requirement under the Bank Secrecy Act or its implementing regulations; it is a best practice. In most instances, a short, concise statement regarding the decision not to file will suffice.

***Protecting Your Credit Union in a Digital World***
October is Cybersecurity Awareness Month! Cyber incidents, like other types of disruptions, can have immediate and long-term impacts and consequences across the credit union. The FFIEC defines cybersecurity as "the process of protecting information by preventing, detecting, and responding to attacks." They can result from a variety of causes, both malicious and non-malicious, with impacts to hardware, infrastructure, applications, and data.

Credit unions must manage internal and external threats and vulnerabilities to protect their information and infrastructure against cyber-based attacks. As trusted financial partners, safeguarding member data is a top priority. With the rise in phishing scams, identity theft, and account takeovers, proactive cybersecurity measures are critical to maintaining trust and security.

While there is no one-size-fits-all solution, here are some common ways credit unions are protecting themselves.

- Implement **Multi-Factor Authentication** (MFA) across all systems to prevent unauthorized access.
- Conduct Regular **Cybersecurity Training** for staff and members to build awareness and reduce human error.
- Invest in **Advanced Threat Detection Systems** that monitor and respond to suspicious activity in real time.
- **Keep Systems and Software Updated** to patch vulnerabilities and stay ahead of emerging threats.
- **Collaborate with Industry Partners** (such as InfoSight360 and your state league/association!) to stay informed about the latest threats, get support in the event of an incident, and make sure you have a solid recovery plan in place.

***Working Together to Fight Fraud***
Cybersecurity is a team effort, and we're here to support your credit union with tools and resources that make a real difference.

**InfoSight:** Find practical guidance and tools in a wide range of topics including Cybersecurity, Cyber-Enabled Fraud, Security Programs for Credit Unions, and Data Breach response.

**RecoveryPro:** Our Cyber Incident Response chapter includes everything you need to prepare and respond, including a Cyber Attack Risk Assessment, incident response guidelines, communication templates, planning resources, and real-world scenario examples that can be integrated into your Business Continuity Plan.

**CU PolicyPro:** Access model policy content to help you build or update policies for Incident Response, Information Security, AI Usage, and Digital Banking.

***Are Your Policies Up to Date?***
It's hard to believe how quickly the year is flying by. As we approach year-end, now is the perfect time to ask:

- Have all your policies been reviewed and board approved this year?
- Are your procedures up to date?
- Are you up to date on the latest changes from InfoSight360?

Annual policy reviews are not just a best practice, they're a regulatory requirement. CU PolicyPro make this process easier by offering:

- Quarterly content updates (the next update is coming soon!)
- Tracked changes
- Assignment reviews
- Auditing notes and reports
- Easy publishing options

**Documentation Matters**
A strong compliance program depends on thorough documentation. It creates a clear audit trail, helps identify gaps, and ensures consistency. CU PolicyPro's auditing tools support the full lifecycle of your policies and procedures, keeping everything organized and accessible.

**Upcoming Training Opportunities**
Stay sharp with these upcoming InfoSight360 sessions:

- Managing Content in InfoSight360 – November 4, 2025
- Ongoing Content Maintenance in InfoSight360 – November 13, 2025

**Quick Tips for Policy Review**

- Use the CU Policies Report in the Admin area for a snapshot of all your policies, including last actions, revised and review dates, board approval dates, and the date the model policy was added to your content.
- Find content update information for each policy in the "Model Policy Updates" section at the end of all policies. There is also summary information on the InfoSight360 Support site on the "Content Updates" page.

***NCUA Issues No Regulation by Enforcement Policy***

Last week, the National Credit Union Administration (NCUA) issued a policy statement that regulation by enforcement is unethical and not permitted at the agency.
In announcing the policy statement, Chairman Kyle S. Hauptman said, "No enforcement action should ever set, or even clarify, policy. In America and other free societies, the sequence is: set speed limits, then give speeding tickets."

The policy statement has four core principles:

- No person or entity regulated by NCUA has any obligation to be aware of any prior enforcement action because no new policy is ever set via an enforcement action. Enforcement actions shall occur only in the case of clear and significant violations of law or regulation.
- No enforcement action shall be motivated by trying to boost the agency's enforcement totals. The NCUA does not set "speed traps" to increase enforcement totals.
- The NCUA's goal is for credit unions to operate safely and soundly in compliance with applicable laws and regulations. The agency will seek to remedy problems without the use of an enforcement action whenever possible.
- NCUA employees are protected against arbitrarily poor performance reviews, allegations of misconduct, and wrongful termination. This same due process must be extended to those they regulate.

If the NCUA finds a harmful practice within the industry that must be addressed, it will consider rulemaking. The sequence at the agency will be to first publish rules, and then (and only then) enforce them.

## Open Comment Calls

If you have input on any comment calls below that you would like to provide for consideration, please direct them to Haleigh.Krombeen@mcul.org no later than 3 weeks prior to the comment due date.

**FinCEN request for comment:** RFC on Section 314(a) Information Requests

FinCEN is seeking comment on the proposed extension, without changes, of existing Bank Secrecy Act (BSA) information-collection requirements related to information sharing between government agencies and financial institutions (commonly referred to as section 314(a) requests). Under these regulations, when FinCEN issues an information request, a financial institution must review its records to determine whether it currently maintains or previously maintained any account for, or has engaged in any transaction with, an individual, entity, or organization identified in the request. If a match is found, the institution must report the relevant information to FinCEN.

The BSA information-sharing requirements under section 314(a) apply to all federally insured credit unions. When FinCEN issues an information request, credit unions are required to review their records to identify any accounts or transactions associated with the named individuals or entities and report any matches in the manner and timeframe specified. Although this information collection is not new and FinCEN is proposing no substantive changes, the process can be operationally burdensome. This is particularly so for smaller credit unions with limited compliance staff, as it requires maintaining appropriate search capabilities, procedures, and documentation to ensure timely responses.

***KEY POINTS:***

- FinCEN is proposing to renew, without changes, the existing information collection requirements under BSA regulations related to government-to-financial-institution information sharing (commonly referred to as section 314(a) requests).
- Credit unions must search their records upon receiving a FinCEN request to determine whether they maintain or have maintained any account or transaction for the named individual or entity and report any matches promptly.
- While no new requirements are being proposed, this RFC provides an opportunity for credit unions to comment on the compliance burden associated with 314(a) searches, including the frequency of requests, the clarity of instructions, and the operational impact on staffing and systems.
- Feedback may help FinCEN better understand how these information-sharing obligations affect institutions of different sizes and whether there are ways to streamline or modernize the process without compromising law enforcement objectives.

**Feedback to America's Credit Unions Due:**
November 10, 2025

Submit Feedback

**Comments Due:**
December 01, 2025

*Federal Register*

Questions, Comments, Concerns? We are here to help! Email us at ComplianceHelpline@mcul.org

**If this newsletter was forwarded to you and you'd like your own emailed copy, or wish to be removed from this list, please contact Haleigh.Krombeen@mcul.org or JaMille.Rauls@mcul.org**