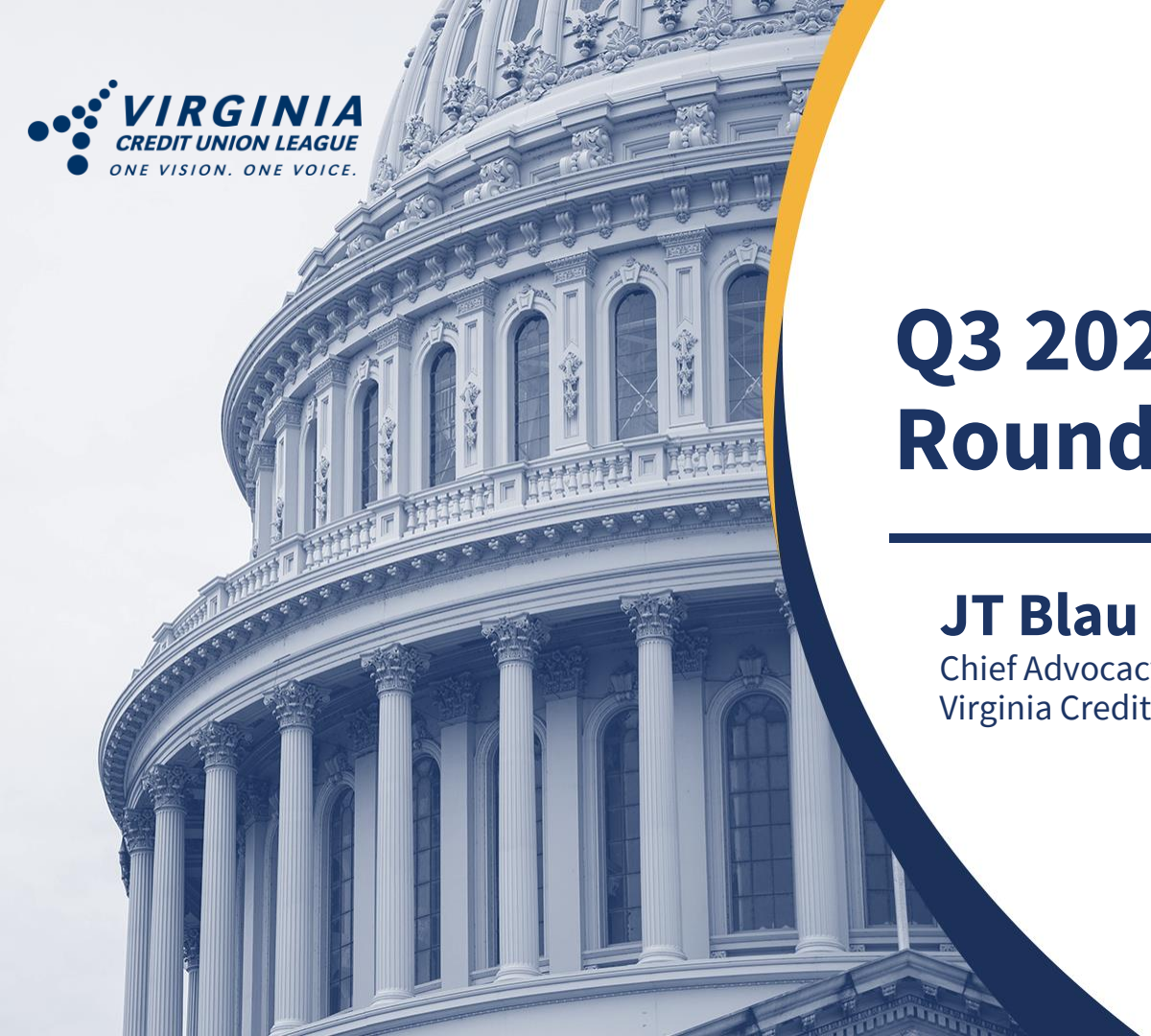


VIRGINIA CREDIT UNION LEAGUE
ONE VISION. ONE VOICE.

Q3 2023 Compliance Roundtable

JT Blau
Chief Advocacy Officer,
Virginia Credit Union League

Jay Spruill, III
Of Counsel,
Woods Rogers Vandeventer Black

Agenda

- NCUA’s new cybersecurity reporting rule
- NCUA’s new member expulsion rule
- IRS Memo on Employee Retention Credits
- FFIEC’s updated BSA/AML Examination Manual
- Upcoming dates and a cautionary BSA tale
- Fraud scams targeting member accounts

NCUA's Cybersecurity Incident Reporting Rule

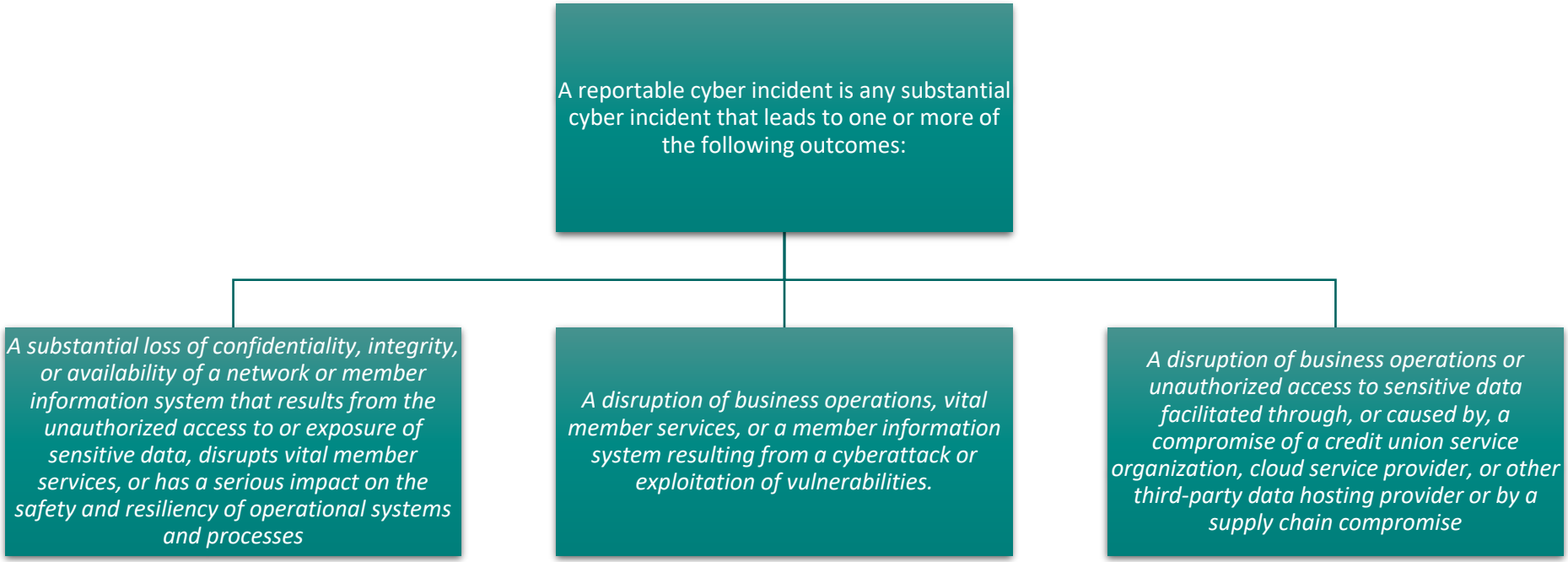
- Requires a CU to notify NCUA of a reportable cyber incident within 72 hours.
- Effective 9/1/2023
- Update policies, procedures, incident response plans, business continuity plans, etc.
- Important to understand:
  - What makes an incident reportable?
  - When does the 72 hours start?
  - How do I report?
  - What should I report?

What qualifies as a reportable cyber incident?

Cyber incident:

> “an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system or actually or imminently jeopardizes, without lawful authority, an information system.”

What qualifies as a reportable cyber incident?



When and how to report?

- The 72 hour clock starts when the credit union reasonably believes that it has experienced a reportable cyber incident.

- If the CU is notified by a vendor of a compromise, the clock starts upon receipt of that notification, or when they form a reasonable belief that an incident has occurred, *whichever is sooner*.

- Two ways to report: phone or email
  - Call the NCUA at 1.833.CYBERCU (1.833.292.3728) and leave a voicemail, or
  - Send a secure email to cybercu@ncua.gov

What to report?

What to Report

Federally insured credit unions should be prepared to provide the following information, if known, at the time of reporting.

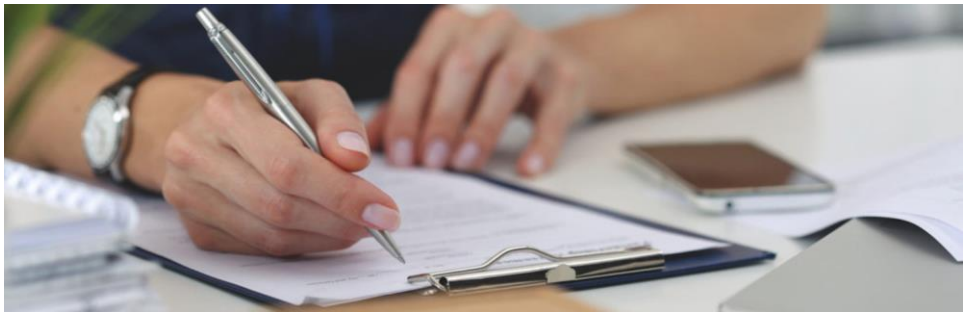
- **Reporter Name and Title:** Name and title of individual reporting the incident
- **Callback Number:** Best callback number for the NCUA to contact regarding the incident
- **Charter Number:** Do not include leading zeros
- **Credit Union Name:** Name of affected credit union
- **Date and Time Identified:** The date and time the credit union reasonably believes a reportable cyber incident took place
- **Description:** A general description of the reportable cyber incident:
  - What services were impacted?
  - Was sensitive data or member information compromised?
  - What impact did it have on operations?

At the time of initial notification, do not send the NCUA:

- **Sensitive personally identifiable information;**
- **Indicators of compromise;**
- **Specific vulnerabilities; or**
- **Email attachments.**

Implementation – Next Steps?

- Steps credit unions should take:
  - Update Response Plan
  - Review Contracts
  - Train Employees
  - Monitor and Review
  - Document All Incidents

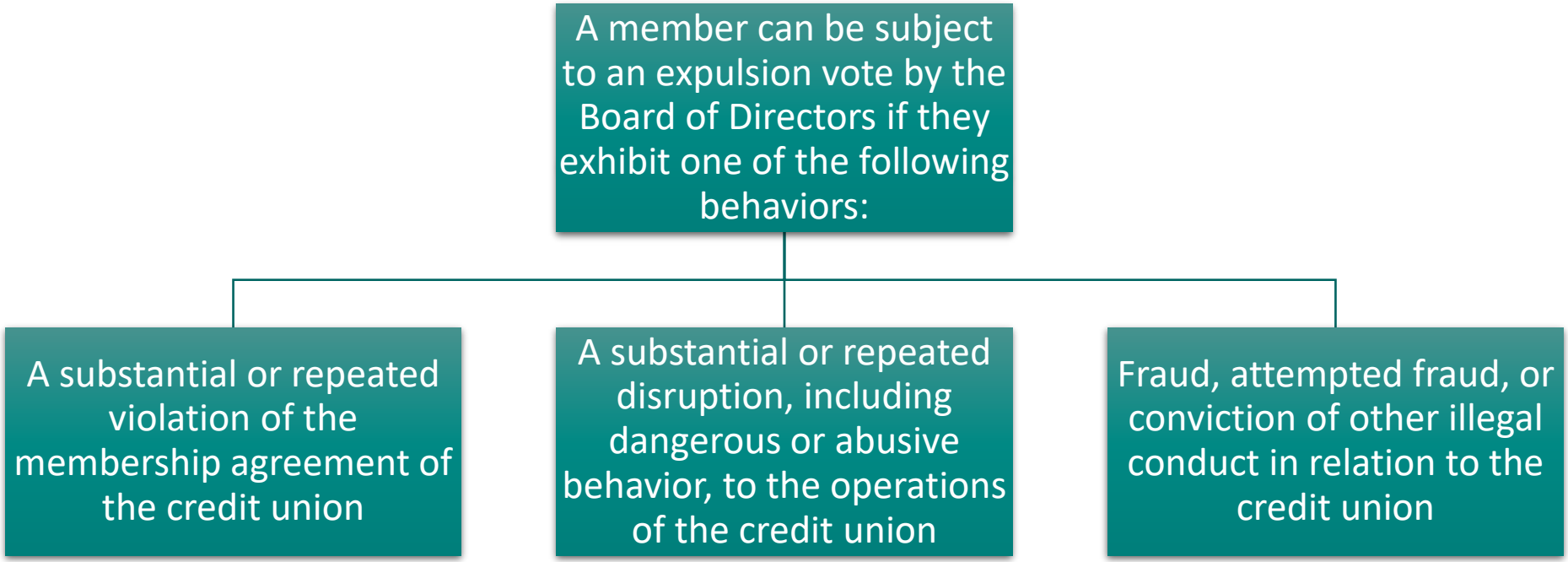


- Resources:
  - NCUA Letter to Credit Unions 23-07
  - Cyber Incident Reporting Quick Reference Guide
  - Final Rule
  - VACUL REGular Blog

NCUA's Member Expulsion Rule

- Allows for a credit union's Board of Directors to expel a member for cause
- New bylaws language was added on 8/25/2023
- Update bylaws, draft policies and procedures, and notify all members of the policy before using this process.
- Complex rule – important to understand all the details.

What qualifies as “for cause?”



What notices are required?

- Member Expulsion Policy – to all members
  - Informs all members of the new policy
- Pending Expulsion Notice
  - Tells a member the Board will vote on their expulsion and they can request a hearing
- Notice of Expulsion
  - Lets a member know they've been expelled, tells them how their account will be wrapped up.
- Sometimes required: Written warning
  - Required for repeated violations of the membership agreement

What happens at the hearing?

- Hearing format and details are up to the credit union.
- Can be in person or via videoconference
  - At member's request, can also be over telephone or conducted with written submission
- 2/3 vote required to expel
- Vote must occur within 30 days of the hearing.
- Members can request re-instatement one time.
  - Majority vote to re-instate
- No right to appeal, but can complain to NCUA.

Implementation – Next Steps?

- Steps credit unions should take:
  - Adopt new bylaws language
  - Implement policies and procedures
  - Train board members on the process
  - Notify all members of the policy, train staff on handling questions

- Resources:
  - NCUA Standard Bylaws
  - Final Rule
  - VACUL REGular Blog
  - With Flying Colors Podcast #125: JT Blau of the Virginia League: Deep Dive on Member Expulsion

IRS Weighs In: Can Credit Unions Claim the Employee Retention Credit?

- Legislation passed after the pandemic offered tax credits to businesses who experienced a disruption of their operations.
- Started with the CARES Act and extended with the Relief Act and subsequent legislation.
- Many credit unions explored their eligibility for these credits, with some using third party vendors to assist them in determining eligibility and filing.

IRS Weighs In: Can Credit Unions Claim the Employee Retention Credit?

- Initial legislation excluded "the Government of the United States, the government of any State or political subdivision thereof, or any agency or **instrumentality** of any of the foregoing“ from receiving the credit.
- IRS recently issued a memo stating that federal credit unions **are** instrumentalities of the federal government.
- The Relief Act (passed late 2020) and subsequent legislation contained additional language making credit unions eligible.
- IRS determined that FCUs **can** claim the credit for 2021 wages but **not** for 2020 wages.

Can FCU Claim Credit?	2020	2021
Q1		Yes
Q2	No	Yes
Q3	No	Yes
Q4	No	

IRS Weighs In: Can Credit Unions Claim the Employee Retention Credit?

- This only applies to federal credit unions – not state charters.

- Credit unions should work with their auditors, vendors, and legal counsel to determine how to properly claim and record these tax credits.

- Resources:
  - IRS Memo
  - VACUL REGular Blog
  - NAFCU Compliance Blog

FFIEC Updated BSA/AML Examination Manual

- FFIEC recently published updates to their BSA/AML Examination Manual, updating 6 sections.
- While most of the updates won't apply to most credit unions, there was an update related to 314 information sharing.
- Previously, FFIEC guidance was to only report that you had a 314(a) positive match, and no additional information. The updated manual now instructs FIs to report name, account number, transaction date, and SSN/TIN, and you can choose to provide more info.
- On 314(b) voluntary sharing, the manual reiterates that you cannot share that a SAR has been filed. You can, however:
  - share transaction information that led to a SAR,
  - use information you receive in determining whether to file a SAR, or
  - work with the other institution to file a joint SAR

- Resources:
  - FFIEC BSA/AML Exam Manual
  - VACUL REGular Blog
  - CUNA CompBlog

Looking Ahead – a few dates

- November 1: Deadline to report unclaimed property to Virginia
  - See the state's website for more details

- January 1, 2024: Effective Date for FinCEN's Beneficial Ownership Information Reporting Final Rule

A Cautionary Tale

- FDIC issued a consent order against Vermont State Bank, a $24 million bank in Illinois for several BSA violations. Specifically, they violated 3 of the original 4 BSA Pillars.

- Pillar 1: Internal controls: Did not conduct risk assessments on RDC, did not define risk categories in their BSA policy, and they did not document suspicious activity reviews.

- Pillar 3: Designated BSA Officer: The bank had 3 co-BSA Officers, none of whom received training or had any oversight of the RDC process

- Pillar 4: BSA Training: Lacked accurate documentation of BSA Training

Fraud Trends Impacting Members

- The Compliance Hotline has been getting a lot of questions about how to assist members who have been the victim of a scam
  - Romance scams, fake purchase scams, phishing, elder abuse, etc.

- A question that frequently arises is: Is the credit union required to reimburse members for a loss?
  - The credit union wants to help members, but shouldn't take unnecessary losses.

- Very fact dependent, but often comes down to the definition/interpretation of "authorized."
  - If a member gives their account information to someone or clicks something to send a payment, but it turns out they were dealing with a fraudster and didn't know it, that is still likely to be "authorized"
  - Did the member evidence an intention to authorize the transaction?

Fraud Trends Impacting Members

- Misconception about the right of a CU to charge back a check when it is returned.
  - CU can charge back the amount against the account, and the member is responsible for the amount.
  - The CU is an agent for the member in collecting.
  - Could also be a defense based on the timing of when the member reports fraud. This also applies to EFTs.

- Be careful about verifying funds – “Is this check good?”

- Best practice: be proactive on prevention
  - Educate members on common scams, trends
  - Have a formal fraud prevention program to help mitigate losses
  - Have a good contact at the FBI and law enforcement

Compliance Hotline Contact Information

- Phone: 800.552.4529
- Email: joseph.spruill@wrvblaw.com

Questions?

VIRGINIA CREDIT UNION LEAGUE
ONE VISION. ONE VOICE.

Thank You

JT Blau

jblau@vacul.org

703.798.2752 (JT)

108 N 8th St
Richmond VA, 23219

VIRGINIA CREDIT UNION LEAGUE
ONE VISION. ONE VOICE.