

Fraud Prevention: It Begins with the Supervisory Committee



June 19, 2025

Presented by:
Mike Richards &
Erin Brophy



When fraud hits your members,
it's not just their problem—
it becomes yours.

Are you doing enough to protect the people who trust you most?

From Mobsters to Malware: Protecting Members in the Age of Modern Scams

- Fraud impacts every member, every employee, and every institution in the credit union movement
- But we're not just talking about compliance.
- We're talking about the people we serve—and what happens when fraud hits home.



Why the Bank Secrecy Act Exists

- 1970: Created to stop Mafia money laundering
- Targeted cash-heavy businesses, illegal gambling, extortion, and racketeering
- Early focus: recordkeeping, CTRs (\$10,000+), and identifying suspicious activity

1970 Acts of Congress

- **Bank Secrecy Act-** Signed into law by **President Richard Nixon** on **October 26, 1970**.
- **Racketeer Influenced and Corrupt Organizations (RICO) Act**
- **Organized Crime Control Act**
- **Comprehensive Drug Abuse Prevention & Control Act**

Details of the Bank Secrecy Act of 1970

- **Currency Transaction Reports (CTRs)** for \$10,000 or more in cash
- **Foreign Bank Account Reporting (FBAR)** for accounts with \$10,000 or more
- **Recordkeeping Requirements** including customer identification information
- **International Financial Transactions** over \$10,000
- **Financial Institution Compliance**
- **Criminal Penalties** for non-compliance
- **Enhanced Government Authority** giving access to financial records
- **Included all Financial Institutions:** banks, credit unions and savings associations

The Evolution of Organized Crime

From Capone to Cartels to Crypto

- 1980s: Colombian cartels use U.S. banks to launder billions
Suspicious Activity Reports (SAR)
- 1990s: Russian syndicates exploit weak regulations
Know Your Customer (KYC)
- 2000s: Cybercrime and terrorist financing rise
USA PATRIOT ACT
- 2010s: Global fraud rings and human trafficking
- 2020s: Ransomware, crypto laundering, and synthetic identity fraud

Modern Organized Crime Looks a Little Different

- Decentralized, tech-savvy networks
- Exploit phones, texts, social media, and crypto
- Target people, not systems



Organized crime doesn't need territory or turf anymore. It needs a Wi-Fi signal and a willing victim



Modern Crimes Targeting Individuals Directly

Crime Type	How It Targets Individuals
Phishing & Email Scams	Fake emails trick people into giving up bank info or passwords
Ransomware Attacks	Encrypts a person's files and demands payment to unlock them
Romance Scams	Builds fake emotional relationships to steal money
Investment/"Pig Butchering" Scams	Promises crypto or trading profits, then vanishes with funds
Kidnapping/Get Out of Jail Scams	Someone needs help immediately. Child has been kidnapped or loved one is in jail. Must pay to resolve.
Tech Support Scams	Pretends to be tech help to take control of a victim's device
Online Shopping Scams	Sells fake or non-existent goods through websites or platforms
Social Media Hijacking	Hacks accounts to steal data, scam friends, or impersonate victims
Money Muling	Convincing someone to transfer money that is actually stolen from someone else

Flipping the Script on BSA Compliance

<u>Old Thinking</u>	<u>New Approach</u>
File the Suspicious Activity Report and move on	Analyze Suspicious Activity Reports for member patterns
Follow Currency Transaction Report rules passively	Watch for structuring and smurfing (breaking large deposits down to avoid detection)
Know Your Customer to open accounts	Use Know Your Customer data to track behavior shifts
Compliance is a department job	Member protection is a Credit Union-wide effort

What Can the Supervisory Committee Do?

- Shift the conversation from compliance to protection
- Prioritize fraud education and scam alerts for members- Use website and social media for education
- Support tech that detects fraud in real time
- Create a culture of fraud reporting and early intervention- Continual conversation with staff and members.

What Compassionate Response Looks Like

For Members: Human-Centered Support

- Listen without blame. Many members feel ashamed — don't ask why, ask how you can help.
- Offer step-by-step recovery help. Freeze accounts, file reports, offer credit monitoring — walk with them, not just behind the teller window.
- Normalize the experience. Say things like:
 - “You’re not alone. These scammers are professionals. We’re here for you.”

What Compassionate Response Looks Like

For Staff: Empowerment and Emotional Safety

- Train staff for empathy, not interrogation.

“I’m so sorry this happened. Let’s take care of it together.”
- Give them permission to feel. Hearing trauma every day can cause burnout.
- Build an internal ‘fraud recovery toolkit’ so they know exactly what to do — and don’t feel helpless in the moment.

Test Your Basic Fraud Knowledge Quiz

How often do you think your members are being targeted by scammers?

- A. Rarely
- B. A few times a year
- C. Monthly`
- D. Weekly or more

 **Answer: D. Weekly or more**

Scammers cast wide nets using robocalls, phishing emails, social media DMs, and text messages. Most members are targeted **multiple times a month**, often without realizing it. The scale is massive and continuous.

Test Your Basic Fraud Knowledge Quiz

Who is most vulnerable to scams in your membership?

- A. Older adults
- B. Young adults
- C. Non-tech-savvy members
- D. All of the above

 **Answer: D. All of the above**

Different scams target different groups:

- **Older adults** – Tech support, romance, IRS scams
- **Young adults** – Job scams, online shopping, crypto fraud
- **Non-tech-savvy members** – Any scam exploiting unfamiliarity with apps or security tools

No group is immune—scammers customize their approach based on the victim.

Test Your Basic Fraud Knowledge Quiz

What percentage of fraud losses do you think come from scams that start with a phone call or email?

- A. Less than 25%
- B. 25–50%
- C. 50–75%
- D. More than 75%

 **Answer: D. More than 75%**

According to the **FTC** and **FBI Internet Crime Report**, the majority of reported financial losses come from scams initiated through **phishing emails, phone calls, or text messages**—not traditional hacks.

Social engineering is now more dangerous than brute force cyberattacks.

Test Your Basic Fraud Knowledge Quiz

What's the biggest barrier to protecting members from scammers?

- A. Lack of education
- B. Limited resources
- C. Rapidly evolving scams
- D. Members don't believe it'll happen to them

 **Answer: C. Rapidly evolving scams**

While education and resources matter, the real challenge is that **scams evolve constantly**—new formats, platforms, and emotional triggers.

Credit unions often struggle to keep up, and members are overwhelmed or unaware of emerging tactics.

Test Your Basic Fraud Knowledge Quiz

Should the board play a more active role in fraud prevention?

- Yes
- No
- Unsure

 **Answer: Yes**

Board oversight and tone from the top are critical. The board:

- Sets strategic priorities
- Approves budgets for education and tech solutions
- Can push for regular member communication and monitoring/reporting programs

Member protection is a **governance responsibility**, not just an operational one.

BSA Terms to Know

- **BSA:** Bank Secrecy Act
- **AML:** Anti-Money Laundering
- **SAR:** Suspicious Activity Report
- **CUSO:** Credit Union Service Organization
- **NCUA:** National Credit Union Administration
- **CTR:** Currency Transaction Report
- **CDD:** Customer Due Diligence
- **EDD:** Enhanced Due Diligence (for higher-risk members)
- **KYC:** Know Your Customer (critical to BSA compliance)
- **OFAC:** Office of Foreign Assets Control
- **FinCEN:** Financial Crimes Enforcement Network
- **MSB:** Money Services Business
- **FATF:** Financial Action Task Force

Thank you, NACUSAC & SC Members!



Mike Richards

mrichards@richardscpas.com

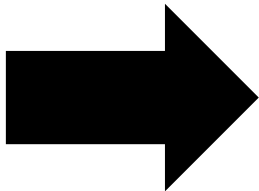
(714) 615-1635



Erin Brophy

ebrophy@richardscpas.com

(949) 395-7569



If you would like to have a confidential conversation related to fraud or a potential fraud, inside or outside of your organization, please feel free to reach out.

