

Credit Unions to the Rescue!

"Not for Profit – Not for Charity – But for Service"! They have a "common bond" Field of Membership!

- **Credit unions are well positioned** to manage the risks migrants take escaping the socialists hot on their trail and the communists now embedded in the U.S. awaiting their arrival.
- **Their best positioned** to manage the new risks created by Artificial Intelligence (AI).
- **Best positioned** to teach how any two not related voters can form a "Political Action Committee (PAC).
- **Best positioned** to teach the QR technology County Parties can use to track ballots and ballot applications from their order, to the printer, to the "time-stamped" counting the day of the election.
- **Best positioned** to understand and teach how the Wisconsin Election Commission (WEC) worked with the Election Records Information Center (ERIC) to track and move voters and

votes in and out of Wisconsin.

- **Best positioned** to "flash-back" in history and teach the lessons we've learned during past elections.
- **Best positioned** to mentor voter-fraud auditing #101 and stage chapter' assets during our "Sting" operation.
- **Best positioned** to explain when voting machines are not required.
- **Best positioned** to audit voting machine software for "Block chains" and AI technologies.
- **Best positioned** to explain the "The "Trump Trap"".
- **Best positioned** to explain How they pulled it off!
- **Best positioned** to "Benchmark" Biden vs. Trump performance before November 5, 2024.
- **Best positioned** to explain the laws governing the ballot harvesting, ballot handling procedures and enforce the "ballot chain of custody" controls needed to ensure all voices are heard and all votes are counted on November 5, 2024.

The Risk Management Learning Center

Managing voter-fraud Risks during the November 5, 2024 Presidential Election

Written by

Rich Woldt CEO: The Risk Management Learning Center

Please share this brochure with your Credit Union Board of Directors, Management Team, Audit/Supervisor Committee Federal (NCUA) and State Regulators!

This flyer can be downloaded from RMLC web sites to include www.freedomhillpatriots.com



As you customize your contingency plans, so should you customize your Voter-fraud auditing plans to fit your Credit Union's Field of Membership

Plans become outdated because employees, buildings, and operations have changed and no one remembered to adjust the contingency plans.

Customize recommendation in this brochure to fit your special needs and personal situation. Create a written action plan and incorporate it into your business contingency plans.

Develop your own family emergency evacuation plan from your home and place of employment. Annually, review building evacuation plans designated by you employer, local fire department, and Director of Emergency Government. Discuss your own "best" evacuation route from your home to a relative or friends in another state. Write your own family contingency plan and share it with your neighbors.

1. **Benchmark Your Company's Contingency Plans:** Obtain a copy of the "Paid Paranoid" by Paul Bergee and conduct your own evaluation of your business' or employer' contingency plans.

Fraud, Embezzlement, Scams & White Collar Crimes:

Embezzlers, scam artists, and normally honest people are all motivated by economic need. Take away someone's means of support and by definition there will be an incentive to perpetrate a scam, fraud, and embezzlement to meet their

needs. Justifications will include, "Everyone is doing it, I have no choice, they owe it to me, and I'll pay it back someday." Embezzlers who have already begun to embezzle will make one last effort and use the disaster to cover their tracks. The following recommendations will strengthen you defense against the seasoned embezzler while discouraging an honest person from doing something illegal during a time of desperation.

1. **Take Control of Building Access:** Businesses should make sure no one person has all the keys, combinations, passwords, etc. to make it from the parking lot to the cash items stored on premise. Separating access controls so it requires more than one person will discourage burglary, robbery, extortion, and efforts to conceal a fraud or embezzlement.
2. **Take Control of Administrative Access Codes:** Computer, website, wire transfer, and internet banking systems are all designed and maintained by an administrator. Computer fraud such as the creation of fictitious accounts, website fraud such as phishing and pharming, wire transfer fraud such as money laundering, and internet banking fraud such as unauthorized closing of accounts, is common before during and after disasters. Therefore, business owners and internal auditors should closely monitor all administrative transaction immediately before, during, and after a disaster.

Immediately following the disaster, all administrative access codes should be changed.

3. Losses from white collar crimes can easily exceed personal property losses during a disaster. Therefore, administrators, while they might need access to maintain your systems should not have total control over your computer, website, wire transfer, or internet banking systems.

- Access codes should be authorized and distributed on a "need to know" basis and changed frequently to discourage an ongoing embezzlement. Administrative duties should be rotated on a surprise basis and system file maintenance reports should be reviewed quarterly to ensure all system changes and maintenance performed was authorized.

We all learn from our mistakes. So while the pessimists focus on blaming others for what went wrong during Katrina, I encourage you to take the optimistic high road and focus on process improvements that will better prepare your family, your employer, and your community for the next life threatening challenge.

Rich Woldt CEO

The RM Learning Center