

# RISK Alert

ACTIONABLE INSIGHTS FOR BOND POLICYHOLDERS.



Alert Type

Awareness

Watch

Warning

## Employee Collaboration Tools Can Pose Increased Legal and Data Risks

With a shift to remote and hybrid work arrangements, many organizations have built enhanced connections between teams through the implementation of employee collaboration (EC) and channel-based messaging applications like Microsoft Teams and Slack. For many employees, these collaboration tools have practically replaced internal email. While these tools have made teams more collaborative and productive, they also pose potential risks related to data governance, employment practices, and retention requirements.

### Details

With credit union leadership recognizing the need to enhance team connections, the adoption of employee collaboration (EC) and messaging platforms has steadily increased. As a result, business communication has become less formal, and contributed to by a broader audience of participants. Despite increased productivity, risks related to data governance, employment practices liability, data retention efforts, and reputational missteps have also increased.

### How do these collaboration tools increase risks?

For instance, instead of an employee working on a static document saved locally to a single device and shared back and forth between co-workers via email; employees may now work on that document together while it's saved on a cloud-based collaboration platform. They may also chat about it via an in-office chat application, post updates via an EC channel, as well as email copies and/or edits back and forth to each other. Capturing and preserving this unstructured data usually falls outside of most standard monitoring and archiving solutions.

For risk and compliance professionals, data governance associated with conversations on collaboration platforms will require more nuanced policy as to not discourage use, but also ensure compliance with regulatory obligations. As for legal proceedings, existing electronic discovery policies, and eDiscovery tools may be compromised by EC platforms which allow users to create different types of messages in different formats. These limitations potentially pose the risk of credit unions failing to meet requests from plaintiff counsel and regulators.

There are also the associated risks that come along with increased unmonitored communication. Non-verbal or text-based claims of bullying, harassment and discrimination via text, image, video, and file sharing are often unmonitored and unrecorded. This perceived freedom has led to increased claims of such behavior.

The proliferation of collaboration tools will continue to shift the dynamics of workplace communications requiring credit unions to update governance measures to account for their increased usage.

**Date:** July 12, 2022

**Risk Category:** Employment Practices; Remote Work; Hybrid Work; Data Governance; Data Retention; Communication

**States:** All

**Share with:**

- Executive Management
- Human Resources
- Legal / Compliance
- Risk Manager



### Facing risk challenges?

[Schedule](#) a free personalized discussion with a Risk Consultant to learn more about managing risk.

## Risk Mitigation

Consider these important mitigation tips:

- Credit unions should partner with legal counsel to ensure Ediscovery policies, and efforts including the preservation and collection of all conversational data associated with employee collaboration (EC) tools. Policies should be expanded to include all attachments, emojis, videos, and metadata storage locations and retrieval protocols.
- Credit unions should consider strong written policies that dictate no sensitive data should be used within collaboration platforms that does not actually address or satisfied previously identified business needs.
- The implementation of data loss prevention tools that will monitor, scan, and classify various data types that may exist across the collaboration ecosystem should also be considered. This will provide for a deeper understanding of what type of data is residing within these collaboration tools counter to established written policy guidelines.
- Credit union leadership should provide in depth evaluation of collaboration tools and any updated features to ensure a benefit versus risk analysis is completed. New collaboration tool features may fall out-of-line with credit union risk appetite and should be disabled if it is determined they are outside the intended scope of use.
- Acceptable use policies, and existing personnel guidelines, should be updated to clearly identify what sort of communication is prohibited. They should also clearly state how individuals - who may feel they are being harassed or discriminated against by conversations taking place within these collaboration tools - can report their concerns. These should be in line with existing harassment and discrimination policies.

## Risk Prevention Resources

Access CUNA Mutual Group's [Protection Resource Center](#) at [cunamutual.com](#) for exclusive risk and compliance resources to assist with your loss control efforts. The Protection Resource Center requires a User ID and password.

- [Flexible / Hybrid Work Arrangements Risk Overview & Checklist](#)
- [Flexible Work Arrangements Risk Overview](#)

### Employment Practices Risk Management Hub

Designed to help reduce exposure to employee practice liability claims, the insights, resources, model policies / procedures, and training modules at [www.epl-risk.com](#) are exclusively available for CUNA Mutual Group Employment Practices Liability policyholders.

Content on the [epl-risk.com website](#) is developed and maintained by The McCalmon Group, Inc. The McCalmon Group works with some of the largest employers in the world to make workplaces safe, equal and more productive.

If you're not sure how to access...review [Quick Start Registration Guide](#).



### Access the Protection Resource Center for exclusive resources:

- [Loss Prevention Library](#) for resources & checklists
- [Webinars and Education](#)
- [RISK Alerts Library](#)
- [Report a RISK Alert](#)

The Protection Resource Center requires a User ID and Password.

© CUNA Mutual Group, 2022

Insurance products offered to credit unions are underwritten by CUMIS Insurance Society, Inc., a member of the CUNA Mutual Group. This RISK Alert is intended solely for CUNA Mutual Group Fidelity Bond policyowners to prevent fraud losses. Any further distribution of this information could subject you to liability under common law and various statutes including the Fair Credit Reporting Act.

This resource was created by CUNA Mutual Group based on our experience in the credit union, insurance, and risk management marketplace. It is intended to be used only as a guide, not as legal advice. Any examples provided have been simplified to give you an overview of the importance of selecting appropriate coverage limits, insuring-to-value, and implementing loss prevention techniques. No coverage is provided by this resource, nor does it replace any provisions of any insurance policy or bond. Please read the actual policy for specific coverage, terms, conditions, and exclusions.