# HOT TIPS FOR DATA PRIVACY DAY – JANUARY 28, 2025

**JANUARY 2025**

To honor National Data Privacy Day on January 28, 2025, we have distilled dozens of possible action items into the most pressing cybersecurity/privacy "hot tips." Immediate action is recommended to help keep your data safe throughout the new year.

## 1. PRIORITIZE TRAINING ON NEW DATA THREATS

Novel approaches to individually targeted "spear phishing" enabled by artificial intelligence (AI) justify security-related outreach efforts to employees well above the longstanding once-a-year security training regime. The recent reality is that too many systems are being compromised by employee responses to threat actor social engineering, notably individual employees clicking on links in emails or texts from apparently reliable sources (internal firm leaders, health care, insurance or investment companies, state and federal agencies) that download malware or capture confidential data or individual financial information. As a priority matter, companies should implement protocols to advise employees of new threats as they arise and, in so doing, continually reinforce good data hygiene (including scanning for possible red flags such as external email notices on purportedly internal communications or oddities in message wording or source email address and undertaking independent checks on validity before clicking on emailed or texted links or entering sensitive data in response to an external message).

## 2. IMPLEMENT MULTI-FACTOR AUTHENTICATION

In addition to password compromise through spear phishing efforts (as mentioned above), threat actors have become increasingly effective at obtaining password information through purchases from the dark web of previously hacked individuals and cracking weak passwords using sophisticated algorithms. Once passwords are compromised, authentication - especially multi-factor authentication - that requires users to verify identities in multiple ways, is the last and best defense to prevent a system breach.

## 3. COMPREHENSIVELY REVIEW YOUR SECURITY PROGRAM TO REFLECT YOUR

## BUSINESS CHANGES AND THREAT ENVIRONMENT

Maintaining a strong and evolving written security program is not just the law in Massachusetts and other states; it represents an increasingly critical bulwark of individually tailored protections to save your business and employees from the risk of data losses. Instead of leaving security programs to a once-a-year update process, leadership should regularly consider whether program updates during the year are warranted by experience with new threats, any company breaches and near misses, and any vendor breaches and near misses (such as the 2023 MoveIt software breach, used by payroll vendors, that affected 60-plus million users). Leadership should also consider whether breach or business risks justify consideration of increases in cyber insurance and insurance coverage and liability limits.

## CONTACT

If you have any questions or if you'd like a confidential assessment of your security-related policies, please contact Rob Munnelly in our Regularory and Administrative Law Practice.