



Introduction to US Privacy and Data Security Regulations and Requirements

Kathryn (Katie) Nadro
Gary Chodes
Alex Sharpe

CYBER SECURITY & DATA PRIVACY 2025



Practical & Entertaining Education for:

- Attorneys • Accountants
- Business Owners
- Executives • Investors

Thank you to our co-producer

THE NATIONAL LAW REVIEW

The National Law Review (NLR) is a premier legal news website offering in-depth analysis on a wide range of legal and business topics. Established in 1888, NLR has evolved into a **trusted resource** for legal professionals, business leaders, and the general public, providing timely and relevant information on legislative changes, court decisions, and regulatory developments

Visit *The National Law Review* to learn more
- <https://natlawreview.com/>

Comprehensive Coverage: NLR covers nearly every legal topic, including litigation, AI & the Law, employment law, IP Law, real estate, energy, health care, bankruptcy and much more.

Expert Analysis: Articles are authored by experienced attorneys and legal professionals, ensuring accurate and insightful commentary.

Daily Updates: NLR provides hourly legal news updates, keeping readers informed about the latest developments in the legal world.

Thank You To Our Sponsor...



Restructuring & Insolvency Professionals • Bankruptcy Trustees
• Chapter 11 Debtors • Assignees • Receivers • Article 9 Sellers

A Better Way to Conduct Single Asset Sales Online!

DailyDAC™ is excited to announce its partnership with [maxXasset™](#), a simpler, easier & better way to conduct asset sales.

Take charge of your sales process! Choose the auction date, set the terms, & establish the closing timeline to suit your needs. Create & upload relevant sale documents behind confidentiality agreements, review every bidder's credentials, decide whether to approve or deny them, & monitor the bidding in real time.

No need to schedule a zoom or have the sale in an office. Now, interested parties can bid anytime, from anywhere! [maxXasset™](#) is also perfect to use in conjunction with real-time auctions, with use cases that include using it as a tool to select a stalking horse or as a tool for a first & or second round in a two-round process.

Disclaimer

- The material in this webinar is for informational purposes only. It should not be considered legal, financial, or other professional advice.
 - You should consult with an attorney & another appropriate professional to determine what may be best for the needs of your specific situation.
 - While the webinar producers & speakers take reasonable steps to ensure that the information presented is accurate, they make no guarantee in this (or any) regard.

*** These slides were produced in connection with a video webinar that premiered on 9/4/2025 . Take note, we make the PDF available for free download because the real benefit of a Financial Poise webinar is the conversation that the faculty has around the slide deck. You can access the webinar on-demand at Cerfi's LegalEdge (f/k/a [West Legal Ed Center](#)) (for attorneys or accountants seeking CLE or CPE) or [Financial Poise](#) (for everyone else).

Meet the Faculty

Panelists

[Kathryn \(Katie\) Nadro](#) - Levenfeld Pearlstein LLC

[Alex Sharpe](#) - Sharpe LLC

Moderator

[Gary Chodes](#) - The National Law Review

About This Webinar

Introduction to US Privacy and Data Security: Regulations and Requirements

- The United States has no federal data security or privacy law covering all businesses or all U.S. citizens. Instead, federal agencies and individual states have created their own patchwork of laws and regulations which must be evaluated for their application to a business.
- This webinar will help you navigate the overlapping and sometimes confusing system of laws and regulations which may impact your business, ranging from emerging state-level privacy legislation to the numerous data breach notification statutes to cybersecurity regulations with extraterritorial effect.

About This Series

Cybersecurity & Data Privacy

- Cybersecurity and data privacy are critical topics of concern for every business in today's environment. Data breaches are a threat to every business and can cause both direct losses from business interruption and loss of data to indirect losses from unwanted publicity and damage to your business's reputation. Compliance with a patchwork of potentially applicable state and federal laws and regulations may cost your business in terms of money and time.
- This series discusses the various laws and regulations that affect businesses in the United States and in Europe, as well as the best practices to use in creating an information security program and preparing for and responding to data breaches.

Episodes In This Series

#1 Introduction to US Privacy and Data Security: Regulations and Requirements

Premiere date: 9/4/25

#2 Introduction to EU General Data Protection Regulation: Planning, Implementation, and Compliance

Premiere date: 10/9/25

#3 How to Build and Implement your Company's Information Security Program

Premiere date: 11/13/25

#4 Data Breach Response: Before and After the Breach

Premiere date: 12/11/25

Episode #1

Introduction to US Privacy and Data Security_Regulations and Requirements

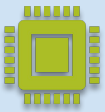
Each Financial Poise Webinar is delivered in Plain English, understandable to investors, business owners, & executives without much background in these areas, yet is of primary value to attorneys, accountants, & other seasoned professionals. Each episode brings you into engaging, sometimes humorous, conversations designed to entertain as it teaches. Each episode in the series is designed to be viewed independently of the other episodes so that participants will enhance their knowledge of this area whether they attend one, some, or all episodes.

Privacy and Data Security Concepts

What is Data Security?



The CIA Triad: Confidentiality, Integrity, Availability



All the practices and processes used to protect data from being used or accessed by unauthorized individuals



How a company safeguards the data it collects and uses from threats



Data is to be protected during transmission, when being processed, and when stored.

What is Data Privacy?



The appropriate use of data, including the use of data according to agreed purposes



How a company uses the data that it has collected



An organization cannot maintain data privacy without maintaining adequate data security

What is Personal Information?

- “personally identifiable information” sometimes called “PII”
 - Can be linked to a specific individual
 - Name, email, full postal address, birth date, SSN, driver’s license number, account numbers
- “non-personally identifiable information”
 - Cannot by itself be used to identify a specific individual
 - Aggregate data, zip code, area code, city, state, gender, age
- “sensitive personal data”
 - includes racial, ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, citizenship or immigration status, precise geolocation data, genetic or biometric data and children’s personal data
 - This definition is based on Virginia’s law, but the other 12 states’ definitions are similar.

What is Personal Information? *cont'd*

- Gray area – “anonymized” data
 - ☐ Non-PII that, when linked with other data, can effectively identify a person
 - ☐ Geolocation data
 - ☐ Site history and viewing patterns from IP address

Why Do We Need to Protect Private Information?

- Data is a corporate asset
- Corporate data is at a higher risk of theft or misuse than ever before
- Consumers now expect companies to take initiative to protect both security and privacy – in the past several years, these topics have been increasingly discussed in public, particularly in light of social media uses of information and highly publicized data breaches

What Must Companies Do to Protect Private Information? *cont'd*

- Compliance with state, local, federal laws and regulations
 - Patchwork of laws developed by sector
 - Contrast to Europe, which has a centralized, uniform law
 - Makes it difficult to comply when multiple, possibly inconsistent laws apply

What Must Companies Do to Protect Private Information? *cont'd*

- Contracts with third parties
 - States are enacting laws requiring businesses to conduct varying levels of vendor risk management. In Virginia, for example, businesses must:
 1. Clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing by the vendor, the duration of processing, and the parties' rights and obligations.
 2. Ensure each vendor processing personal data is subject to confidentiality regarding such data.
 3. Direct vendors to return and/or delete personal data it processes unless retention is required by law.
 4. Require vendor to submit to reasonable audits to demonstrate vendor's compliance with the law and contract.
 5. Require vendor's subcontractors to sign a written contract with similar personal data protection requirements.

What Must Companies Do to Protect Private Information? *cont'd*

Your company may have more PII than you are aware of

- For example, if your company gives out commercial loans, it must comply with GLB
- BUT: if you also take guarantees, then you have personal information such as account information, possibly life insurance information, mortgage information, etc. that must be secured
- Have to think more creatively about what types of information you might be collecting
 - Credit card payments – have to secure that information

Financial Laws and Regulations

Gramm-Leach-Bliley (GLB)

Overseen by the FTC

- Requires financial institutions (companies that offer consumers financial products or services like loans, financial or investment advice, or insurance) – to explain their information-sharing practices to their customers and to safeguard sensitive data through use of privacy policies and prohibitions against disclosing non-public personal information to third parties
- Also requires financial institutions to protect the security and confidentiality of their customers' non-public personal information

[FTC website](#)

FTC Safeguards Rule

Applies to financial institutions subject to the FTC's jurisdiction and that are not subject to the enforcement authority of another regulator under Gramm-Leach-Bliley Act

- Examples of covered institutions are mortgage lenders, payday lenders, finance companies, mortgage brokers, account services, check cashers, and wire transferors
- Requires covered institutions to develop, implement, and maintain an information security program, regularly monitor and test the effectiveness of their safeguards, train their staff, monitor service providers, create a written incident response plan, and require a qualified individual to oversee the information security program and report to the board of directors regularly

New York Cybersecurity Regulation, 23 NYCRR Part 500



Regulation from the New York Department of Financial Services, which went into effect March 2017 and was fully effective March 1, 2019



Mandates minimum cybersecurity standards for any banking, insurance and brokerage firm using a license to operate in New York



Covered entities had to certify compliance June 1, 2020

New York Stop Hacks and Improve Electronic Data Security (“SHIELD”) Act



Expands NY breach notification law and imposes data security program requirements on businesses that possess the private information of New York State residents

- Applies regardless of whether the businesses have any physical presence in New York State



Program requirements include administrative, technical, and physical safeguards for detecting and responding to intrusions and maintaining security of information



Businesses subject to and in compliance with Gramm-Leach-Bliley, HIPAA, or the NY Dept. of Financial Services Cybersecurity Requirements are exempted from this requirement under the SHIELD Act

New York Stop Hacks and Improve Electronic Data Security (“SHIELD”) Act *cont’d*



Limited reprieve for “small businesses” with fewer than fifty employees, less than \$3 million in gross revenues in the last three fiscal years, or less than \$5 million in year-end total assets



Expands the definition of “private information” subject to NY data breach notification law



NY Attorney General can pursue civil penalties, but there is no private right of action

Massachusetts Standards – 201 C.M.R. 17

- 2010 law – most protective privacy and security law in the US at that time
- Requires every business that licenses or owns personal information of Massachusetts residents to comply with the minimum security standards set forth in the regulation and implement a written information security program (“WISP”) with appropriate administrative, technical, and physical safeguards
 - Standards must be consistent with those set forth in state and federal regulations to which a business is subject, including data breach notification laws, HIPAA, and the Gramm-Leach-Bliley Act
- Require, when technically feasible, the encryption of personal information stored on portable devices and personal information transmitted across public networks or wirelessly

SEC Cybersecurity Rule

SEC adopted rules in July 2023 requiring registrants to disclose material cybersecurity incidents they experience and to disclose on an annual basis material information regarding their cybersecurity risk management, strategy, and governance. Registrants now must:

- Disclose on new Item 1.05 of Form 8-K any cybersecurity incident they determine to be material and to describe “the materials aspects of the incident’s nature, scope, and timing” as well as its “material impact or reasonably likely material impact on the registrant”
- Describe their processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats, as well as the material effects or reasonably likely material effects of risks from cybersecurity threats and previous cybersecurity incidents
- Report the board of directors’ oversight of risks from cybersecurity threats and management’s role and expertise in assessing and managing material risks from cybersecurity threats

Health Information and Biometric Information

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) regulates medical information.

- HIPAA Privacy Rule:
 - Requires appropriate safeguards to protect the privacy of “protected health information” (PHI).
 - Sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization.
- Gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

HIPAA *cont'd*

- HIPAA Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of “electronic protected health information” (ePHI).
- Privacy Rule and Security Rule are primarily enforced by the U.S. Department of Health & Human Services Office for Civil Rights.

Biometric Information

Primarily regulated by state statutes in the US

- Biometric information definitions can vary, but frequently include identifiers such as retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry, as well as any other information based on an individual's biometric identifier used to identify a specific individual
- Illinois Biometric Information Privacy Act: requires companies to obtain written consent from individuals before collecting or using biometric information and to maintain publicly available written policies related to the collection, use, and storage of biometric information. The policy must specify the purposes for which the biometric information will be used and the retention period for the information.
- Increasing use of facial recognition technology has led to the passage of additional laws, such as statutes in Maryland, Texas, and Oregon, and local ordinances in New York and Oregon, which require certain levels of notice and consent in order to use facial recognition or other biometric information technology

Consumer Data Protection and Privacy Laws

California Consumer Privacy Act

- Effective January 1, 2020, companies will have to observe restrictions on data monetization business models, accommodate rights to access, deletion, and porting of personal data, and update privacy policies
- “Consumers” (defined as natural persons who are California residents) have the right to know what personal information a business has collected about them and what it is used for, the right to opt out of allowing a business to sell their personal information to third parties, the right to have a business delete personal information, and the right to receive equal servicing and pricing from a business even if they exercise their privacy rights under the Act.

California Consumer Privacy Act *cont'd*

- “personal information” is “any information that...relates to...a particular consumer or household”
 - Information about a household may include information like utility bills or pricing
- Companies must comply if they receive personal data from California residents and they or their parent company or a subsidiary exceed (a) annual gross revenues of \$25 million, (b) obtains personal information of 50,000 or more California residents, households or devices annually, or (c) 50 percent or more annual revenue from selling California residents’ personal information.

California Consumer Privacy Act *cont'd*

The Act provides a private right of action that allows consumers to seek, either individually or as a class, statutory or actual damages and injunctive relief, if their sensitive personal information is subject to unauthorized access and exfiltration, theft or disclosure as a result of a business's failure to implement and maintain reasonable security measures

- Statutory damages can be between \$100 and \$750 per California resident per incident, or actual damages, whichever is greater
- The California Privacy Rights Act also established the California Privacy Protection Agency (CPPA) to enforce provisions of the CCPA/CPRA

Other State Privacy Laws

- Virginia Consumer Data Protection Act: effective Jan. 1, 2023
- Colorado Privacy Act: effective July 1, 2023
- Connecticut Data Privacy Act: effective July 1, 2023
- Utah Consumer Privacy Act: effective December 31, 2023
- Texas Data Privacy and Security Act: effective July 1, 2024
- Oregon Consumer Privacy Act: effective July 1, 2024
- Florida Digital Bill of Rights: effective July 1, 2024
- Montana Consumer Data Privacy Act: effective October 1, 2024
- Iowa Consumer Data Protection Act: effective January 1, 2025
- Tennessee Information Protection Act: effective July 1, 2025
- Indiana Consumer Data Protection Act: effective January 1, 2026
- Oregon Consume Privacy Act: effective July 1, 2024 and January 1, 2026
- Delaware Personal Data Privacy Act: effective January 1, 2025
- New Jersey Data Privacy Act: effective January 15, 2025
- Rhode Island Data Transparency and Privacy Protection Act: effective January 1, 2026
- Nebraska Data Privacy Act: effective January 1, 2025
- New Hampshire Privacy Law (SB 255): effective January 1, 2025
- Kentucky Consumer Data Protection Act: effective January 1, 2026
- Maryland Online Data Privacy Act of 2024: effective October 1, 2025
- Minnesota Consumer Data Privacy Act: effective July 31, 2025

California vs. The Rest

- All statewide privacy laws currently apply to businesses which process data from over a certain threshold of consumers (usually 50,000 or 100,000)
- All have different exemptions, definitions of “processor” or “controller,” different consumer rights and protections, and different penalties for noncompliance
- California Model: includes a revenue model which sweeps businesses in even when they process data of fewer than 100,000, as well as employee and business to business data
- Virginia Model: no private right of action, includes more exemptions for small businesses, financial institutions, health and insurance sectors
- Both the California and Virginia model provide basic consumer data rights such as the right to opt-out of certain processing, additional protections for sensitive and children’s data, and additional notice requirements
- Florida Model (Virginia-lite): applies only to businesses with \$1 billion or more in gross annual revenue – targeted to large tech companies

Federal Trade Commission (FTC)

FTC is the main federal regulator in charge of policing privacy and cybersecurity practices among U.S. companies generally.

FTC derives its power from Section 5(a) of the FTC Act and pursues cases against companies for “unfair” or “deceptive” practices, where the company allegedly had inadequate cybersecurity practices, or overstated how comprehensive their privacy and cybersecurity practices were.

Consent decrees and settlements often result in monetary damages, and requirements that companies establish rigorous privacy and data security practices (which would be overseen by the FTC).

Other Applicable Federal Laws

- CAN-SPAM Act: regulates emails that companies send for commercial purposes and requires opt-out ability for consumers.
- Telephone Consumer Protection Act (TCPA): restricts the making of telemarketing calls and creates a private right of action for consumers.
- Fair Credit Reporting Act (FCRA): regulates consumer reporting agencies and the use of such information by private parties.
- Children's Online Privacy Protection Act (COPPA): regulates the collection and use of data belonging to children under 13

Data Breach Laws and Regulations

State Level Data Breach Laws

- All 50 states, the District of Columbia, and some U.S. territories have their own data breach notification laws
- These laws generally require notification of affected individuals and regulators when a company suffers a breach of the security of an individual's personally identifiable information (PII).
- If a company suffers a data breach involving the PII of customers or employees who are resident in multiple states, it will need to comply with each applicable state's laws.

What is a Data Breach?

Unauthorized acquisition of PII that compromises the security, confidentiality or integrity of PII...

- That results or could result in identity theft or fraud (OH)
- Unless PII is not used or subject to further unauthorized disclosure (NE)
- Unless no misuse of PII has occurred or is not reasonably likely to occur (NJ)
- Unless no reasonable likelihood of harm to consumer whose PII was acquired has resulted or will result (CT)

What is a Data Breach? (That May Trigger State Notification Laws) *cont'd*

- That has caused or is likely to cause loss or injury to resident (MI)
- That causes or is reasonably likely to cause substantial economic loss to the individual (AZ)
- Unless no reasonable likelihood of financial harm to consumer whose PII was acquired has resulted or will result (IA)

Why We Should be Careful with the Word “Breach”

- Using “breach” to describe a data-privacy related incident assumes the incident meets the definition of a security breach which triggers various notification requirements
 - Be careful to notify the correct person/entity
- An “incident” does not always rise to the level of “breach” (i.e., encryption safe harbor)
- “Incident” is better received by the public than “breach”

Breach Notification Laws

State laws differ with respect to:

- Deadline for notifying (14, 30, 45 days; reasonable time)
- Notification to Attorney General
- Notification to other State agencies
- Including Attorney General contact information
- Substitute notice (email, website, media)
- Specific facts of incident and type of PII compromised
- Maintaining records of incident (for 3-5 years)
- Countries also differ with notice requirements

Other Data Breach Requirements

- HIPAA requires covered entities to provide notification of the breach to affected individuals the government, and in certain circumstances, the media
- SEC cybersecurity regulations require public companies to disclose material cybersecurity incidents they experience and to disclose on an annual basis material information regarding their cybersecurity risk management, strategy and governance
- Financial institutions are required to report cybersecurity incidents to the Federal Deposit Insurance Corporation, the Federal Reserve Board, and the Comptroller of the Currency within 36 hours

Standing for Data Breach Purposes

- The Supreme Court in *Ramirez v. TransUnion*, 136 S. Ct. 1540 ruled in June 2021 that victims of a data breach may not have Article III standing unless they suffered “concrete” harm from the breach
- Mere violations of a statute, even a statute which provides a private right of action, may not be sufficient for Article III standing in federal litigation
- The Second Circuit recently ruled in *Stevens v. Carlos Lopez* that the increased risk of identity theft alone may not establish standing either but will depend on the facts of each particular case, and held that there was no circuit split (foreclosing a ripe opportunity for Supreme Court review of the issue)

Artificial Intelligence

Existing US Laws and Regulations

Most US regulation is in the space of “automated decision-making” or “profiling” features, which are a subset of artificial intelligence

- The CPRA, the Colorado Privacy Act, the Virginia Consumer Data Protection Act, and the Connecticut Data Privacy Act all grant consumers rights regarding opting out of the processing of their personal information for purposes of profiling and create requirements that impact automated decision-making
- These laws require data controllers to conduct a data protection impact assessment (DPIA) for processing activities which present a “heightened risk of harm to a consumer”
- Also, laws such as the Illinois Artificial Intelligence Video Interview Act, which requires employers to disclose the use of an AI tool to analyze video interviews of applicants for positions based in Illinois
 - New York City’s AI Law (Local Law 144) regulates employer use of automated employment decision tools in hiring and promotions

International Aspects

GDPR and the Shrems II Decision

- 2020 decision from the Court of Justice of the European Union
- Invalidated the US-EU Privacy Shield
- Closes off key mechanisms for transferring personal data from the EU to the US
- Shrems I invalidated European Commission adequacy decisions with respect to EU-U.S. Safe Harbor

GDPR and the Shrems II Decision *cont'd*

- CJEU was concerned with US government access to personal data for national security purposes and the rights of EU citizens in the US to judicial review and redress
 - CJEU found the U.S. was not according EU personal data the protection and rights of redress available in the EU
- In June 2021, the European Commission adopted two sets of modernized Standard Contractual Clauses to allow for international data flows consistent with the decision

EU-US Data Transfers Currently

- The EU and US were in talks for years to create a replacement for Privacy Shield, finally agreeing on the E.U.-U.S. Data Privacy Framework
 - On July 10, 2023, the European Commission deemed the E.U.-U.S. Data Privacy Framework adequate, finding that the enhanced protections for EU individuals under President Biden's Executive Order 14086 and the Data Privacy Framework offer an adequate level of protection for personal data transferred from the EU to the US
 - Questions remain about how organizations transfer their data after implementing standard contracts and other mechanisms to comply
 - Companies can self-certify their compliance using a website established by the US Department of Commerce

American Data Privacy and Protection Act

- American Data Privacy and Protection Act – introduced in both the House and the Senate in June 2022 with bipartisan support
- Provisions for: enhanced children's protections, limits on targeted advertising, preemption over facets of state laws, and a limited private right of action
- Also mandates a chief privacy officer position for organizations and imposes data minimization requirements
- FTC would be charged with enforcement of its provisions

Recommended Reading

- [How the GDPR Set a New Standard for Data Privacy and Protection in the EU and America](#)
- [When Collecting Personal Data, Restraint and Insurance are Key](#)
- [How Threat-Savvy Companies Can Defend Against Data Breaches](#)
- [Reasonable Measures in Cybersecurity: Guidelines for Breach Prevention and Response](#)

Questions or Comments?

If you have any questions about this webinar that you did not get to ask during the live premiere, or if you are watching this webinar [On Demand](#), please do not hesitate to email us at info@financialpoise.com with any questions or comments you may have. Please include the name of the webinar in your email & we will do our best to provide a timely response.

IMPORTANT NOTE: The material in this presentation is for general educational purposes only. It has been prepared primarily for attorneys & accountants for use in the pursuit of their continuing legal education & continuing professional education.

*** These slides were produced in connection with a video webinar that premiered on [9/4/2025](#). Take note, we make the PDF available for free download because the real benefit of a Financial Poise webinar is the conversation that the faculty has around the slide deck. You can access the webinar on-demand at Cerfi's LegalEdge (f/k/a [West Legal Ed Center](#)) (for attorneys or accountants seeking CLE or CPE) or [Financial Poise](#) (for everyone else).

Meet The Faculty

Gary Chodes - gchodes@natlawreview.com



Gary is currently the CEO of the National Law Review and its parent publisher the Daily DAC. The National Law Review is a Top Ten online legal and business news and information source with a 100+ year history. A serial entrepreneur having founded multiple successful legal-tech, legal services and on-line lending businesses, Gary has experienced several notable exits to private equity firms, insurance companies and publicly-traded strategic buyers.

Gary previously served as the CEO of American Consumer Lending (ACL), an affiliate of Prospect Capital Corp (NYSE: PSEC), one of the largest purchasers of consumer and small business loans originated by leading on-line originators, such as Lending Club, Prosper and OnDeck. ACL's aggregate loan portfolio at 6/30/2015 exceeded \$500 million.

Gary also built and ran a number of legal-tech and legal services businesses from 1993 to 2018. Several of the brands and companies he was associated with during that time period were the Legal Recovery Fund, Signal Funding, Pegasus, Disability Corner and Viaticus.

Investors and lenders to these businesses included some of the largest financial institutions in the world, such as CNA Insurance, Deutsche Bank, Fifth Third Bank, Fortress Investments, Highbridge Investments and HIG Capital.

Gary holds a B.S. in Economics from the Wharton School at the University of Pennsylvania and an M.B.A. from the Kellogg School of Management at Northwestern University. [Read More](#)

Kathryn (Katie) Nadro - knadro@lplegal.com



Kathryn (Katie) Nadro is a partner in the firm's Corporate Group, advising clients on cybersecurity and data privacy matters.

A Certified Information Privacy Professional (CIPP/US), Katie helps clients navigate various data security and privacy issues. She assists clients with policy drafting, program management, and data collection. She also advises clients on best practices for compliance with evolving state, federal, and international data protection laws.

If a data breach occurs, Katie guides clients through the breach response process and relies on her previous litigation experience to advise clients through any potential legal claims or regulatory investigations.

With previous experience as in-house counsel, Katie understands and is attuned to her clients' business objectives.

[Read more](#)

Alex Sharpe - alex@sharpe LLC.com



Alex Sharpe is a long-time Cybersecurity, Governance, and Digital Transformation expert with real-world operational experience. He has spent much of his career helping corporations and government agencies reap the rewards afforded by advances in technology while mitigating risk.

He began his career at the NSA before moving into the Management Consulting ranks building practices at Booz Allen and KPMG.

He subsequently co-founded two firms with successful exits, including The Hackett Group. Alex holds degrees in Business from Columbia Business School, Systems Engineering from Johns Hopkins University, and Electrical Engineering from New Jersey Institute of Technology (NJIT).

He is a published author, speaker, instructor, and advisor.

Thank you to our co-producer

THE NATIONAL LAW REVIEW

The National Law Review (NLR) is a premier legal news website offering in-depth analysis on a wide range of legal and business topics. Established in 1888, NLR has evolved into a **trusted resource** for legal professionals, business leaders, and the general public, providing timely and relevant information on legislative changes, court decisions, and regulatory developments

Visit *The National Law Review* to learn more
- <https://natlawreview.com/>

Comprehensive Coverage: NLR covers nearly every legal topic, including litigation, AI & the Law, employment law, IP Law, real estate, energy, health care, bankruptcy and much more.

Expert Analysis: Articles are authored by experienced attorneys and legal professionals, ensuring accurate and insightful commentary.

Daily Updates: NLR provides hourly legal news updates, keeping readers informed about the latest developments in the legal world.

About Financial Poise



The primary mission of Financial Poise™ is to provide reliable plain English business, financial, & legal education to individual investors, entrepreneurs, business owners, & executives, & to help trusted advisors do the same.

*Newsletter subscribers are occasionally offered free webinars. Subscribers never receive more than one email per week & their information is never shared.

Sign up for our free weekly e-newsletter [here](#)*.

Learn how to write or speak for Financial Poise [here](#).
The antithesis of “pay-to-play.”

Check out our other webinars [here](#).

Send any other inquiry to info@financialpoise.com