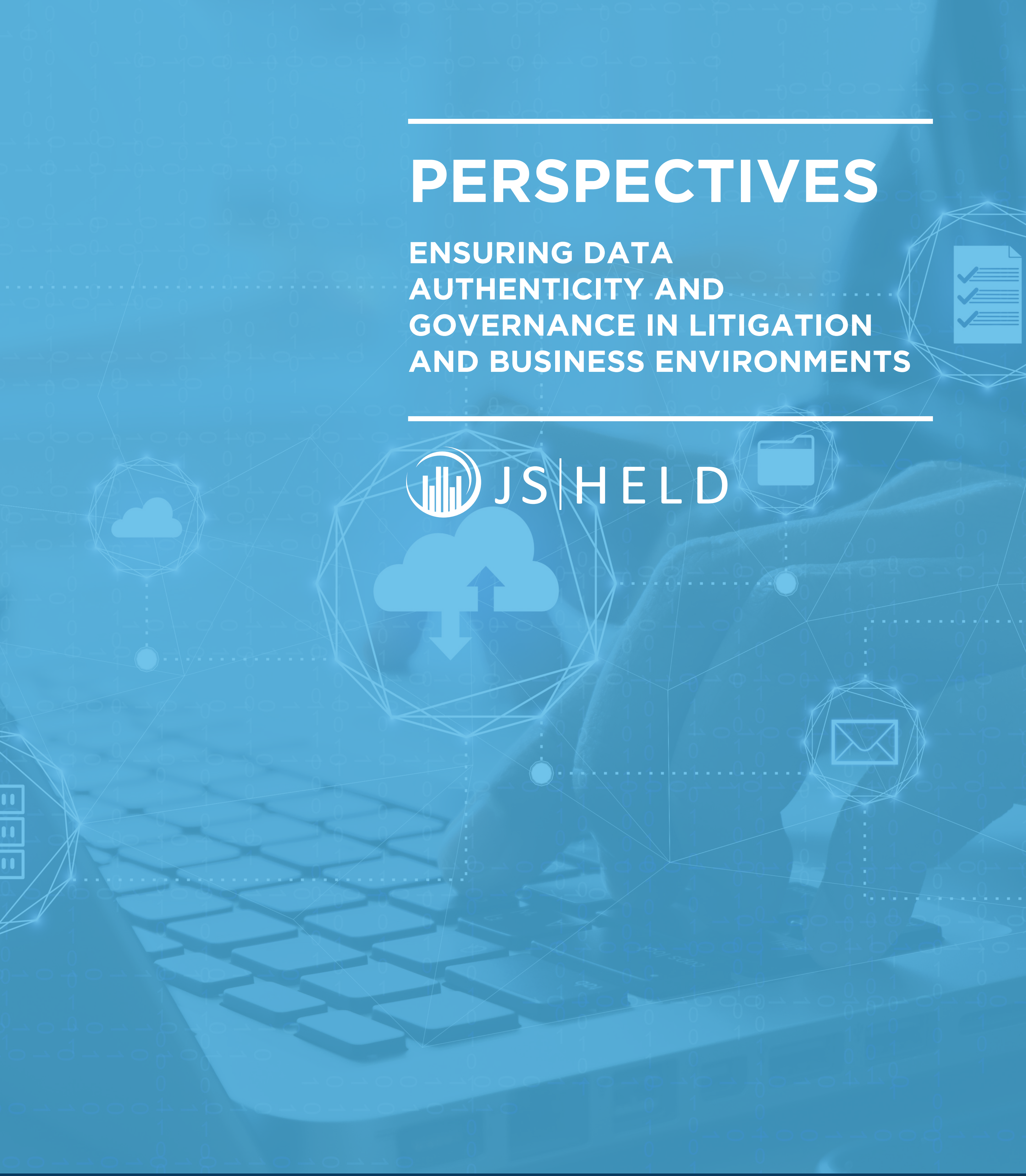

PERSPECTIVES

ENSURING DATA AUTHENTICITY AND GOVERNANCE IN LITIGATION AND BUSINESS ENVIRONMENTS

Our perspectives feature the viewpoints of our subject matter experts on current topics and emerging trends.

thebrief™ | JS|HELD

Insurance professionals should read this article to:

- Understand the growing risks of data manipulation and fraud schemes
- Learn why Artificial Intelligence (AI) technologies require robust governance frameworks and proactive risk management
- Explore examples of liability arising from inaccurate AI-generated content

Legal advisors should read this article to:

- Assess liability risks tied to AI-generated misinformation
- Examine evolving global data privacy regulations
- Understand strategic approaches to data authentication and intellectual property (IP) protection

Executive Summary

As digital interdependence and geopolitical fragmentation grow, ensuring data authenticity, security, and regulatory compliance is more crucial than ever. Trust in data has eroded due to the opaque nature of artificial intelligence (AI) systems, varying regulatory regimes, and governance gaps, reinforcing a critical need for transparency and accountability. J.S. Held's multidisciplinary expertise in forensic analysis, intellectual asset management, and global regulatory frameworks equips clients to mitigate risk, protect proprietary data, and unlock strategic value. In doing so, it offers a roadmap for ensuring that data is authentic and reliable for litigation purposes, meets various compliance standards, and is protected as intellectual property.

EXPERT VOICES

Greg Campanella, CLP

Greg applies his expertise focused on strategic advisory and the valuation of intangible assets and intellectual property to inform this article.

Ken Feinstein

Ken draws on his expertise in investigative data analytics to address how organizations can strengthen data authenticity, mitigate fraud risks, and implement governance frameworks in the age of AI.

Introduction

Ensuring data authenticity, security, and regulatory compliance is more crucial than ever as digital interdependence and geopolitical fragmentation continue to grow. Structured data has become highly valued in the digital world, and accordingly, the risk of data manipulation and related fraud has increased. Artificial intelligence ("AI") has enabled threat actors such as terrorist groups and cybercriminals to create deepfakes and more easily gain access to environments that hold sensitive personal information. While methods existed to make fake data appear authentic before the advent of AI, new technologies have made it harder to distinguish between real and deceptive data.

Some common types of data authentication fraud schemes include:

- Account Takeover
- Business Email Compromise

- BYOD (Bring Your Own Device) and Departing Employee Programs
- Cookie/Tracking Pixel Consent & Compliance Management
- Falsifying Electronic Documents
- Healthcare, where billing is conducted for unprovided services and medical identity theft
- Legal Hold Procedures, where the preservation of data and documents is compromised
- Off-Channel Communications, where texts, personal emails, and other social media are at risk for fraud and insider trading in cases where the communications have bypassed company monitoring and recordkeeping
- SIM Swap
- Synthetic Identity

The consequences of data integrity failures can be severe: costly investigations, litigation, reputational damage, and operational disruptions.

AI Inaccuracies, Corporate Liability, and Why Governance Matters

These risks are not theoretical. For example, consider a Canadian case in which a passenger used a chatbot on an airline's website and received inaccurate information. The chatbot conveyed that bereavement fares could be applied retroactively. Relying on that representation, the passenger purchased a ticket. Subsequently, airline personnel informed him that retroactive applications were not permitted. Based on this discrepancy, the passenger sought a partial refund. In response, the airline asserted before the civil resolution tribunal that the passenger had failed to follow the prescribed procedure for bereavement fare requests and was therefore ineligible for the fare reduction. The airline further contended that it bore no responsibility for information provided by its chatbot.

The tribunal ordered the airline to issue a refund to the passenger who relied on inaccurate bereavement fare information provided by its chatbot, ruling: "It should be obvious to [the airline] that it is responsible for all the information on its website. It makes no difference whether the information comes from a static page or a chatbot." This case illustrates how companies can be held liable for their interactions with customers using AI technology. It also demonstrates that companies must have experts with a wide range of capabilities — from proficiency in economic damages and valuation to specialization in information governance, as well as experience in managing litigation and disputes.

Given these risks, authenticating electronically stored and transmitted information is crucial, particularly for companies with cross-border operations, complex supply chains, or significant financial exposure. To mitigate these risks, companies can establish robust internal governance policies, implement proactive privacy and security protocols, and ensure employees are aware of emerging threats and historical methods of information manipulation.

AI Compliance Frameworks & the Future of Data Governance

While AI can accelerate product development, companies that fail to properly test AI-generated products and services face heightened risks. AI code generation models, for example, may offer speed and efficiency, but they also introduce risks ranging from cybersecurity exposure to the amplification of biases embedded in their training data.

These risks aren't limited to startups. AI agents — also known as agentic AI — are transforming decision-making and automation for large companies as well. Cloudera, an AI platform provider, conducted a global survey of nearly 1,500 information technology decision-makers across 14 countries in various sectors. The survey identified key challenges to adopting AI agents, including concerns about data privacy, integration into existing systems, high adoption costs, a lack of technological expertise, ethical and regulatory issues, and governance concerns.

83% of organizations believe it's important to invest in AI agents to maintain a competitive edge within their industry.
(Source: Cloudera)

Compliance Challenges in a Fragmented Regulatory Landscape

The General Data Protection Regulation (GDPR) must be considered by all organizations that do business in Europe. Since its implementation in 2018, the primary goal of GDPR has been to protect the personal data and privacy of individuals within the European Union.

However, the European Commission (EC) is currently debating a "Digital Omnibus" package that would streamline rules on AI, cybersecurity, and data. The package rewrites EU privacy laws and is estimated to save companies 5 billion euros in administrative costs by simplifying compliance.

For the GDPR, the EC says the omnibus package proposes to modernize cookie rules. It also aims to simplify certain obligations for businesses and organizations "by clarifying when they must conduct data protection impact assessments and when and how to notify data breaches to supervisory authorities."

Currently, GDPR enforcement varies across countries. Companies may engage outside counsel and consultants to understand jurisdiction-specific policies and regulations. This is critical for developing governance frameworks and managing data as a business asset, including determining where it resides within a company's infrastructure and whether it may trigger local or regional laws. At a minimum, companies should adhere to the high privacy and security standards mandated by the GDPR, ensuring data is encrypted and secure.

Furthermore, the EC is proposing amendments to the EU's Artificial Intelligence Act. Those amendments will include simplified technical documentation requirements for small and medium-sized enterprises. An amendment would also ease compliance measures, allowing innovators to use regulatory sandboxes. The EC also notes that the omnibus package will introduce "a single-entry point where companies can meet all incident-reporting obligations. Currently, companies must report cybersecurity incidents under several laws, including, among others, the NIS2 Directive, the General Data Protection Regulation (GDPR), and the Digital Operational Resilience Act."

In contrast, the US has not enacted a comprehensive federal data privacy law. Instead, state-level and sector-specific laws on the federal level, such as the Health Insurance Portability and Accountability Act (HIPAA), have been enacted to protect personal health-related information.

25 privacy and data security laws have been enacted to protect California residents, such as the California Consumer Privacy Act (CCPA). Additional states that have enacted privacy and data security laws include Colorado, Connecticut, Delaware, Florida, Iowa, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Texas, Utah, and Virginia.
(Source: American Bar Association)

However, the Trump Administration is moving to block the patchwork of state laws regulating AI. In late 2025, the Administration announced an executive order that directs the Attorney General to establish an AI Litigation Task Force to challenge state AI laws that it deems harmful to innovation and create costly compliance requirements. The order specifically calls out California's and Colorado's laws. The EO highlights the Colorado AI Act's prohibition on "algorithmic discrimination" as an example of harmful state overreach, arguing that such provisions compel companies to embed ideological bias and generate false results. California will arguably feel the greatest impact of the EO, as it is home to 33 of the world's highest-grossing privately held AI companies and has enacted more AI laws than any other state. The EO targets California laws that require creators of AI to offer tools to help users identify AI-generated content and mandate high-level transparency regarding the data used to train models.

Currently, to further safeguard data, some states require multi-factor authentication, which has become a preferred and reliable measure of protection. Data privacy and security are critical, but organizations need to first understand what data exists within their environment. During data mapping, legacy data that is no longer needed may be purged to reduce exposure to breaches or attacks. Certain data sets, such as personally identifiable information (PII), financial records, or protected health information (PHI), require higher-level encryption.

As AI plays a growing role in data storage and management, the US Cybersecurity and Infrastructure Security Agency (CISA) issued guidance titled "AI Data Security: Best Practices for Securing Data used to Train and Operate AI Systems." The advisory recommends sourcing data from trusted providers, tracking its provenance, maintaining logs of origin and system flow, and using cryptographically signed provenance databases and digital signatures to ensure integrity and prevent tampering.

Protecting Intellectual Property Through AI Governance Frameworks

AI systems are composed of three foundational components: data, compute, and algorithms. As we discuss in AI as IP™, among the three foundational components of AI, data often stands out as the most fundamental and valuable. High-quality, relevant, and contemporaneous data can significantly reduce reliance on complex algorithms and expensive computer resources. In many cases, data can drive superior AI performance, making it the cornerstone of AI value creation. Viewed through the lens of IP, these foundational components, particularly data, offer unique opportunities for asset recognition, protection, valuation, and monetization.

This is especially relevant, given that data integrity directly supports the value of a company's intellectual property (IP).

Consider that intangible assets currently comprise roughly 90% of the S&P 500's market value. The data and underlying computational power that enable AI to train models, process data, and perform calculations are in high demand and can be protected as trade secrets. Additionally, algorithms that enable AI systems to conduct learning, prediction, or generation of outputs can be protected as trade secrets, copyrights, and patents.

As we discussed in The Need for an Efficient, Market-based Transactional Platform for Licensing Data and Artistic Content in the AI Era, proprietary data requires robust protection, starting with a clear understanding of the data room and continuous monitoring of when and how data exits that controlled environment. While watermarking helps track data, it is only one part of a broader technological ecosystem designed to prevent uncontrolled proliferation. Emerging solutions include the use of secure user-controlled environments that allow data owners to share and license access without transferring or duplicating the underlying asset. These environments enable third parties to perform analysis, validation, or model training within a contained framework, preserving confidentiality and ensuring compliance with use and licensing terms.

This is especially critical during high-stakes transactions such as mergers and acquisitions (M&A), where sensitive data must be validated without direct exposure. In these scenarios, third-party validators can conduct due diligence within secure environments, maintaining data integrity while facilitating commercial engagement. By combining traceability, containment, and controlled access, companies can protect proprietary data while unlocking its full economic potential.

Companies seeking to monetize their data assets should consider hiring an expert who understands both the strategic and technical aspects of data commercialization. Not all data is monetizable, so organizations must be deliberate when selecting which datasets to monetize. Effective governance begins with a clear understanding of the types of data held, how they can be transacted, and the broader implications of those transactions on asset value. Critically, once data is used to train a large language model (LLM), its exclusivity and confidentiality are effectively lost. Moreover, if legally accessed data is used to train an LLM, the resulting transformation may not be protected under copyright law. For finite, one-time-use data, controlling access is critical — once distributed, it is freely available and may no longer be licensable.

To maximize the strategic value of data, companies must implement systems that support both data protection and controlled licensing. Secured data environments can enable data usage without exposing the raw asset, helping prevent proliferation while allowing for monetization. Pricing strategies should reflect whether data is finite, reusable, or sensitive, and account for its market value and distribution risks.

Frameworks

As artificial intelligence reshapes how information is created and shared, the ability to verify data authenticity has become a cornerstone of reliance and compliance. Digital forensics plays a critical role in litigation, regulatory investigations, and corporate transactions, ensuring that evidence and operational data can withstand scrutiny.

With AI tools creating photographic images, documents, and, in some instances, hallucinations, it is critical for those seeking to collect, evaluate, and present data as evidence in litigation to authenticate the origin of the data being relied upon.

Forensic computer images, for example, utilize hash verification techniques to ensure that the information captured is not altered post-imaging. The evolution of AI, resulting in more realistic documents and images, has outpaced early AI-generated content detection tools, rendering them less reliable.

Organizations must therefore adopt a layered approach to authentication, combining forensic validation with corroboration from independent sources and third-party attestations.

This is particularly vital during mergers and acquisitions, where companies inherit not only data but also the governance frameworks or gaps of acquired entities. Assessing inherited privacy, security, and compliance structures, eliminating redundancies, and aligning practices with global standards are critical steps to mitigate risk.

Data Integrity Risk Assessment for Emerging AI Trends

Many organizations struggle with data encryption and the protection of PII and PHI, often due to limited visibility in their data storage.

Misunderstandings, such as mistaking active data for backups, can lead to improper data handling. These foundational issues are increasingly concerning as global data flows become more complex. Although current data flows are structured and traceable, future trends indicate that autonomous AI agents will manage data exchanges, which may complicate oversight. Reflecting this shift, Market.us projects that the global agentic AI market will grow from $7.5 billion in 2025 to $196.6 billion by 2034.

Conclusion

An organization's data is one of its most valuable assets, yet it is one of its most vulnerable. The growing prevalence of AI across industries has introduced new litigation risks and compliance demands, requiring companies to blend innovative and traditional methods for policy development, privacy programs, and regulatory alignment. Furthermore, as organizations integrate AI tools, they should proactively identify areas of potential risk, update existing systems and privacy programs, and ensure alignment with applicable regulatory frameworks, including the GDPR, the CCPA, and other state laws now in effect.

To protect and monetize proprietary data, companies must implement strong governance frameworks that protect IP, shield sensitive information, support regulatory compliance, and build trust with stakeholders. As these efforts converge, one principle remains clear: data authenticity and integrity are the foundation of effective AI deployment and long-term enterprise value.

Acknowledgements

We would like to thank Greg Campanella, CLP, and Ken Feinstein, whose contributions greatly assisted this research.

Greg Campanella, CLP, is a Senior Managing Director and joined J.S. Held in March of 2022 as part of J.S. Held's acquisition of Ocean Tomo. He is responsible for leading the Management Consulting & Valuation practice of Ocean Tomo, a part of J.S. Held. His work has focused on strategic advisory and the valuation of intangible assets and intellectual property for acquisitions and divestitures, bankruptcy and restructuring, establishment of monetization strategies, including licensing, mergers, joint venture/partnership formations, litigation support, and tax matters. He is skilled in the creation of models to both evaluate the economics of alternative spin-out strategies and to establish the value of IP to be contributed in a joint venture.

Greg can be reached at
gregory.campanella@jsheld.com or
+1 415 946 2605.

Ken Feinstein is a Senior Managing Director in the Digital Investigations & Discovery service line within the Global Investigations practice at J.S. Held. He specializes in investigative data analytics and provides investigations, regulatory risk and litigation support solutions spanning multiple sectors, including retail and consumer products, life sciences, technology, financial services, industrial products, and government agencies. His clients include law firms and Fortune 500 legal and compliance teams for whom he delivers large-scale, complex investigations, regulatory response matters, proactive anti-fraud efforts, and compliance programs. He is a member of the American Institute of Certified Public Accountants and the Association of Certified Fraud Examiners.

Ken can be reached at
ken.feinstein@jsheld.com or
+1 917 277 7868.

This publication is for educational and general information purposes only. It may contain errors and is provided as is. It is not intended as specific advice, legal, or otherwise. Opinions and views are not necessarily those of J.S. Held or its affiliates and it should not be presumed that J.S. Held subscribes to any particular method, interpretation, or analysis merely because it appears in this publication. We disclaim any representation and/or warranty regarding the accuracy, timeliness, quality, or applicability of any of the contents. You should not act, or fail to act, in reliance on this publication and we disclaim all liability in respect to such actions or failure to act. We assume no responsibility for information contained in this publication and disclaim all liability and damages in respect to such information. This publication is not a substitute for competent legal advice. The content herein may be updated or otherwise modified without notice.

J.S. Held, its affiliates and subsidiaries are not certified public accounting firm(s) and do not provide audit, attest, or any other public accounting services. J.S. Held is not a law firm and does not provide legal advice. Securities offered through PM Securities, LLC, d/b/a Phoenix IB or Ocean Tomo Investments, a part of J.S. Held, member FINRA/SIPC. All rights reserved.