International Legal Highlights | Spring 2024

Spring, 2024

Julian L. André | Rosa Barcelo | Caitlyn M. Campbell | Edward B. Diskant | James Durkin | Jonathan Ende | Christopher Foster | Paul M.G. Helms | Hon.-Prof. Dr. Henrik Holzapfel | Charles (Chuck) Larsen | Matthew Madden | Romain Perray | Sagar K. Ravi | Paul M. Thompson | Lorraine Maisnier-Boché | Mark E. Schreiber | David Beach | Ashley Hoff | Brian Long | Simon Mortier | Lisa Nassi | Diana Pisani

SUMMARY

DOJ DOUBLES DOWN ON CORPORATE ENFORCEMENT WITH NEW WHISTLEBLOWER PROGRAM

During the 2024 American Bar Association National Institute on White Collar Crime (the 2024 White Collar Conference) earlier in March US Attorney General (AG) Merrick Garland, US Deputy Attorney General (DAG) Lisa Monaco, Acting US Assistant Attorney (AAG) General Nicole Argentieri and other US government officials spoke extensively on the US Department of Justice's (DOJ) heightened corporate enforcement efforts. Building on last year's changes to DOJ's corporate enforcement policies, DOJ will be using a "mix of carrots and sticks" – including a new DOJ-run whistleblower program – to promote corporate compliance, encourage voluntary self-disclosure, and hold individuals and corporations accountable for corporate misconduct.

DAG Monaco and AAG Argentieri unveiled plans for a whistleblower program that will reward individuals who help DOJ uncover significant corporate or financial misconduct. The new whistleblower program will "fill gaps" not covered by existing whistleblower programs and provides DOJ with another tool to encourage companies to enhance their compliance programs and voluntarily self-disclose misconduct. DOJ will use the next 90 days to fully develop its whistleblower program before formally implementing a pilot program.

At the conference, AG Garland, DAG Monaco and others discussed recent DOJ corporate enforcement policy initiatives. DOJ's leadership repeatedly emphasized the substantial financial benefits of voluntary self-disclosure, cooperation and remediation while stressing the importance of accountability for individual wrongdoers and the need to address corporate recidivism. Companies with a history of misconduct can expect to receive harsher financial penalties designed to deliver meaningful consequences.

DOJ officials also discussed a number of ongoing DOJ enforcement priorities, including artificial intelligence (AI), cryptocurrency, data protection and sanctions. DOJ cautioned that criminal deployment of AI will result in prosecutors seeking stiffer penalties and highlighted an increasing connection between corporate enforcement objectives and American national security interests related to the protection of sensitive data.

IN DEPTH

DOJ's New Whistleblower Pilot Program

The headline from the 2024 White Collar Conference is DOJ's new whistleblower program. DAG Monaco and AAG Argentieri announced that DOJ will use the next 90 days to develop and implement a DOJ-run pilot whistleblower program, which is expected to start later this year. If an individual helps DOJ discover misconduct that was otherwise unknown to DOJ, then the whistleblower can qualify for a monetary share of any resulting civil or criminal forfeiture action.

By implementing its own whistleblower program, DOJ is hoping to emulate the success of other whistleblower programs, which have become "indispensable" for many federal agencies. For example, in 2023, the US Securities and Exchange Commission's (SEC) Whistleblower Program received more than 18,000 tips and awarded nearly $600 million to whistleblowers. The Commodity Futures Trading Commission's (CFTC) Whistleblower Program has resulted in enforcement actions leading to more than $3 billion in financial penalties in the past decade.

DOJ's whistleblower program is meant to "fill gaps" and proactively address misconduct that existing federal whistleblower programs do not already cover. In particular, DOJ is focused on criminal abuses of the US financial system, foreign corruption matters outside the jurisdiction of the SEC and domestic corruption matters involving bribes to government officials. DOJ also appears to be heavily focused on privately-owned companies. As examples of cases that would fall within DOJ's new whistleblower program, DAG Monaco referenced the chief financial officer of a private equity firm forging loan documents or a private technology startup paying bribes to obtain regulatory approvals.

DAG Monaco and AAG Argentieri also made clear that DOJ's whistleblower program is designed to drive companies to voluntarily self-disclose misconduct and to do so quickly. Whistleblowers can only obtain an award by providing original information, and companies can only obtain the benefits of DOJ's voluntary self-disclosure program if they are "first in the door." As DAG Monaco explained, "[w]hen everyone needs to be first in the door, no one wants to be second." DOJ expects these "incentives to reinforce each other and multiplier effect, encouraging both companies and individuals to tell us what they know as soon as they know it."

DAG Monaco and AAG Argentieri said DOJ will offer payments to whistleblowers under the following conditions:

- Only after all victims have been properly compensated
- Only to those who submit truthful information not already known to the government
- Only when the information is provided voluntarily and not in response to any government inquiry, preexisting reporting obligation or imminent threat of disclosure
- Only to those not involved in the criminal activity itself
- Only in cases where there is not an existing financial disclosure incentive – such as a qui tam or another applicable federal whistleblower program

Other key details of the forthcoming whistleblower program, however, have yet to be developed or announced. DOJ provided no information regarding the range of potential whistleblower awards, the criteria for determining the amount of a whistleblower award, or who will be ultimately responsible for determining whether an individual is entitled to a whistleblower award. Until these additional details are known, it is difficult to predict whether the program will have a meaningful impact on corporate enforcement going forward.

DOJ's 'Carrots and Sticks' Approach to Corporate Enforcement

Throughout the 2024 White Collar Conference, DOJ officials spoke extensively about DOJ's ongoing corporate enforcement efforts and policies. AG Garland, DAG Monaco and other officials repeatedly emphasized the need to hold both individuals and corporations accountable for misconduct, while encouraging companies to invest in a culture of compliance and voluntarily self-disclose any misconduct. To achieve these goals, DOJ continues to implement what it refers to as a "carrots and sticks" approach to corporate enforcement.

The "sticks" include aggressive prosecution of the most serious individual and corporate wrongdoers and significant consequences for corporate recidivists. AG Garland noted that DOJ's "first priority in the area of white collar crime is going after individual bad actors." He explained that the "greatest deterrence to white collar crime is fear of individual prosecutions of executives." DAG Monaco and AAG Argentieri then emphasized convictions DOJ has recently obtained against individual corporate executives, including the convictions of FTX's CEO Samuel Bankman-Fried and Binance's CEO Changpeng Zhao. DAG Monaco, AAG Argentieri and other officials also spoke repeatedly about the need to address corporate recidivism, with increased financial penalties for companies with a history of past misconduct.

As for the "carrots," DAG Monaco highlighted the benefits of DOJ's voluntary self-disclosure (VSD) programs, touting the single corporate VSD policy for all US Attorney's Offices nationwide that was rolled out last year. Voluntary self-disclosure remains at the core of DOJ's corporate enforcement efforts. DAG Monaco's mantra for corporations that discover misconduct is to "step up and own up," encouraging disclosure first and foremost if they desire the most beneficial treatment considerations, including declination, non-prosecution agreements and deferred prosecution agreements, and substantially reduced monetary penalties. She, however, noted that even if

DOJ discovers misconduct in the absence of company disclosure, cooperation and remediation remain valuable considerations for DOJ in the process of resolution.

DOJ believes its "carrots and sticks" approach is working. AAG Argentieri noted that DOJ has already seen "substantial year-over-year increases in disclosures" from companies to DOJ's fraud section, with nearly twice as many disclosures in 2023 as in 2021.

DOJ's Current Enforcement Priorities

AG Garland, DAG Monaco and other officials also discussed a number of ongoing DOJ's enforcement priorities. In addition to traditional financial crimes, government officials repeatedly referenced AI, cryptocurrency, data security and sanctions.

DOJ and other government officials focused heavily on AI throughout the 2024 White Collar Conference. AG Garland observed that AI demonstrates great promise, but it has evolved with equally great risk, particularly in accelerating cyberattacks, advancing fraud and enhancing national security threats. DOJ will be hiring experts in computer science and technology to address AI capabilities and enforcement concerns. DAG Monaco also noted that federal prosecutors will seek penalty enhancements if AI is used to further criminal activity.

Assistant Attorney General for National Security, Matthew Olsen, emphasized the importance of sensitive data security as a crucial measure to protect US national security interests. Citing President Joe Biden's recent Executive Order that grants authority to DOJ to issue regulations to strengthen security protections for Americans' bulk sensitive data, including personal, health and financial data, AAG Olsen encouraged companies to have a clear understanding of the data that they have collected for their businesses and how it is safeguarded, where that data is being transmitted, who has access to the data, and where the data will potentially be shared, through sales or otherwise.

AAG Olsen also noted that corporations "are on the front lines when it comes to enforcing critical national security tools, like sanctions and export controls." AAG Olsen said that the National Security Division has more than "doubled the number of prosecutors working on sanctions, export control, and foreign agent laws" and "brought on two veteran prosecutors to serve as the division's first ever chief and deputy chief counsel for corporate enforcement."

DOJ and other government agencies remain focused on fraud involving cryptocurrency. As noted above, AAG Argentieri highlighted the recent FTX and Binance convictions. And SEC's Director of Enforcement, Grubir Grewal, and CFTC's Director of Enforcement, Ian McGinley, both addressed their agencies' ongoing enforcement efforts regarding cryptocurrency.

KEY TAKEAWAYS

- DOJ is aggressively encouraging companies to voluntarily self-disclose misconduct and to do so at the earliest possible opportunity. DOJ clearly expects the threat of increased whistleblower activity to further pressure companies to voluntarily self-disclosure misconduct.
- While the new whistleblower program underscores DOJ's efforts to incentivize self-disclosure, it is unclear whether the program will have a meaningful impact on enforcement. Rewards will only be available to individuals with no involvement in the alleged misconduct and only after all victims have been paid. These limitations could substantially reduce the financial incentives for potential whistleblowers to come forward and report wrongdoing.
- Companies that do not voluntarily self-report misconduct should expect DOJ to seek harsher financial penalties going forward. Throughout the 2024 White Collar Conference, government officials explained that financial penalties cannot become "the cost of doing business" and noted that increased penalties may be necessary to deter future misconduct.
- A well-designed and robust corporate compliance program is critical in the current enforcement environment, where DOJ is actively encouraging whistleblowers to come to DOJ first. Companies should ensure that their compliance programs are designed to proactively identify misconduct which is then investigated and remediated so that self-disclosure is at least an option.
- dOJ increasingly views corporate enforcement as a national security issue. Companies can expect DOJ to continue to focus on sanctions and export control violations.
- DOJ recognizes both the promise and perils of AI. DOJ officials expressed growing concern about the use of AI to commit sophisticated financial fraud, as well as cybercrimes that manipulate data and threaten national security interests. If AI is uncovered as part of corporate misconduct, federal prosecutors are likely to pursue enhanced penalties. Companies should continuously monitor fraud prevention strategies and data security protocols to identify and address evolving risks associated with disruptive technologies like AI.

[redacted]

[redacted]2024[redacted]2024[redacted]DOJ[redacted]DOJ[redacted]DOJ[redacted]DOJ[redacted]

[redacted]DOJ[redacted]DOJ[redacted]90[redacted]

DOJ DOJ

DOJ AI DOJ DOJ AI

DOJ

2024 DOJ DOJ DOJ 90 DOJ

DOJ 2023 SEC 1 8000 6 CFTC 10 30

DOJ DOJ SEC DOJ DOJ CFO

DOJ DOJ DOJ DOJ DOJ

DOJ

- Qui Tam
- DOJ

DOJ

2024DOJDOJDOJ

DOJ

DOJFTX-CEOBinanceCEODOJ

DOJVSDVSDOJDOJDOJDOJ

DOJDOJ2023202122

DOJ

DOJAI

DOJ2024AIAIDOJAI

AI

DOJ

[illegible]2[illegible]2[illegible]

DOJ[illegible]FTX[illegible]SEC[illegible]CFTC[illegible]

[illegible]

- DOJ[illegible]DOJ[illegible]
- [illegible]DOJ[illegible]
- [illegible]DOJ[illegible]2024[illegible]
- [illegible]DOJ[illegible]DOJ[illegible]
- DOJ[illegible]DOJ[illegible]
- DOJ[illegible]AI[illegible]DOJ[illegible]AI[illegible]AI[illegible]AI[illegible]

THE AI ACT: THE EU'S BID TO SET THE GLOBAL STANDARD FOR AI REGULATION

In a groundbreaking move, the European Union has launched its bid to set the new comprehensive standard for the regulation of artificial intelligence (AI) with the European Parliament passing the EU AI Act on March 13, 2024. This pioneering legislation, set to come into effect in the coming years, ushers in a new era in AI regulation and stands as a testament to the EU's commitment to ensuring a subtle balance between safe, ethical, and innovative use of AI.

In this article we will first explore the **eleven key aspects of the EU AI Act**, offering an in-depth look at its broad scope and essential requirements, including its interplay with the EU General Data Protection Regulation (GDPR), and how businesses can leverage their existing GDPR compliance programs to meet the EU AI Act's requirements.

We will then dive into **five key takeaways** focusing on the key points and actionable steps you can take to navigate the evolving landscape of AI regulation and the EU AI Act in particular.

IN DEPTH

Eleven Key Aspects of the EU AI Act

The EU AI Act introduces several pivotal provisions that will significantly impact the regulatory framework of AI. Most significantly these include:

1. Broad Scope and Specific Exclusions: The EU AI Act is intended as a horizontal regulation and provides a comprehensive definition of AI systems, applicable to a wide array of applications in sectors such as healthcare, finance, public administration, and consumer technologies. Drawing from the OECD's definition, the Act describes an AI system as "*a machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments*". As inclusive as the GDPR in order to ensure the highest level of protection possible, this definition aims to encompass the diversity in AI systems' levels of autonomy and adaptability after their initial deployment.

At the same time, the Act makes it clear that it does not apply to areas outside the scope of EU law, including national security and defense, and excludes AI models and systems used solely for research, innovation, or for non-professional purposes.

2. Extraterritorial Effect: The AI Act will apply not only within the EU but also to entities outside its borders. This includes non-EU providers placing AI systems or models on the EU market, those putting AI systems into service within the EU, and cases where the output of an AI system located outside the EU is used within its borders. In this respect, the AI Act aligns with both GDPR and the other acts included in the new EU digital package that it belongs to, although with quite a special angle notably as the only one directly governing technologies in contrast with the others which merely focus on data usage.

3. Risk-Based Approach: The Act employs a structured, risk-based approach to AI regulation, organizing AI systems into four categories based on their potential risk levels: Prohibited AI, High-Risk AI, Risk AI, and Minimal Risk AI. This system ensures that stricter regulatory measures are applied to AI applications with higher potential risks, particularly those used in critical areas such as healthcare or infrastructure. Conversely, AI systems with minimal risk are subject to less rigorous requirements. This tiered model is designed to balance the necessity of safeguarding user safety and privacy rights with the goal of fostering innovation in lower-risk AI technologies.

4. Prohibited AI and Law Enforcement Exemptions: The EU AI Act sets clear boundaries by prohibiting certain AI applications that pose risks to privacy, ethics, and fundamental rights. Again following the GDPR quite closely these include:

- **Subliminal Techniques**: The use of manipulative or deceptive techniques that significantly distort behavior and impair informed decision-making.
- **Exploiting Vulnerabilities**: AI systems that exploit vulnerabilities related to age, disability, or socio-economic circumstances.
- **Biometric Categorization**: Systems inferring sensitive attributes from biometric data, such as racial or ethnic origin, political opinions, religious beliefs, or sexual orientation.
- **Social Scoring**: Evaluation or classification of individuals based on social behavior or personal characteristics, leading to detrimental treatment of individuals.
- **Predictive Policing**: Assessing the risk of an individual committing criminal offenses based solely on profiling or personality traits.
- **Facial Recognition Databases**: Compiling databases through untargeted scraping of facial images from the internet or CCTV footage.
- **Emotion Inference**: Inferring emotions in workplaces or educational institutions, except for AI systems used for medical or safety reasons.

In the context of law enforcement, the Act generally restricts the use of real-time biometric identification in public spaces, allowing it only under limited, pre-authorized circumstances.

5. High-Risk AI Systems and Key Requirements: The EU AI Act identifies high-risk AI systems as those critical to sectors such as healthcare, transportation, HR management, education, essential public services, and systems influencing democratic processes. It categorizes these into two main groups:

- **Annex II Systems**: AI systems acting as safety components of products or as standalone products, which are subject to EU laws already requiring a conformity assessment. These are typically associated with high-risk and regulated products (medical devices, machinery, protective equipment, etc.).
- **Annex III Systems**: AI systems designed for specific purposes such as biometrics (excluding banned types), critical infrastructure, educational and vocational training tools, employment and workers' management systems, essential services access (including credit scoring and insurance pricing), law enforcement, migration and border control, and the administration of justice and democratic processes.

The Act mandates comprehensive obligations for providers and deployers of these systems, covering governance measures and technical interventions necessary from the design stage through the entire lifecycle. This includes ensuring CE marking, transparency, accountability, technical documentation, data governance, human oversight, and maintaining accuracy, robustness, and cybersecurity. Providers of these systems will have to report serious incidents to market surveillance authorities.

Despite recent efforts to refine the scope and introduce exemptions for certain AI systems, ambiguities in

classification remain. To address this, companies are advised to maintain high governance standards for all AI systems in use. The EU Commission will provide further classification guidelines within 18 months of the Act's entry into force, aiming for clarity and consistency in high-risk AI system regulation.

Interestingly, the AI Act also allows, where strictly necessary and under additional conditions, the processing of special categories of personal data, such as ethnicity, for the purpose of ensuring bias detection and correction in relation to high-risk AI systems. As feeding such systems, this processing will also remain subject to the GDPR, under which it will be allowed for purposes of substantial public interest within the meaning of Article 9(2)(g).

6. Limited/Minimal Risk AI: Under the EU AI Act, AI systems categorized at the lower risk level are subject to specific transparency and identification requirements. This primarily targets AI technologies that engage directly with users, mandating that any synthetic content produced—be it audio, visual, or textual—must be clearly labeled in a way that machines can recognize as artificially created or altered. Providers are responsible for the efficacy, compatibility, and dependability of these labeling mechanisms. Additionally, the Act imposes obligations on AI functionalities like emotion detection, biometric sorting, AI-generated content, deep fakes, or the alteration of significant textual content to ensure they are transparently marked and made detectable to uphold transparency and prevent misinformation. Regarding Generative AI applications specifically, individuals must be clearly informed when they are interacting with such as chatbots and content generation tools. For AI systems deemed to pose minimal risk, the Act envisages the adoption of voluntary best practices through future codes of conduct.

7. General Purpose AI: The EU AI Act introduces specific requirements for General Purpose AI (GPAI) Models, generally known as Foundation Models, which are defined as those "capable to competently perform a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications". GPAI was not expressly considered in the initial draft AI Act, while the risk-based approach based on the AI intended purposes and applications created the risk of leaving underlying foundation models uncovered. GPAI became a bone of contention, discussed until the last stages of negotiation of the Act, because of the specific risks it presents for users' fundamental rights and safety. The Act thus focuses on GPAI transparency and accountability. All GPAI models, such as those used for broad applications, are required to provide extensive technical documentation, summaries of training data, and adhere to copyright and intellectual property safeguards. Models released under open-source license are considered as already insuring high levels of transparency and benefit from exemptions. For high-impact GPAI models, i.e., that pose systemic risks, the Act mandates additional stringent requirements, including thorough model evaluations, comprehensive risk assessments, adversarial testing, and incident reporting.

8. Innovation-Friendly Ecosystem: To nurture innovation, the Act introduces measures such as regulatory sandboxes and provisions for real-world testing. These initiatives intend to benefit SMEs and startups, offering them the flexibility to experiment and refine their AI systems within a controlled environment before wider deployment.

This approach recognizes the dynamic nature of AI development and seeks to provide a supportive ecosystem for emerging AI innovations.

9. The interplay between the EU AI Act and the GDPR: AI systems that process personal data will be subject to both the GDPR and the EU AI Act (and respective fines in case of violations). Both acts lay down some requirements that have strong commonalities. A key question is whether it is possible to leverage compliance efforts, and if so, how. For instance, under the GDPR, data controllers are required to carry out a data protection impact assessment (DPIA) in certain circumstances, whereas under the EU AI Act, providers/users of high-risk AI systems have to carry out DPIAs, which, among others, need to consider privacy risks. In line with the effective explainability and transparency principles – which are the cornerstones of trustworthy AI systems – the EU AI Act imposes requirements to inform individuals when they interact with AI systems (e.g., chatbots and content generation tools).

10. Penalties and Enforcement: The EU AI Act establishes a comprehensive framework for penalties and enforcement. Fines for violations are scaled, with up to 7% of global annual turnover or EUR 35 million for prohibited AI violations, up to 3% for other breaches, and up to 1.5% or EUR 7.5 million for supplying incorrect information, including specific caps for SMEs and startups. Enforcement will be coordinated through a newly established central 'AI Office' and 'AI Board' at the EU level, complemented by market surveillance authorities in each EU country, ensuring a balanced and effective application of the Act across all member states.

11. Entry into force: The AI Act will start applying gradually: prohibited AI will be banned six months from the Act entering into force, while the Act will start applying to GPAI one year after entry into force; two years for high-risk AI systems of Annex III and three years for high-risk AI systems already covered by other EU regulations mandating a third-party conformity assessment.

Five Takeaways on the EU AI Act

The above compilation of key aspects is intended to serve as a useful starting point to inform proactive steps legal and compliance managers as well as DPOs can take to position their companies and their teams for success. Below, we are sharing five key takeaways for businesses to prepare for the rapidly evolving risks and challenges posed by AI:

1. Comprehensive Impact Assessment and Compliance Evaluation: Businesses should conduct a thorough assessment to understand how the AI Act will affect their operations. This evaluation should cover not just mapping and identifying high-risk AI systems but also the wider range of entities involved in AI deployment, distribution, or usage. It's important to review existing governance frameworks to ensure they align with the Act's requirements. Additionally, organizations should proactively examine how the AI Act might impact their daily operations and specifically, systems already covered by other EU mandatory conformity assessments (medical devices, machinery,

protective equipment, etc). This requires gaining a comprehensive understanding of the legal, technological, and ethical aspects of AI to facilitate responsible integration and usage within the organization.

2. Developing a Robust AI Governance Program: It's essential for organizations to develop an AI governance program that integrates the AI Act's requirements with broader business strategies and objectives. This program should cover risk management, privacy, ethics, data governance, intellectual property, safety, and security, among others, and adapt existing policies and procedures to meet the new standards. Any types of organizations, more specifically businesses in tech- and data-driven industries, should assess how to leverage their existing GDPR compliance programs to also meet most, if not all, of the AI Act's requirements. The role of the board in overseeing AI use within the organization is also a critical consideration.

3. Global Coordination and Voluntary Initiatives: Businesses, above all, should pay close attention to international efforts to harmonize AI regulations, including the EU's collaborations with global bodies and initiatives. In this regard, the EU Commission has initiated an 'AI Pact', encouraging organizations to anticipate the AI Act by voluntarily sharing their internal guidelines, processes and concrete actions carried out to address the AI Act requirements, and by testing their solutions within the community. Participating in such voluntary commitments to implement the AI Act's requirements ahead of deadlines can position organizations as leaders in ethical AI use and governance.

4. Proactive Adaptation and Compliance Strategy: With the regulatory landscape rapidly evolving, businesses need to be agile, ready to update their AI strategies and compliance programs as new guidelines and requirements emerge. Starting early on this adaptation process will help mitigate risks and liabilities and ensure compliance. Keeping an eye on regulatory developments in the EU (including the AI Act delegated / implementing acts and guidance), the UK, the US, and other regions further along in AI regulation is vital for a comprehensive compliance effort.

5. Engagement and Transparency: Collaboration with regulators, transparent communication, and fostering global harmonization are critical for successful AI governance. Businesses should also consider public engagement and transparency in their AI operations as part of their compliance and risk management strategies. This includes clear communication about AI's role and impact within the organization and ensuring that AI technologies are deployed in a way that is ethical, responsible, and aligned with societal values. On a more operational standpoint, it would also make a lot of sense to combine as much as possible information to individuals respectively required under GDPR and the EU AI Act.

EU AI□:AI□□□□□□□□□□□□□□□□□□□□EU□□□

[illegible]EU[illegible]2024[illegible]3[illegible]13[illegible]EU AI[illegible]AI[illegible]AI[illegible]AI[illegible]EU[illegible]

[illegible]EU AI[illegible]11[illegible]EU一般データ保護規則（GDPR[illegible]GDPR[illegible]EU AI[illegible]

[illegible]AI[illegible]EU AI[illegible]5[illegible]

[illegible]

EU AI[illegible]11[illegible]

EU AI[illegible]AI[illegible]

1[illegible]: EU[illegible]AI[illegible]AI[illegible]OECD[illegible]AI[illegible]GDPR[illegible]AI[illegible]

[illegible]EU[illegible]AI[illegible]

2. [illegible]: AI[illegible]EU[illegible]AI[illegible]EU[illegible]EU[illegible]EU[illegible]AI[illegible]EU[illegible]AI[illegible]EU[illegible]AI[illegible]GDPR[illegible]EU[illegible]AI[illegible]

3.
[illegible]:
[illegible]AI[illegible]AI[illegible]4[illegible] [illegible]AI[illegible]AI[illegible]AI[illegible]AI[illegible]AI[illegible]AI[illegible]AI[illegible]

4. [illegible]AI[illegible]: EU AI法は、プライバシー、倫理、基本的権利にリスクをもたらす特定のAI[illegible]GDPR[illegible]

- [illegible]: [illegible]
- [illegible]: [illegible]AI[illegible]
- [illegible]: [illegible]
- [illegible]: [illegible]
- [illegible]: [illegible]
- [illegible]: [illegible]CCTV[illegible]
- [illegible]: [illegible]AI[illegible]

[illegible]

5. [illegible]**AI**[illegible]: EU AI[illegible]AI[illegible]2[illegible]

- **Annex II Systems**[illegible]II[illegible]: [illegible]AI[illegible]EU[illegible]
- **Annex III Systems**[illegible]III[illegible]: [illegible]AI[illegible]

[illegible]
CE[illegible]

[illegible]AI[illegible]AI[illegible]EU[illegible]AI[illegible]18[illegible]

[illegible]EU AI[illegible]AI[illegible]GDPR[illegible]9(2)(g)[illegible]

6. [illegible]**AI**[illegible]**AI**: EU AI[illegible]AI[illegible]
AI[illegible]AI[illegible]AI[illegible]AI[illegible]AI[illegible]
AI[illegible]AI[illegible]
[illegible]AI[illegible]

7. [illegible]AI: EU AI[illegible]AI[illegible]General Purpose AI[illegible]AI[illegible]AI[illegible]AI[illegible]AI[illegible]AI[illegible]AI[illegible]AI[illegible]AI[illegible]

8. [illegible]: [illegible]AI[illegible]AI[illegible]AI[illegible]

9. EU AI[illegible]GDPR[illegible]: [illegible]AI[illegible]GDPR[illegible]EU AI[illegible]GDPR[illegible]DPIA[illegible]EU AI[illegible]AI[illegible]DPIA[illegible]AI[illegible]EU AI[illegible]AI[illegible]

10. [illegible]: EU AI[illegible]AI[illegible]7[illegible]3,500[illegible]3[illegible]1.5[illegible]750[illegible]EU[illegible]AI[illegible]AI[illegible]EU[illegible]

11. [illegible]: EU AI[illegible]AI[illegible]6[illegible]AI [illegible]1[illegible]III[illegible]AI [illegible]2[illegible]EU[illegible]AI[illegible]3[illegible]

EU AI[illegible]5[illegible]

[illegible]DPO[illegible]AI[illegible]5[illegible]

1. [illegible]: [illegible]EU AI[illegible]AI[illegible]AI[illegible]EU AI[illegible]EU[illegible]AI[illegible]

2. [illegible]AI[illegible]: EU AI[illegible]AI[illegible]

[illegible]GDPR[illegible]EU AI[illegible]AI[illegible]

3. [illegible]:
[illegible]EU[illegible]AI[illegible]EU[illegible]AI Pact[illegible]EU AI[illegible]EU AI[illegible]EU AI[illegible]AI[illegible]

4. [illegible]: [illegible]AI[illegible]EU[illegible]AI[illegible]/[illegible]AI[illegible]

5. [illegible]: AI[illegible]AI[illegible]AI[illegible]AI[illegible]GDPR[illegible]EU AI[illegible]

MAJOR DEVELOPMENTS IN US LABOR UNION LAW: INSIGHTS FOR EFFECTIVELY NAVIGATING TRANSACTIONS AND OPERATIONS

Labor relations in the United States are highly regulated, and the regulatory environment fluctuate greatly with presidential administrations. This reality compounds transactional costs and risks. Nonetheless, Japanese companies with subsidiaries in the United States or interested in investing, acquiring or establishing operations in the United States can navigate and overcome these regulatory complexities with strategic planning and execution.

OVERVIEW OF US LABOR LAW

The National Labor Relations Act (NLRA) governs labor relations in the United States by regulating interactions between employees, employers and labor unions. The NLRA is administered by the National Labor Relations Board (NLRB), a federal administrative agency consisting of a five-person board to decide cases and a general counsel who investigates and prosecutes alleged violations of the NLRA.

Members of the NLRB are appointed by the president. Four of the five board positions are split between the country's two major political parties, with the decisive fifth seat awarded to the same party as the sitting president.

The NLRB general counsel is also appointed by the president. As a result, US labor law incurs significant shifts (often 180-degree reversals) between presidential administrations.

There are three key areas of the NLRA that impact business operations in the United States:

1. Regulation on how employees form a union
2. Regulation on which terms of employment require "bargaining" once a union is formed
3. Regulation on what rules and policies employers may implement for their workplaces (including nonunion workplaces)

CURRENT TRENDS IN US LABOR LAW

President Biden campaigned, in large part, on a promise to be "pro-union." Unsurprisingly, the NLRB – based on his appointments – has followed suit and made major changes to US labor law both by regulation and by decisions in specific cases that favor unionization and impose additional burdens on employers.

These shifts in prior law include the following:

Expediting Union Recognition

One of the NLRA's primary functions is governing how unions become the legal representative of employees. Until recently, this was only accomplished in one of two ways: (1) The employer voluntarily recognized a union (usually after the union provided proof that a majority of employees wished to join, making an election unnecessary) or (2) a majority of employees voted to join a union through an NLRB-administered secret ballot election. These pathways to recognition have been enshrined in US labor law for decades.

In 2023, however, the current NLRB created a third pathway intended to facilitate unionization. Now, unions are permitted to demand and potentially obtain automatic recognition. Employers receiving a demand for recognition from a union must promptly file an election petition or forfeit their employees' right to a secret ballot election.

The right to an employee secret ballot election has long been considered fundamental and sacrosanct. This right enables employees to hear their employer's perspective on voting for or against a union (during the employer's "campaign") and the potential implications of doing so. It also allows for the employee to then decide to vote for or against a union representative without fear of coercion or intimidation. Now, the NLRB will potentially force employers to recognize and bargain with a union regardless of the election's outcome if the NLRB finds any technical campaign infractions in the run-up to that election, including relatively minor ones. In other words, unions may end up obtaining very swift certification (and resulting rights of representation) without an employee

secret ballot voting process.

Employers will likely challenge these attempts to undermine secret ballot elections as the primary basis for determining union representation, but these challenges will take time (potentially years) to work their way through the US federal court system. In the meantime, Japanese companies with subsidiaries in the United States or evaluating investment opportunities must account for the reality of expedited union recognition.

Restricting Operational Changes at Unionized Facilities Without Bargaining

A core principle of US labor law is that employers with unionized workforces may not change employment conditions until they complete a bargaining process with the appropriate union. There is, however, one important caveat. Until recently, employers were permitted to take actions consistent with historical practices without bargaining and without union consent.

For example, employers of unionized operations must typically bargain with their employees' union before implementing any layoffs. However, if the employer was implementing layoffs because of an economic downturn, and it has always implemented layoffs during economic downturns throughout its history, the employer was permitted to implement the layoffs in question without any bargaining, saving time and money.

Now, employers with unionized workforces must bargain with a union on any discretionary decision regardless of the employer past practices (outside very limited exceptions). This requirement not only restricts operational freedom but it may create delays and opportunity costs that should be considered well in advance of any major employment-related decision.

Expanding 'Joint Employer' Obligations and Liability

On October 27, 2023, the NLRB issued a new rule expanding bargaining obligations and unfair labor practice liability to multiple entities at once. Under US labor law, it is possible for several companies to legally employ the same group of workers at the same time, so long as each company controls key aspects of the workers' employment. When this is the case, each company is required to bargain with the union representing the workers and all are equally liable for any labor violations. The application of this principle has been limited, however, by the commonsense requirement that each purported joint employer must actually exercise direct control over the employees at issue.

The NLRB's new rule now considers any company with indirect or reserved authority over workers as a joint employer (e.g., any company which use staffing agencies), even if those workers are controlled by another company (i.e., staffing agencies). In other words, any company with a contractual or potential right to control a worker's

employment will be considered a joint employer, even if it never actually exercises any control. This change will extend bargaining obligations, unfair labor practice liability and labor disruptions, including strikes, to companies utilizing staffing agencies and other forms of contracted third-party labor. These arrangements are common in US labor markets and must be accounted for when analyzing operational risks and contingency plans.

Expanding Employer Liability for Unfair Labor Practices

Section 10(c) of the NLRA allows the NLRB to "make whole" any employee subjected to an unfair labor practice. For nearly 80 years, the NLRB's remedies have largely been restricted to worker reinstatement (if appropriate) and monetary damages equal to the income the employee would have received but did not because of the unfair labor practice less interim earnings. In December 2022, the NLRB expanded the monetary damages it will award to "all direct and foreseeable pecuniary harms suffered" because of a labor violation, possibly including:

- Out-of-pocket medical expenses incurred after losing employer-sponsored insurance
- Costs associated with securing new health insurance
- Credit card debt incurred due to loss of income
- Compensation for damages to an employee's credit score
- Fees and expenses for training or coursework required to renew or obtain a new security clearance, certification or professional license
- Expenses related to housing, relocation, transportation and/or childcare

The NLRB's recent expansion of unfair labor practice likely exceeds its statutory authority and may be struck down by a US court of appeals. Until then, this expansion will increase litigation costs, which unions will try to leverage to extort concessions from employers during bargaining with a union.

NAVIGATING LABOR RISKS FOR SUBSIDIARIES AND TRANSACTIONS IN THE UNITED STATES

Japanese companies evaluating US subsidiary operations, investments or operational opportunities in the United States should consider the burdens and impacts of the NLRB's new agenda. While these costs and risks are potentially significant, these can be overcome through careful analysis and forward planning.

For currently unionized operations of a subsidiary or investment target, it is important to develop a full and accurate understanding of past and current labor relations of the relevant workforces. This includes determining if the relationship with the union is cordial or hostile as well as how long the company has been unionized. It is also crucial to analyze all existing labor agreements, as the acquiring company will likely be bound by their terms as the successor. It is especially important to determine whether there are "labor neutrality," automatic accretion or other such terms that require the company to idly stand by if the union seeks to expand to other facilities or other groups

at that facility. A labor neutrality term can give a union access, information and recognition rights to help it quickly organize other employees or facilities of affiliates or parent entities. An accretion term enables a union to automatically represent other employee groups.

Certain subsidiary operations and opportunities will be attractive despite union status or risks. In these cases, there are strategies companies can utilize to mitigate or avoid risk at unionized operations. For example, companies might consider restructuring workforces (combinations or separations) or engaging in asset transactions whereby a purchase is not necessarily obligated to recognize a union or a collective bargaining agreement.

For investment opportunities involving nonunionized operations, the focus must remain on the risk of unionization post-acquisition. Pre-transaction diligence should examine any ongoing organizing activity, union outreach and/or unfair labor practices. Diligence should also consider industry trends and whether union drives are proliferating at similar or nearby facilities.

Companies setting up new operations should evaluate organizing trends. Union participation and support varies greatly across the country, and setting up operations in an area with low union participation will help avoid subsequent encroachment. If unionization at a new operation is unavoidable, consider advantageous organizational structures where a separate legal entity employs any unionized workers. This will help prevent the union from extending its reach to other operations.

For all current or potential operations in the United States, companies should anticipate the possibility of union engagement and should determine their philosophical approach to union encroachment in advance. The primary leverage unions hold over companies is their ability to increase transactional and operational costs through strikes or other work stoppages, slow bargaining and excessive litigation.

Companies need to know whether their approach will be to make peace, prepare for battle or chart a middle course. Some companies choose to foster a harmonious relationship with the union. Others seek to avoid unions and, when necessary, defend their right to act. Both approaches can work and promote prosperous operations when properly executed. The key is knowing which approach fits the company's culture and outlook, and consistently applying the chosen course of action once it is determined.

Disclaimer: This article was published in the January 2024 issue of *The Journal of the Japanese Institute for International Business Law*. The discussion above is reflecting general market trends and developments. It is not a summary, analysis or commentary on any local laws. This article cannot be regarded as legal advice.

[redacted]

[redacted]

[redacted]National Labor Relations Act[redacted]NLRA[redacted]NLRA[redacted]National Labor Relations Board[redacted]NLRB[redacted]NLRB[redacted]5[redacted]NLRA[redacted]

NLRB[redacted]NLRB[redacted]5[redacted]4[redacted]2[redacted]5[redacted]NLRB[redacted]180[redacted]

[redacted]NLRA[redacted]3[redacted]

1. [redacted]
2. [redacted]
3. [redacted]

[redacted]

[redacted]NLRB[redacted]

[redacted]

[redacted]

NLRA[redacted]1[redacted]2[redacted](1) [redacted](2)NLRB[redacted]

[redacted]2023[redacted]NLRB[redacted]3[redacted]NLRB[redacted]

[redacted]

[illegible]

[illegible]

[illegible]1[illegible]

[illegible]

[illegible]

[illegible]

2023[illegible]10[illegible]27[illegible]NLRB[illegible]

[illegible]NLRB[illegible]

[illegible]

NLRA[illegible]10[illegible](c)[illegible]NLRB[illegible]80[illegible]NLRB[illegible]2022[illegible]12[illegible]NLRB[illegible]

- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

- [redacted]/[redacted]

NLRB[redacted]

[redacted]

[redacted]/[redacted]NLRB[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]: [redacted]2024[redacted]1[redacted]

UPC COURT OF APPEAL ISSUES FIRST DECISION, OVERTURNS PRELIMINARY

INJUNCTION

Back in September 2023, the Unified Patent Court's (UPC) Local Division Munich issued a preliminary injunction against the defendant in *10x Genomics, Inc. v. NanoString Technologies, Inc*. On February 26, 2024, in a landmark decision, the UPC's Court of Appeal overturned the preliminary injunction, allowing NanoString to return to most European markets.

The Court of Appeal clarified three key substantive issues in the case: the standard for **claim construction**, the standard for granting a **preliminary injunction** and the substantive **evaluation of inventive step**. Specifically, the Court of Appeal established the following:

1. Regarding the standard for claim construction, the patent claim is not only the starting point but the decisive basis for determining the scope of protection. The interpretation must always use the "description" and the "drawings" as explanatory aids and is not limited to cases where the claims include ambiguities. There will be no protection for what is disclosed only in the description or the drawings but has no basis in the patent claims. The same principles for claim construction will apply when assessing both infringement and validity.
2. Regarding the standard for a preliminary injunction, a proper decision for granting one must be based on it being "*more likely than not*" that the asserted patent is infringed and "*more likely than not*" that the patent will be found valid. This creates a balance – the opportunities to present facts and evidence by way of summary proceedings are limited, so the standard of proof must not be set too high. It also cannot be set too low in order to prevent the defendant from being harmed by an order for a provisional measure that is revoked at a later date. A sufficient degree of certainty is therefore needed, both for infringement and validity.
3. In provisional proceedings without hearing the defendant, the burden of proof for all relevant facts, including potential invalidity, lies with the applicant. In contrast, in provisional proceedings in which the defendant is heard, the burden of proof for entitlement and infringement lies with the applicant, while the burden of proof for invalidity lies with the defendant.
4. On the merits, the Court of Appeal held that the Local Division Munich incorrectly evaluated the likelihood that the patent would be found valid. The Court of Appeal determined that while the Local Division correctly concluded that the asserted patent would be found infringed and novel, it incorrectly concluded that the patent would likely be found to have an inventive step.
5. To reach this determination, the Court of Appeal relied on its own analysis of the prior art and on the opinion of its own technically qualified judges, with only a brief mention of a contrary view from the defendant's expert.
6. Additionally, the Court of Appeal applied a "classical" style inventive step analysis, determining and applying the understanding and capability of a skilled person in the art (as reflected in the cited prior art references) rather than strictly applying the "problem/solution" analysis commonly practiced at the

> European Patent Office. A skilled person in the art would have had a reasonable expectation of success when using the claimed method because, based on their expertise, they would have been able to deal with issues such as "molecular crowding" and "autofluorescence."

In setting these legal standards, the Court of Appeal has demonstrated that it is committed to actively leading the development of law and practice across the UPC, even if that means reigning in the work of the Local Divisions.

To learn more, visit our UPC Resource Center.

[illegible]

2023[illegible]9[illegible]UPC[illegible]*10x Genomics, Inc. v. NanoString Technologies, Inc*
[illegible]2024[illegible]2[illegible]26[illegible]UPC[illegible]NanoString[illegible]

[illegible]3[illegible]

1. [illegible]
2. [illegible]
3. [illegible]
4. [illegible]
5. [illegible]

[illegible]UPC[illegible]

HOW THE NEW PCI DSS 4.0 WILL IMPACT THE AUTOMOTIVE INDUSTRY

The automotive industry is experiencing a shift to an e-commerce model through direct interactions with the customer to accept credit card payments. This innovation allows drivers and passengers to make payments for products and services directly from their vehicles, offering an enhanced consumer experience. The automotive industry, like others, must comply with the Payment Card Industry Data Security Standard (PCI DSS) with respect to card transactions. The new version of PCI DSS (4.0) became mandatory April 1, 2024, and introduced many new rigorous requirements.

Changing Automotive Payment Modalities

Subscription services such as music streaming services, third-party apps, security services, and telemetric or concierge services are being offered and paid through cars' infotainment systems using payment cards. These payments may be collected directly by the car manufacturer or other third parties.

Entities that provide these new infotainment-based services and accept payment cards are likely "merchants" or "service providers" under the PCI DSS definitions. Both merchants and service providers must complete either a report on compliance (ROC) or a self-assessment questionnaire (SAQ) at least annually to comply with PCI DSS. ROCs or SAQs that are started after March 31, 2024 (the retirement date of prior PCI version 3.2.1) will need to use the new 4.0 version with its more rigorous requirements.

Some merchants and service providers may be in the midst of their PCI DSS compliance validation efforts under prior PCI version 3.2.1 as of March 31, 2024. In that case, merchants or service providers should reach out to the organizations that require their PCI compliance (e.g., acquiring banks, card brands, processors) to determine next steps, including whether they can continue with their 3.2.1 validation exercise.

As with any other channel used to process payment cards, in-car payments' connectivity, security and authentication are paramount concerns. Even if the entire cardholder data environment is outsourced, there are still obligations to comply with PCI DSS.

IN DEPTH

While participants in this industry may have some familiarity with PCI DSS obligations, the confluence of new technologies and connected-to systems with the advent of PCI DSS 4.0 drives a new PCI DSS compliance imperative.

PCI DSS 4.0 Brings New Requirements

After two years to prepare, the March 31, 2024, date for compliance with PCI DSS 4.0 is almost here. PCI DSS 4.0—which brings major changes to the payments ecosystem—places an increased focus on targeted risk analysis, organizational maturity and governance. It also makes PCI DSS compliance a continuous effort, rather than an annual snapshot exercise, and introduces a customized approach to PCI assessments, enabling businesses to implement alternative technical and administrative controls that meet the customized approach objective.

Merchants, service providers, issuers, acquirers and any other businesses that accept card payments or store, process or transmit payment cardholder data should have already begun planning for PCI DSS 4.0. Implementing PCI DSS 4.0 will require structural changes that go beyond tweaking security controls. Businesses will also need to prepare for the increased legal risks of PCI DSS 4.0's obligations. PCI assessments under version 4.0 will require more security documentation, risk analysis and affirmative statements than before, exposing the company's security posture to greater scrutiny.

According to Mazars's USA PCI qualified security assessor (QSA) team, automotive manufacturers, app developers and other companies that accept payments through in-vehicle systems will need to carefully assess how their in-vehicle payment solutions integrate with their existing payment platform. Particular attention should be paid to the communications protocols, deployment model and integrated payment infrastructure.

Because of the complexity of the new requirements and the time required to implement structural changes, companies should promptly begin addressing and internally validating compliance in advance of an assessment by their QSA. Businesses should consider whether to involve legal counsel and other consultants (under privilege) in this assessment and other aspects of their transition to PCI DSS 4.0, including for purposes of encouraging full and open communication and consideration of risks and exposure.

WHAT'S NEW IN PCI DSS 4.0?

PCI DSS 4.0 is an extensive change to the previous version, PCI DSS 3.2.1. Some of the significant changes are included below.

Increased Requirements for Yearly Diligence for Merchants and Service Providers

PCI DSS 4.0 increases the requirements for periodic diligence by merchants and service providers by adding several new controls, including the following:

- Service providers now have an explicit requirement to provide merchants with information necessary for

the merchant to comply with its monitoring requirements under PCI DSS 12.8.4 and 12.8.5 (PCI DSS 12.9.2).

- At least every 12 months and upon a significant change, merchants and service providers must document and confirm the PCI DSS in-scope environment (PCI DSS 12.5.2), with additional documentation requirements for service providers (PCI DSS 12.5.2.1-2).
- Merchants and service providers must conduct a targeted risk analysis for any controls that use the customized approach, at least every 12 months with written approvals by senior management (PCI DSS 13.3.2).
- Merchants and service providers must complete at least an annual risk analysis for any controls that have flexibility for the frequency of controls (PCI DSS 13.3.1, best practice until 2025).
- Merchants and service providers must review at least annually cipher suites and protocols (PCI DSS 12.3.3, best practice until 2025).
- Merchants and service providers must conduct at least an annual review of hardware and software technologies in use, with a plan to remediate outdated technologies approved by senior management (PCI DSS 12.3.4, best practice until 2025).

These additional annual diligence requirements will take time and effort to establish. Merchants and service providers may want to build these new processes well in advance of having to rely on them for PCI DSS compliance through their ROC or SAQ processes and QSA oversight. Starting sooner rather than later will be key to pragmatic results, allowing at least one practice cycle of these assessments prior to relying on them for PCI DSS compliance.

New Customized Approach

When merchants and service providers cannot meet the prescriptive controls of PCI DSS 3.2.1, they must propose a compensating control and justify it with a risk assessment and a compensating control worksheet. In PCI DSS 4.0, this option still exists, but there is also a new option for a customized control approach. This customized approach retains the requirement to evaluate risk but allows for a more strategic pathway to meet a control. Instead of compensating for the lack of a control, the customized approach allows the merchant or service provider to document a different control based on the objective of the control that is being customized. The assessor will then assess the customized control in place of the control that is being substituted, allowing for a long-term customization rather than a shorter-term "compensating" control. (Not all controls are eligible for the customized approach. Notably, PCI DSS 3.3.1 prohibits storage of sensitive authentication data after authorization.)

Expanded Risk Analysis Guidance

PCI DSS 4.0 also provides expanded guidance on conducting risk analysis. Risk analysis has always been a part of PCI DSS, and it significantly is used as part of the compensating control worksheet. This new version includes a Sample Targeted Risk Analysis Template (PCI DSS Appendix E2). While using the template is not mandatory, the

template provides more information on how the PCI Security Council expects a risk analysis to be carried out.

Clarifications to "Significant Change" Standard

PCI DSS 4.0 clarifies key PCI DSS concepts, including a more fulsome description of a "significant change," which was not specifically defined in prior PCI DSS versions. While this latest version does not provide an exact definition, PCI DSS 4.0 does provide descriptions and examples of a significant change (PCI DSS, 7 Description of Timeframes Used in PCI DSS Requirements). This is important given the many interim changes, adaptations and updates (especially in the mobile payments industry) in the United States and other countries, such as India.

WHEN DOES PCI DSS 4.0 TAKE EFFECT?

PCI DSS 4.0 was issued on March 31, 2022, but will remain optional until March 31, 2024, when PCI DSS v. 3.2.1 will be retired. Assessments begun after that date must be under version 4.0. Some companies have opted into 4.0 already and are conducting PCI assessments and SAQs/ROCs under 4.0.

Several new requirements added for version 4.0 will not become mandatory until March 31, 2025. Until that date these requirements are considered "best practice."

WHAT ARE THE LEGAL RISKS?

Failure to comply with PCI DSS 4.0 may lead to further investigations, fines, penalties and assessments, especially if there is a card breach after PCI DSS 4.0 becomes mandatory. Several state laws already incorporate PCI DSS, and other state laws include compliance with PCI DSS as a safe harbor.

The increased focus on risk analysis in PCI DSS 4.0 means that entities are likely to disclose more information about their security program to QSAs than they would under version 3.2.1. Given that PCI security assessments are not conducted under privilege, businesses should be prepared for the assessment papers to be scrutinized, particularly in the wake of a security incident. This will be increasingly significant, because the widespread adoption of chip transactions in the United States has reduced the viability of card cloning, reportedly causing credit card fraudsters large and small to target card-not-present transaction data and increase cybersecurity risk to a wide variety of companies.

Statements made in risk analyses should be accurate, verifiable and consistent with other disclosures. Security documentation should reflect actual, provable and current practices. Customized controls should defensibly meet the defined customized approach objectives.

The transition to PCI DSS version 4.0 will prove challenging and time-consuming to many companies. Companies should begin their transition planning promptly. An initial step in the transition should be an assessment against the PCI DSS 4.0 standard to identify compliance gaps and opportunities to implement a customized approach. Engaging outside counsel to help oversee the conduct of the internal assessment or other aspects of transition planning can mitigate risk and contribute to a successful transition.

新しいPSI DSS 4.0が自動車産業に与える影響

[illegible]E[illegible]PCI DSS[illegible]Payment Card Industry Data Security Standard[illegible]PCI DSS[illegible]4.0[illegible]2024[illegible]4[illegible]1[illegible]

[illegible]

[illegible]

[illegible]PCI DSS[illegible]merchants[illegible]service providers[illegible]PCI DSS[illegible]1[illegible]report on compliance[illegible]self-assessment questionnaire[illegible]2024[illegible]3[illegible]31[illegible]PCI[illegible]3.2.1の廃止日）以降に実施する遵守報告書または自己評価アンケートは、より厳格な要件を備えた新バージョン4.0を使用する必[illegible]

[illegible]2024[illegible]3[illegible]31[illegible]PCI[illegible]3.2.1に基づくPCI DSS[illegible]PCI[illegible]3.2.1の検証作業を継続できるかどうかを含め、次[illegible]

[illegible]PCI DSS[illegible]

[illegible]

[illegible]PCI DSS[illegible]PCI DSS 4.0[illegible]PCI DSS[illegible]

PCI DSS 4.0[illegible]

2年間の準備期間を経て、PCI DSS 4.0の遵守期限は2024[illegible]3[illegible]31日に迫っている。決済業界のエコシステムに大きな変化をもたらすPCI DSS 4.0[illegible]PCI DSS[illegible]PCI[illegible]

[illegible]PCI DSS 4.0[illegible]PCI DSS 4.0[illegible]PCI DSS 4.0[illegible]4.0[illegible]PCI[illegible]

Mazars[illegible]PCI[illegible]qualified security assessor[illegible]

[illegible]PCI DSS 4.0[illegible]

PCI DSS 4.0[illegible]

PCI DSS 4.0[illegible]PCI DSS 3.2.1[illegible]

[illegible]

PCI DSS 4.0[illegible]

- [illegible]PCI DSS 12.8.4[illegible]12.8.5[illegible]PCI DSS 12.9.2[illegible]
- [illegible]12[illegible]PCI DSS[illegible]PCI DSS 12.5.2[illegible]PCI DSS 12.5.2.1-2[illegible]
- [illegible]12[illegible]1[illegible]PCI DSS 13.3.2）。
- [illegible]1[illegible]PCI DSS 13.3.1[illegible]2025[illegible]
- [illegible]1[illegible]PCI DSS 12.3.3[illegible]2025年までのベストプラクティス）。
- [illegible]1[illegible]PCI DSS 12.3.4[illegible]2025[illegible]

[redacted]PCI DSS[redacted]PCI DSS[redacted]1[redacted]

[redacted]

[redacted]PCI DSS 3.2.1[redacted]PCI DSS 4.0[redacted]PCI DSS 3.3.1[redacted]

[redacted]

PCI DSS 4.0[redacted]PCI DSS[redacted]PCI DSS Appendix E2[redacted]PCI [redacted]

[redacted]

PCI DSS 4.0[redacted]PCI DSS[redacted]PCI DSS [redacted]PCI DSS 4.0[redacted]PCI DSS[redacted]PCI DSS[redacted]

PCI DSS 4.0[redacted]

PCI DSS 4.0[redacted]2022[redacted]3[redacted]31[redacted]PCI DSS v.3.2.1[redacted]2024[redacted]3[redacted]31[redacted]4.0[redacted]4.0[redacted]PCI[redacted]/[redacted]

[redacted]4.0[redacted]2025[redacted]3[redacted]31[redacted]

[redacted]

PCI DSS 4.0[redacted]PCI DSS 4.0[redacted]PCI

DSS[redacted]PCI DSS[redacted]

PCI DSS 4.0[redacted]3.2.1[redacted]PC
I[redacted]

[redacted]

PCI DSS[redacted]4.0[redacted]PCI DSS 4.
0[redacted]

GET IN TOUCH

Julian L. André
View Profile

Rosa Barcelo
View Profile

Caitlyn M. Campbell
View Profile

Edward B. Diskant
View Profile

James Durkin
View Profile

Jonathan Ende
View Profile

Christopher Foster
View Profile

Paul M.G. Helms
View Profile

Hon.-Prof. Dr. Henrik Holzapfel
View Profile

Charles (Chuck) Larsen
View Profile

Matthew Madden
View Profile

Romain Perray
View Profile

Sagar K. Ravi
View Profile

Paul M. Thompson
View Profile

Lorraine Maisnier-Boché
View Profile

Mark E. Schreiber
View Profile

David Beach
View Profile

Ashley Hoff
View Profile

Brian Long
View Profile

Simon Mortier
View Profile

Lisa Nassi
View Profile

Diana Pisani
View Profile