GC Guide to Navigating 2023

Bloomberg Law

Top Challenges Facing GCs in 2023

In 2022, general counsel (GC) were still grappling with unprecedented operational challenges brought on by the pandemic, while trying to address emerging issues facing their organizations, like developing strategies for environmental, social, and corporate governance (ESG) issues, dealing with the so-called "Great Resignation", and managing costs in an inflationary environment – to name a few. Stepping up to fill the demanding role of GC was never an easy feat, and 2023's legal landscape is showing no signs of making things any simpler for attorneys who acquire the top in-house position.

In particular, ESG, labor and employment, privacy, and transactional matters – both distinct and overlapping – will require GC to be well-informed of ongoing legal developments while strengthening their collaborative relationships with fellow executive leaders at their respective companies.

Here's a look at how key issues in these areas of practice might play out this year.

ESG: In 2022, GC had to help their companies navigate a minefield of state legislation and federal rulemakings surrounding ESG. This year, while much of this activity is expected to continue, businesses will also need to increasingly deal with the ESG-related concerns of their shareholders as investor activist campaigns signal a shift toward corporate policies that cut across the three pillars of environmental, social, and governance issues.

Labor & Employment: Although 2023 may provide new challenges for unions, GC of companies where employees are newly unionized will still need to work hard to ensure favorable collective bargaining outcomes for their business amid a push by the White House to strengthen organizing rights. Meanwhile, the ongoing trend of states passing laws that require disclosure of pay ranges will impact legal teams regardless of whether unions are involved.

Privacy: With five comprehensive state privacy laws taking effect this year, GC will need to be aware of material nuances between new statutes and accompanying regulations, including how they relate to artificial intelligence (AI) and health data privacy in light of the US Supreme Court's June 2022 *Dobbs v. Jackson Women's Health Org.* decision. On the national front, 2023 could be a banner year for the Federal Trade Commission's privacy endeavors.

Transactions: Companies impacted by last year's global supply chain woes will need to be vigilant of new types of disruptions, including war, extreme weather, and the risk of a global recession, while also monitoring the US government's enforcement of trade rules. In the world of private equity, while GC for companies seeking deals can expect a much slower year compared to 2022, there is still plenty of unspent capital to be put to use in acquisitions this year.

Table of Contents

Privacy

ANALYSIS

As AI Meets Privacy, States' Answers Raise Questions

by Peter Karalis
Legal Analysts, Bloomberg Law
Nov. 13, 2022

While artificial intelligence may stir debates about the future, it's already a part of many attorneys' current practice. And in 2023, companies doing business in four states—California, Virginia, Colorado, and Connecticut—will need to comply with consumer privacy laws governing AI-powered data processing. The regulatory answers proposed by these states on how to leverage AI in compliance with privacy laws are already spurring questions that will likely linger long after the laws take effect.

There are some high-level similarities among these laws' AI-related requirements, including mandatory risk assessments and individual rights to opt out of certain automated decisions. But there are also some major gaps—particularly surrounding the redress available for harmful outcomes—as well as various inconsistencies in the laws.

In light of these issues, and as complex of a subject matter as AI is, significant ambiguity will likely hang around throughout the next year.

AI Invasion of Privacy Law

For those new to AI, the function known as "machine learning" facilitates the large-scale analysis of data to predict outcomes. Numerous industries are already leveraging this technology for beneficial uses, ranging from thwarting cyberattacks to designing safer scooters.

AI's rapid implementation has also led to greater scrutiny of its risks, notably regarding discrimination and social media harms. For privacy regulators, one area of concern lies in the massive pools of personal data that machine learning often requires.

Businesses subject to the EU's General Data Protection Regulation (GDPR) since its May 2018 effective date should be familiar with that law's AI-related requirements, for which the European Commission adopted guidelines roughly five years ago.

The GDPR refers to the automated processing of personal data for predictive purposes as "profiling." Additional GDPR provisions govern the "automated decision-making" that may result from profiling or other processing methods.

In the US, these terms and related provisions have been partially emulated in four states' comprehensive consumer privacy laws taking effect throughout next year. The following graphic compares AI-related requirements from the GDPR and California's, Virginia's, Colorado's, and Connecticut's privacy laws.

Some (Non-Algorithmic) Predictions

As next year's state privacy enforcement priorities begin to take shape, expect businesses and privacy advocates to seek answers to three questions in particular.

1. How should companies explain the logic behind automated decisions?

Once the statute-driven rulemaking proceedings currently underway in California and Colorado are complete, both states will require businesses to explain their automated decision-making logic to individuals. These requirements are plainly inspired by the GDPR's mandate to provide "meaningful information" on such logic.

But some privacy scholars are questioning whether providing US consumers with an explanation of how AI works would be worthwhile. The Stanford Institute for Human-Centered Artificial Intelligence recommended in a January 2022 article that California instead require businesses to provide details on the contents and sources of data used for automated decision-making.

Colorado's proposed regulations are a bit more advanced in this regard, as they would require businesses to tell individuals which types of personal data are used to make automated decisions and to provide a "plain language explanation" of the logic. Nevertheless, businesses will likely need further guidance on how to satisfy this new requirement while simultaneously keeping consumer confusion to a minimum.

Consumer Privacy Laws Governing Profiling and Automated Decision-Making (ADM)

Jurisdiction	EU	California	Virginia	Colorado	Connecticut
Law	**GDPR**	**CCPA, as amended by CPRA**	**VCDPA**	**CPA**	**CTDPA**
Effective date	May 25, 2018	Jan. 1, 2023	Jan. 1, 2023	July 1, 2023	July 1, 2023
Requires assessment of high-risk processing?	Yes, including profiling specifically	Yes, pending regulations	Yes, including profiling specifically, pending regulations	Yes, including profiling specifically	Yes, including profiling specifically
Rights to notice of processing purposes?	Yes, including ADM specifically	Yes	Yes	Yes, including ADM specifically, pending regulations	Yes
Right to notice of information on ADM logic?	Yes	No	No	Yes, pending regulations	No
Right to request access to information on ADM logic?	Yes	Yes, pending regulations	No	No	No
Prohibits ADM with significant effects?	Yes, if no human involvement, with exceptions	No	No	No	No
Right to opt-out of ADM with significant effects?	Yes	Yes, pending regulations	Yes	Yes, if no human involvement, pending regulations	Yes, if no human involvement
Right to opt-out of profiling without ADM?	Yes	No	No	No	No
Right to contest results of ADM with significant effects?	Yes, if no human involvement	No	No	No	No

Source: Bloomberg Law

2. What redress will individuals have if automated decisions cause harm?

Colorado, Connecticut, and Virginia will require businesses to let individuals opt out of having their personal data used for automated decisions. Each state's law expressly limits this right to decisions that could have serious outcomes, including ones concerning employment and lending. The CCPA requires California to adopt regulations that enable a similar opt-out right, although it's currently uncertain whether this will also be limited to certain decision categories.

However, these laws all fail to specify what actions individuals may take if they're harmed by automated decision-making. In contrast, the GDPR, as well as the national privacy laws of Brazil, China, and

South Africa, each grant individuals some form of redress, such as the right to contest or otherwise obtain human review of an automated decision. The White House's recently released Blueprint for an AI Bill of Rights similarly encourages a right to human consideration of "high-risk" matters.

Granted, individuals may often challenge automated decisions through other applicable laws, such as the Fair Credit Reporting Act or Americans with Disabilities Act. But for significantly impactful decisions that don't affect credit or result in unlawful discrimination, companies will likely require greater clarity to effectively assess the risks of fielding complaints over AI logic gone wrong.

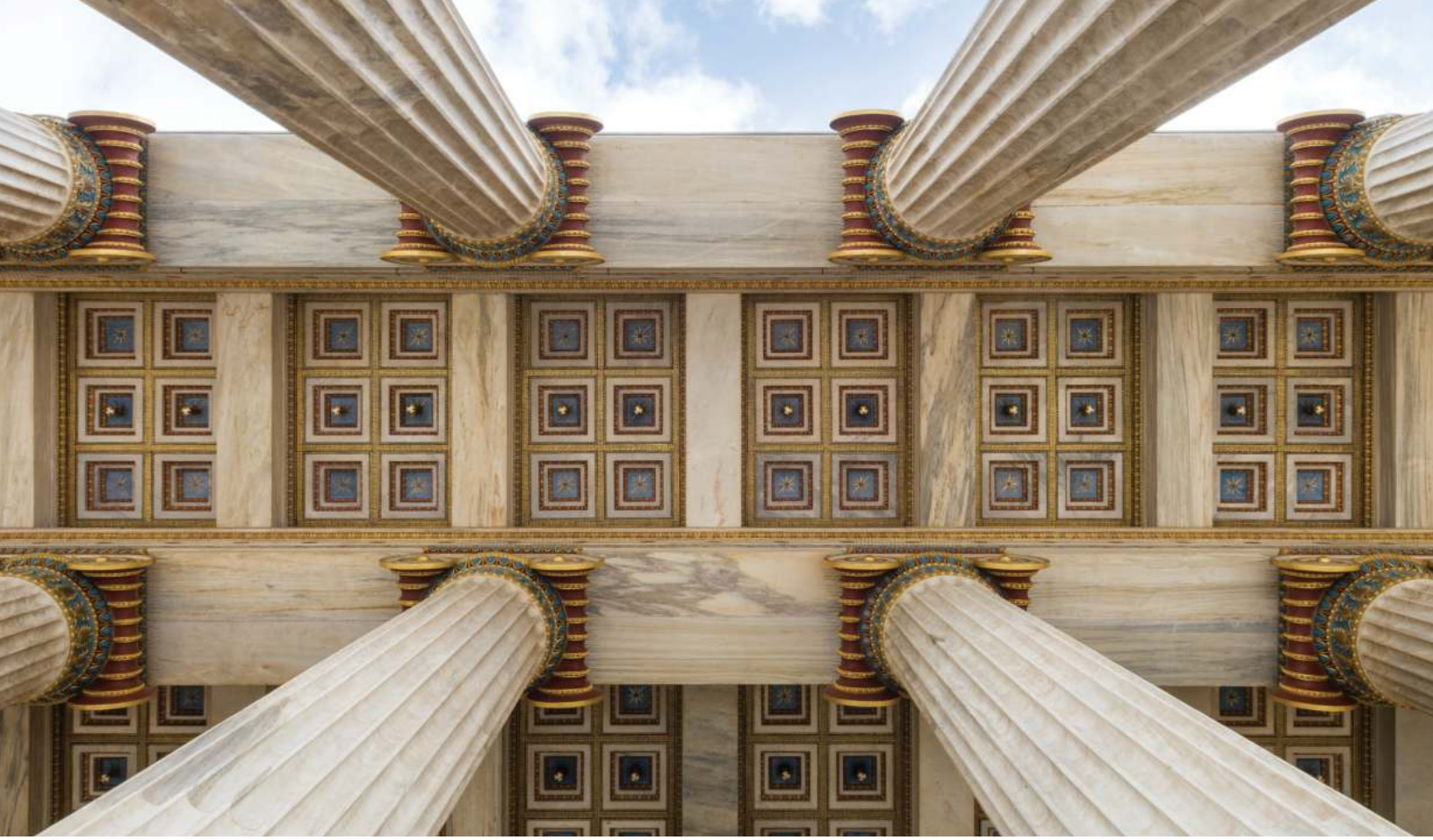
3. How will states enforce the right to delete personal data from algorithms?

In addition to the right to opt out of certain personal data processing, each state will grant individuals the right to have their personal data deleted. But none of these states' privacy laws—nor the GDPR, for that matter—explicitly addresses how the right to deletion relates to personal data used to shape AI algorithms.

The Stanford article suggested that businesses could rectify some privacy concerns by creating synthetic data to essentially replace someone's personal data, thereby avoiding the cost of retraining an algorithm to operate without such information. Of course, it would be quite helpful to businesses if state regulators signaled their approval of such practice as a valid means of fulfilling deletion requests.

Further complicating matters, the Federal Trade Commission has begun enforcing the wholesale deletion of algorithms that rely on unlawfully gathered personal data. Businesses will need to be mindful of this novel approach regardless of where they do business.

States may also decide to analyze public comments submitted for the FTC's ongoing commercial surveillance rulemaking—which encompasses automated decision-making, among numerous other topics—to help shape their own guidance in this evolving area. Even if the FTC doesn't achieve its lofty goal of passing a broad federal privacy rule, states are well-positioned to carry the baton of AI regulation forward.



ANALYSIS

FTC Privacy Authority Is Poised for Breakthrough Year

Mary Ashley Salvino, Senior Legal Content Specialist, Bloomberg Law

If the Federal Trade Commission were a major league baseball team, it might be fair to view 2022 as a rebuilding year regarding its privacy enforcement authority. 2023, on the other hand, might just be the season that marks the FTC's long-awaited return to a privacy authority winning streak.

The FTC spent 2022 recalibrating after it suffered setbacks to its privacy enforcement game plan, stemming from low morale, divisive partisanship, and a dearth of resources.

To be clear, the FTC still remains underfunded, but 2023 could nevertheless be a remarkably productive year for the privacy watchdog. A strengthened FTC—with a deadlock-proof panel of commissioners—could reach new heights, especially with the possible adoption of new privacy rules and bipartisan support for proposed federal privacy legislation

2023 could be a banner year for FTC enforcement endeavors, particularly in the areas of algorithmic disgorgement remedies, child online privacy, unfair data practices, and deceptive digital patterns.

Algorithmic Disgorgement

Legal practitioners should be aware of a new FTC trend: Utilizing algorithmic disgorgement as a powerful deterrent against unlawful data collection and as a potent tool for consumer redress in 2023.

Algorithmic disgorgement, which involves the destruction of artificial intelligence-powered algorithms, is a legal remedy used by the FTC to

require companies to relinquish the "fruits" of ill-gotten data, including the very algorithms developed or utilized with such data. Armed with this veritable enforcement weapon, the FTC has demonstrated ingenuity in exercising its privacy authority to penalize companies' allegedly deceptive data practices.

Any baseball enthusiast—or privacy practitioner—should be impressed by the agency's 3-for-3 record in securing settlement orders against companies that were investigated for developing AI models or algorithms through purportedly tainted, ill-gotten data. This is most recently evidenced by the FTC's March 2022 settlement with WW International, formerly known as Weight Watchers, which followed prior algorithm-related settlements with Everalbum in 2021 and Cambridge Analytica in 2019.

In a particularly resourceful maneuver, the FTC's court-enforced settlement order mandated the deletion of all ill-gotten data that WW International allegedly obtained from children without their parents' consent, and required the destruction of any algorithms trained on, derived, or developed from such data—along with levying a hefty $1.5 million civil fine.

While questions remain regarding how exactly the FTC will implement and monitor algorithmic disgorgement, these recent settlement precedents demonstrate that the agency will continue to pursue companies that deceive consumers through unlawful personal data collection in inventive ways. With the Supreme Court's 2021 gutting of the FTC's ability to obtain equitable monetary relief under Section 13(b) of the FTC Act in AMG Capital Mgmt. v. FTC, it's clear that the FTC will likely pursue this non-monetary mechanism to obtain redress for wronged consumers going forward.

Aggressive 'Unfairness' Enforcement

In 2023, the FTC will also likely continue to engage in aggressive policy statements and to pursue increased "unfairness" enforcement pursuant to Section 5 of the FTC Act.

The agency in May published a curious blog post asserting that Section 5 may require companies to notify individuals of breaches of their personal data—even where there's no specific breach notification requirement under state or other federal data breach laws. The slightly out-of-left-field post explained that

a failure to provide breach notifications may "increase the likelihood that affected parties will suffer harm," and that in such cases, the FTC Act creates a "de facto breach disclosure requirement."

This is somewhat remarkable, but also in line with the FTC's trend of issuing confusing and opaque guidance—which I've previously written about with regard to the agency's ambiguous "dark patterns" guidance. Yet strangely, that vagueness may serve as a useful tool by giving the agency some maneuverability in its policymaking and affording it relatively wide leeway in defining potentially unfair or deceptive breach notification practices.

In 2022, the FTC has similarly exhibited an increasingly aggressive enforcement stance against "unfair" data security practices. Pursuant to its Section 5 "unfairness authority," the agency can leverage its ability to enforce a greater scope of unlawful behavior through privacy and data security enforcement. In 2023, look for the FTC to continue to establish strong precedent under this prong, which will serve to armor the agency against potential constitutional challenges to its authority.

'Ramped-Up' Dark Patterns Enforcement

In line with forward-looking enforcement trends, practitioners should expect the FTC to "ramp up" enforcement efforts targeting digital dark patterns in 2023 by striking against the legality of these deceptive interfaces, which are prevalent in mobile apps, websites, and e-commerce platforms.

The FTC portended such heightened scrutiny in its September staff report, "Bringing Dark Patterns to Light". The report clarified much of the vagueness and ambiguities presented by the agency's policy statement on negative option marketing, cited applicable precedents and case law for the FTC's continued dark patterns enforcement, and delved into how deceptive digital patterns can subvert, manipulate, or obscure consumer choice.

Although it's non-binding guidance, the staff report exemplifies how strongly the FTC views dark patterns enforcement as a key priority. Companies are on notice that the agency intends to fiercely back up its bold enforcement statements, especially for dark patterns designed to manipulate children and teens. And as recently as November of this year, the FTC imposed a dark patterns enforcement consent order penalizing telecommunications service Vonage to the tune of $100 million for the company's unlawful use of junk fines and near-impossible cancellation options.

New Privacy Rulemaking

If Congress passes the American Data Protection and Privacy Act in 2023, it will be a game-changer for the FTC's privacy authority. As currently drafted, the ADPPA would grant the FTC new rulemaking authority and expressly name the agency as the law's primary enforcer.

But regardless of whether such federal legislation passes, the FTC has evinced more plans for an aggressive privacy and data security agenda through the unveiling of their most recent rulemaking—thereby covering all its bases. The new Advanced Notice of Proposed Rulemaking encompasses most industry sectors and touches upon a litany of online data practices, including online harms posed to children, algorithmic discrimination, and potential expansion of enforcement remedies.

Overall, practitioners should be on notice in 2023 of a determined, aggressive FTC zeroing in on key privacy enforcement priorities and playing hardball through scrutinizing and policing data security and privacy abuses covered under its mandate.

ANALYSIS

Who Will Regulate Privacy in Femtech After *Dobbs*?

by Laura Travis
Legal Content Specialist, Bloomberg Law
Nov. 13, 2022

The US Supreme Court's Dobbs v. Jackson Women's Health Org. decision has brought health privacy and femtech into the spotlight on a federal and state level.

Femtech is a term covering the technology used for such health purposes like period tracking, reproductive health, and fertility solutions. The *Dobbs* ruling could impact users of femtech products because information stored on them can be used to determine if someone has had an abortion. Period trackers, for example, store information that can be used by government actors for this purpose.

Members of Congress have pushed for revisions to the federal health privacy framework in response to *Dobbs*, but the most tangible federal response relating to femtech has been guidance from HHS on how to protect health information when using a cell phone or tablet. So, unless there are revisions federally that will protect femtech user information, regulation of femtech will fall to the states.

However, there is a chance that there will be no relevant regulation at either level.

The Federal Privacy Framework and Femtech

The regulation of an individual's health information on a federal level relies on a patchwork system that was created before most of the modern technology that's used to store health care information even existed.

Health information privacy in technology is federally governed by four rules through three agencies: HIPAA, through HHS; the Food, Drug, and Cosmetic Act, through the FDA; and the Federal Trade Commission Act and the Health Breach Notification Rule, through the FTC. Despite so much regulation, this enforcement scheme doesn't fully protect the health information of individuals using femtech products.

For example, HIPAA only applies to covered entities and business associates. Covered entities are health care providers, health plans, and health care clearinghouses—and most femtech doesn't fit into these categories. HIPAA will not stop most femtech companies from sharing information, nor require them to meet technical security standards. The law's business associate requirements will not provide strong protection for femtech products, because these products are usually used in a personal capacity, not in conjunction with care from a covered entity.

An exception to HIPAA allows covered entities to disclose health information to government agencies and law enforcement in certain circumstances, but there's an important push for HHS to remove or to narrow this exception. Additionally, the bipartisan American Data Privacy and Protection Act is looking at potential passage in Congress. In the meantime, state action will be the critical avenue for femtech regulation.

Rise in State Governance of Femtech

Many will look for states to act, given the lack of federal femtech governance. But it's unclear what post-*Dobbs* privacy protections would look like.

Many states' privacy protections have exceptions stating when the government can require providers to report private health information, and states already are using their authority to require providers to report abortions. Reports from information stored on femtech applications likely will become a way for certain states to discover if a person has had an abortion. The applicability to femtech applications and products will vary by state, but it will likely be an avenue that states use to enforce their abortion bans.

These exceptions are also being used to try to get information on abortions that occur in states still allowing abortions. States facing this pressure may respond by narrowly tailoring the exceptions to specifically exclude information about abortion stored on femtech products. States likely will also create legislation that outright prohibits the sharing of information involving reproductive health or abortion—or at least the sharing of an individual's health information without informing them.

For example, the California Consumer Privacy Act of 2018 gives California consumers the right to know the personal information that businesses collect from and about them and how it's used. California also recently enacted a law that will prevent California companies from complying with search warrants related to abortion investigations originating in other states. Several states have been following California's lead in passing state level privacy laws or bringing new bills to the table.

As states take on a role in femtech regulation, conflicts between different state laws will likely happen. US senators voiced this concern in a letter to HHS, warning that confusion will grow "as state lawmakers continue to implement a patchwork of laws restricting access to abortion and other reproductive health care services."

But unless the federal framework changes, the status of health information protections involving abortion and reproductive health will remain confusing and vague for femtech companies.

The Role of Technology Companies

Some technology companies and femtech product makers themselves have leaned toward taking steps to protect consumers. Google has announced that it will delete location data from abortion clinics and that it will make it easier to delete logs on period trackers. A popular period tracker called Flo will offer an anonymous profile option.

Unless government entities act, femtech companies may have the most tangible influence on how private health information is used and what level of privacy femtech products have. In lieu of any concrete government directive or oversight, privacy in femtech will become a Wild West, where private companies decide how their customers' information is to be shared and used.

Bloomberg Law

2022 In-House Counsel Customer ROI Survey

In 2022, we surveyed in-house counsel customers to examine the potential return on investment (ROI) legal departments may realize by utilizing Bloomberg Law.

94% of GCs and CLOs surveyed agree that Bloomberg Law has all the legal research tools, resources, and content in-house counsel need on a single, integrated platform.

Click here to download the Executive Summary
and see how Bloomberg Law can help your department:

Advise With Confidence

Bloomberg Law helps them advise business stakeholders and handle matters across a broad range of practice areas and topics with confidence.

Bloomberg Law helps their legal department act as trusted advisors and key counsel to the business.

Reduce Reliance on Outside Counsel

Bloomberg Law allows their legal department to bring more work in-house and reduce reliance on outside counsel.

Bloomberg Law helps their company avoid hiring outside counsel for low-value or "introductory" issues in areas beyond their primary fields of legal expertise.

Boost Department Productivity

Bloomberg Law helps their legal department track and stay current on the latest compliance and regulatory requirements

Bloomberg Law frees up time for their legal department to focus on higher-value work.

CHECKLIST

Managing Privacy and Cybersecurity Law Risks in Vendor Contracts (Annotated)

Contributed by Reena Bajowala, Ice Miller

Editor's Note: This checklist raises key issues and topics for attorneys to consider in ensuring that their client company and its vendors abide by applicable compliance requirements and maintain the security of the company's and its customers' data.

1. Shifting Liability

Comment: Contract provisions should attempt to transfer whatever risk the company is not able to mitigate on its own. When contracting with vendors, consider how common contract provisions can be used in ways that shift liability when it comes to matters related to data security.

❑ Does the contract mitigate the inherent uncertainties of vendors managing and handling data by requiring the vendor to have cyber liability insurance?

Comment: Cyber liability insurance can help mitigate the risks associated with having vendors manage and handle customer and client data. A common request, which depends on the risk involved, is for $5 million in cyber insurance.

These contract provisions will often prescribe minimum limits, detail the types of incidents covered, or even demand that the company be added to the policy as a beneficiary. Confirm that policies cover ransomware incidents.

❑ Does the contract's limitation of liability clause adequately allocate the liability between the parties?

Comment: In these clauses, companies can seek to limit the amount of monetary damages with a cap. Also, companies can put limits on the possible categories of damages which the vendor may pursue, such as barring against damages for lost profits or special damages.

❑ Does the contract allocate which party will be responsible for any fines or other costs relating to the vendor's violations of requirements to keep data secure?

Comment: When contracting, companies can create indemnification categories, such as "violations of confidentiality" or "violations of security," to protect themselves from potential legal issues.

Companies should seek reimbursement of investigation costs and other costs to legally evaluate both a vendor's and its own compliance with data security obligations, including reasonable attorneys' fees.

2. Information Sharing & Notifications

Comment: Because companies relinquish some control when they give vendors access to customer and client data, companies should be kept up to date on how vendors are operating. Additionally, companies should ensure that they are being updated when security incidents happen.

❑ Does the contract require the vendor to share information with the company about how the vendor is managing the company's data?

Comment: Companies can add data security-specific addendums that have detailed requirements on the administrative, technical, and physical safeguards that must be in place for the contract to move forward. An additional way to approach this is by requiring data security questionnaires and information about how vendors are ensuring confidentiality.

❑ Does the contract have mechanisms in place that allow the company to promptly respond to security incidents?

Comment: When contracting, the company should require the vendor to notify the company when suspected security incidents and confirmed data breaches occur so that the company can quickly and appropriately respond.

Companies should also reserve the right to require the vendor to provide notifications to the company's customers at the vendor's own cost, as well as the right to approve the specific notices that are sent out on the company's behalf.

❑ Does the contract require vendors to notify the company if the vendor materially alters an aspect of its security practices?

Comment: This is important because companies should know exactly when a vendor changes its practices so that the company can quickly evaluate if these new practices maintain the level of security the company agreed upon at the time the contract was executed.

❑ Does the contract require vendors to notify the company when the vendor hires a new contractor?

3. Flow Down of Requirements

Comment: As the supply chain for vendors and subcontractors gets longer, the company's risk of experiencing data security breaches grows. If just one link in the chain has weak security, that makes every party involved even more vulnerable to data breaches.

❑ Does the contract require vendor requirements to flow down to subcontractors?

❑ Do breach notification obligations flow up from subcontractors to the vendor?

❑ Does the contract recognize that data localization laws are an important part of the flow down of requirements?

Comment: If a company hires a vendor which then hires a subcontractor in a different country, then the vendor may be violating data localization laws. This is especially important with the growing activity in the international regulatory environment.

❑ Does the contract require that new subcontractors are well versed in the specific standards of security and confidentiality obligations that the subcontractor is required to comply with?

4. Ongoing Compliance

Comment: A perfectly written contract is only useful for ensuring data security if the company continues to check on its vendors to ensure ongoing compliance.

❑ Does the contract allow companies to have a streamlined process for amending the contract when new regulations come into effect?

❑ Does the contract allow the company to monitor the ongoing compliance of the vendor?

Comment: This can be done on an annual basis or upon the company's request that additional information be provided to help the company ensure that the vendor is maintaining the security posture with which it started. Ongoing compliance also involves making sure the vendor does not have any other reported data breaches or security issues. Finally, compliance can be monitored with third-party audit reports.

With assistance from Emma Robinson, JD candidate, University of Michigan Law School

CHECKLIST

Key Data Security Questions When Reviewing Vendor Contracts (Annotated)

Contributed by Melissa Krasnow, Partner, VLP Law Group LLP, where she advises clients in the e-commerce/internet, health care, education, financial services, manufacturing and technology areas on domestic and cross-border privacy, data security, big data, artificial intelligence and governance matters, technology transactions and mergers and acquisitions.

If a company has conducted a preliminary assessment of vendors, or if the company has not conducted such preliminary assessment of vendors or does not have such preliminary assessment process, the following checklist raises key questions as a company reviews the terms of a proposed vendor contract.

Personal Information

1. How is personal information defined?

Comment: How personal information is defined can determine whether the contract is favorable to a given party. A broad definition generally favors the company, while a narrow definition favors the vendor, especially in light of security incidents or other covered events and security practices.

- Does the definition refer to a specific law/regulation, e.g., GDPR, CCPA/CPRA, and/or other foreign, federal, or state law, etc. or other source?

Comment: Consider whether a specific law/regulation is applicable to the contract or whether a definition from a law/regulation would be appropriate even in the absence of the law's/regulation's applicability.

Note: The CCPA's provisions remain in effect and are enforceable until the same CPRA provisions become enforceable. The CPRA generally becomes operative on January 1, 2023. CPRA enforcement of the provisions added or amended by the CPRA begins on July 1, 2023.

- Does the definition refer to special categories of personal information, such as sensitive personal information? If so, how are they defined?
- Does the definition refer to a specific contract or document?

Comment: Determine whether a specifically referenced contract or document is applicable and/or appropriate.

- Are examples of personal information and/or personal information identifiers specified?

Comment: Determine whether examples of personal information and personal information identifiers are representative of the information at issue in the contract.

2. Is there a separate definition for confidential information?

- How is confidential information defined?
- Is personal information included in the definition of confidential information?
- Is personal information to be treated as confidential information?

3. Are there types of information defined separately from personal information and confidential information?

Comment: If personal information is included in the definition of confidential information or if personal information is to be treated as confidential information, then the provisions for confidential information also need to be taken into account regarding personal information.

Applicable Law

1. Are specific laws/regulations incorporated into the contract?

- If not, should they be?
- If so, in which context?
- If so, are requirements of such specific laws/regulations included in the contract and are such requirements required to be in the contract?
- If so, are requirements included in the contract that are not required by and beyond such specific laws/regulations?

Comment: Consider the extent to which a specific law/regulation, e.g., GDPR, CCPA/CPRA, etc. applies to the contract. Determine what clauses regarding compliance with "all applicable laws and regulations" mean in a particular contract. Review other contracts referenced in clauses incorporating other contracts, including to determine which laws/regulations are cited therein.

2. Is specific guidance, or are specific industry practices, standards, or frameworks incorporated into the contract?

- If not, should they be?
- If so, how are they included and defined?
- Are they required or recommended as a "best practice"?

Comment: Certain guidance, industry practices, standards, or frameworks can apply to a company in addition to laws/regulations. Determine their applicability, whether they should be referenced, and which party must abide by them.

3. Are cyber liability insurance requirements included in the contract?

Comment: Certain cyber liability insurance requirements can apply to a company in addition to laws/regulations/guidance. Determine their applicability, how to address them, and which party must abide by them.

4. Does the contract address potential and actual changes to laws/regulations/guidance, e.g., CCPA/CPRA, foreign, federal and/or state laws, etc., and cyber liability insurance requirements?

Comment: Consider including a clause indicating how the parties should respond to changes in laws/regulations/guidance and cyber liability insurance requirements affecting their respective obligations. If a forthcoming change is known, consider provisions with appropriate effective dates.

Security Incident or Other Covered Event

1. How is security incident or other covered event defined?

- Are unauthorized and/or unlawful collection, maintenance, use, or disclosure, and/or provision of access addressed? If so, how?

Comment: Unauthorized and/or unlawful collection, maintenance, use, or disclosure, and/or provision of access may be defined separately from security incident or other covered event. All definitions should be analyzed together in order to ensure clarity regarding a party's obligations regarding an event or events.

- Are misuse, loss, theft, alteration, destruction, and/or other compromise addressed? If so, how?

Comment: Misuse, loss, theft, alteration, destruction, and/or other compromise may be defined separately from security incident or other covered event. All definitions should be analyzed together in order to ensure clarity regarding a party's obligations regarding an event or events.

- Is a suspected security incident or other covered event included in addition to an actual security incident or other covered event?

Comment: Suspected security incident or other covered event language is generally favorable to the company. Sometimes a suspected security incident or other covered event becomes an actual security incident or other covered event. The vendor may not agree to suspected security incident or other covered event language because it may increase the number of security incidents or other covered events covered by the contract.

- Does the definition incorporate language from or refer to the CCPA/CPRA?

Comment: If the CCPA is or could be applicable, CCPA language should be included, i.e., "unauthorized access and exfiltration, theft, or disclosure of nonencrypted and nonredacted personal information as a result of the [vendor's] violation of [its] duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information" (Cal. Civ. Code §1798.150). Such language would be generally favorable to the company, and any other CCPA contract requirements should be complied with.

Note that when the CPRA's provisions become operational on January 1, 2023, language should reflect the updated text, i.e., "unauthorized access and exfiltration, theft, or disclosure of nonencrypted and nonredacted personal information (including email address together with a password or security question and answer that would permit access to the account) as a result of the [vendor's] violation of [its] duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information" (Cal. Civ. Code § 1798.150, italicized text added by the CPRA). Such language would be generally favorable to the company, and any other CPRA contract requirements could be addressed.

- Are ransomware, account takeover, business email compromise, phishing, and/or vulnerabilities addressed?
- Are there specific exceptions to the definition of a security incident or other covered event?

2. Does the contract address how, when, and to whom a security incident or other covered event must be reported?

- Who is required to report the security incident or other covered event?

- Is there a specific contact and contact information for providing and receiving such reporting?
- Is anyone else permitted to provide or receive the report of the security incident or other covered event?
- Which specific information must be reported?

Comment: Consider whether a specific list of information would more beneficial than a generic obligation to produce "all relevant information."

- How must it be reported?

Comment: For example, in writing, via email, etc.

- Must it be reported within a specific time frame?
- Are updates required, and if so, with any particular frequency?

Comment: Since facts and circumstances can change, an obligation to provide updated information is key. Frequency depends on what the parties negotiate.

- Which actions must be taken to prevent, investigate, contain, and mitigate the security incident or other covered event?

Comment: The party that receives the report of the security incident or other covered event should be provided with information about such actions.

- Which other actions must be taken regarding the security incident or other covered event?

3. Is a prompt or immediate investigation required?

4. Is cooperation regarding the security incident or other covered event required:

- between parties?
- with law enforcement, regulators, and/or government entities?
- with incident response personnel (internal and external)?
- with insurers and insurance brokers?
- Must a root cause analysis of the security incident or other covered event be provided?

5. Are there restrictions regarding disclosure of or publicity regarding a security incident or other covered event?

Comment: A party may wish to restrict disclosure of or publicity regarding a security incident or other covered event to align messaging and minimize the potential for discrepancies.

6. Does the contract specify which party is to have control of the investigation and management (including reporting) of the security incident or other covered event?

Comment: Both parties may seek to retain control for brand and reputation purposes. Determine reporting obligations to affected individuals, regulators, and others.

7. Does the contract specify which party is responsible for costs relating to the security incident or other covered event, e.g., legal, forensics, credit monitoring, printing and postage, other remediation, etc.?

Comment: Costs vary depending on the nature and magnitude of the security incident or other covered event. Certain laws/regulations address obligations relating to credit monitoring, e.g., California and Massachusetts breach notification laws.

- Does the contract require mitigation measures and/or actions to prevent recurrence?

Comment: The party that receives the report of the security incident or other covered event should be provided with information about such mitigation and actions.

- Does the contract require reporting and/or documentation regarding mitigation measures and/or actions to prevent recurrence? If so, to whom and in what format?

8. Does the contract require implementation and maintenance of, and testing of, a written incident response plan?

Comment: A written incident response plan for a security incident or other covered event which may vary depending on the given security incident or other covered event, e.g., ransomware.

Security Practices

1. Does the contract require specific physical, administrative, and technical safeguards?

- If so, what are these safeguards?
- Who has responsibility for which safeguards?
- Are the safeguards for personal information only?
- Do they cover confidential information?
- Do they cover other specified or defined information?

2. Does the contract require implementation and maintenance of a written information security program (WISP) with specific safeguards and is it in reference to a specific law/regulation or other source?

Comment: Certain laws/regulations require WISPs; requirements vary. Determine which laws/regulations apply and determine appropriate requirements. If a WISP is not required by law/regulation, consider contract requirements based on specific guidance, industry practices, standards, or frameworks and cyber liability insurance requirements.

3. Does the contract include security requirements specific to the vendor?

4. Does the contract require policies and procedures to detect and protect against actual or suspected security incidents or other covered events?

5. Does the vendor have separate policies and procedures addressing security?

- If so, what do they cover?

6. Does the contract require business continuity policies and procedures and disaster recovery plans?

- If so, what must they address?

7. Does the contract require and define backup and data recovery?

- If so, what is the recovery point objective, e.g., what is backup frequency?
- If so, what is the recovery time objective?

8. Does the contract require due diligence and include other measures regarding the vendor's employees and/or subcontractors, e.g., background checks, training, policy and contract requirements, etc.?

9. If the contract specifies access control measures, which access control measures?

10. Does the contract address and define multi-factor authentication?

- If so, for what is multi-factor authentication used?

Comment: Multi-factor authentication can be defined by law/regulation/guidance. See, e.g., the Federal Trade Commission's Final Rule regarding Standards for Safeguarding Customer Information.

11. Does the contract address and define encryption measures?

- If so, which data is to be encrypted, e.g., at rest, in transit, etc.?
- If so, what type of encryption?

Comment: Encryption measures can be defined by law/regulation/guidance. See, e.g., the California and Massachusetts breach notification laws.

12. Does the contract address and define penetration tests, and if so, how?

- If so, what is the frequency?
- Who performs them?
- Is remediation addressed, and if so, how?
- Is disclosure addressed, and if so, how?

Comment: Penetration testing can be defined by law/regulation/guidance. See, e.g., the Federal Trade Commission's Final Rule regarding Standards for Safeguarding Customer Information.

13. Does the contract address and define vulnerability assessments, vulnerability scans, and other discovery/awareness of a vulnerability and if so, how?

- If so, what is the frequency?
- Who performs them?
- Is remediation addressed, and if so, how?
- Is disclosure addressed, and if so, how?

14. Does the contract address and define patching software and updating software, and if so, how?

- If so, which software and what is the frequency?

- Who performs them?
- Is remediation addressed, and if so, how?
- Is disclosure addressed, and if so, how?

15. Does the contract specify restrictions on the use and/or disclosure of personal information, confidential information, and/or other specific or defined information?

16. Does the contract include specifications regarding personal information, confidential information and/or other specified or defined information relating to:

- secure transmission?
- secure storage?
- secure disposal?
- retention before deletion, e.g., regarding termination?

17. Does the contract address monitoring, testing, and updating of safeguards, program, policies, procedures, and/or requirements?

18. Does the contract permit or require assessments or audits of safeguards, program, policies, procedures, and/or requirements?

- What are the assessments or audits?
- How are they invoked and performed?
- How frequently?
- Who performs them?
- Who pays for them?
- To what extent and how can information about the assessments or audits be obtained?

19. Does the contract specify that deficiencies found in safeguards, program, policies, procedures, and/or requirements must be corrected?

- If so, how must correction of such deficiencies be communicated and to whom?

20. Does the contract address potential and actual changes regarding security practices, safeguards, program, policies, procedures, and/or requirements?

- If so, how?

PRACTICAL GUIDANCE

Cross-Border Data Transfers in China – Frequently Asked Questions

Contributed by Ken (Jianmin) Dai and Jet (Zhisong) Deng, Dentons
October 2022

Legal Framework

Q1. What constitutes a cross-border data transfer?
Cross-border data transfer refers to the provision of data collected and generated from mainland China to other countries and outside regions, including Hong Kong, Macao, and Taiwan. In addition to the electronic and physical transfer of data, granting access to such data for overseas recipients also constitutes a cross-border data transfer.

Q2. What is the legislation regulating cross-border data transfers?
The three pillars regulating data protection in China include:

- The Cybersecurity Law of the People's Republic of China (CSL), which sets forth the data localization requirements and cross-border transfer rules for critical information infrastructure operators (CIIOs)
- The Personal Information Protection Law of the People's Republic of China (PIPL), which regulates cross-border transfers of Personal Information (PI)
- The Data Security Law of the People's Republic of China (DSL), which regulates cross-border transfers of important data

Supplemental measures include:

- The Measures for Security Assessment of Data Cross-border Transfer (Measures) (in Chinese), which specifies the security assessment
- Guidelines for Cybersecurity Standards Practices – Security Certification Specifications for Cross-Border Processing of Personal Information (Certification Guidelines) (in Chinese), which clarifies details on the certification process for PI export.

The Provisions on Standard Contract for Cross-border Transfer of Personal Information (Draft for Comments) (in Chinese), along with the Standard Contract for Cross-border Transfer of Personal Information (SCC), is now in the comment phase and is expected to be finalized very soon.

Industry-specific legislation also regulates data export in industries such as finance, health care, express delivery, and others.

Q3. Who must comply with these rules?
According to the applicable scope stipulated by the CSL, DSL, and the PIPL, the following entities need to comply with the cross-border transfer rules of the People's Republic of China (PRC):

- PI handlers/processors located within the PRC
- PI handlers/processors located outside the PRC if the purpose of the PI processing is to provide products/services to natural persons located within the PRC or if the PI processing is for analyzing or assessing the behaviors of natural persons located within the PRC
- Important data handlers/processors within/outside the PRC

Q4. What mechanisms are available for cross-border data transfers?
For cross-border PI transfers, three mechanisms are available:

- Passing the security assessment organized by the Cyberspace Administration of China (CAC)
- Signing the SCC formulated by CAC with the overseas recipient
- Obtaining the certification granted by a CAC-recognized special agency

For cross-border transfers of important data, only the security assessment is available. For data besides PI and important data, no specific mechanism is required to carry out the cross-border transfer.

Q5. Which mechanism is suitable for your entity?
According to Art. 4 of the Measures, the security assessment is mandatory for PI providers that:

- Provide important data abroad
- Have been identified as CIIOs
- Have processed the PI of over 1 million individuals

- Have provided the PI of more than 100,000 individuals abroad cumulatively since January 1 of the preceding year
- Have provided sensitive personal information (SPI) of more than 10,000 individuals abroad cumulatively since January 1 of the preceding year

According to the Certification Guidelines, the certification is applicable to the following scenarios:

- Intra-group cross-border PI transfers among multinational corporations (MNCs), subsidiaries, or affiliates of the same business entity
- Outbound data handlers who directly collect PI from the PRC pursuant to Art. 3 (2) of the PIPL

The SCC applies to PI exporters that:

- Are not CIIOs
- Process the PI of less than 1 million individuals
- Have neither exported the PI of 100,000 individuals nor the sensitive PI of 10,000 individuals since January 1 of the preceding year

Generally, the SCC is preferrable for PI exports that occur less frequently, whereas the certification is suitable for PI exports among MNCs in daily business operations.

Additionally, the current version of the SCC does not apply to scenarios in which data processors provide PI to overseas data handlers/processors. Unless the finalized version of the SCC includes such scenarios, the only available mechanism might be certification.

Q6. What is the relationship between thelocalization requirement and the data cross-border transfer rules?

The localization requirements—Art. 37 of the CSL, Art. 31 of the DSL, Art. 40 of the PIPL— obligate certain data handlers to store particular types of data within the PRC by principle, whereas the cross-border data transfer rules regulate methods when such transfers become necessary.

It is not yet clear whether the threshold for mandatory security assessments as stipulated in the Measures are the same as the threshold for data localization as stipulated by Art. 40 of the PIPL.

Cross-Border PI Transfers

Q7. What is PI?
PI is defined as any kind of information, electronically or otherwise recorded, related to an identified or identifiable natural person within the PRC, excluding anonymized information that cannot be used to identify a specific natural person and is not reversible after anonymization.

Q8. What is SPI?
The PIPL defines SPI as PI that, if disclosed or illegally used, may cause harm to the security or dignity of natural persons. SPI includes information on biometric characteristics, religious beliefs, specific identity, medical health, financial accounts, individual location tracking, etc. Moreover, any PI of a minor under the age of 14 is regarded as SPI.

While the PIPL does not define "specific identity," given other regulations and national standards, the term may include race, ethnic group, sexual orientation, and special social identities like union membership.

Q9. What is PI protection impact assessment (PIPIA)?
The PIPIA is a mandatory precondition for cross-border PI transfers regardless of which mechanism is chosen. The PIPIA must assess:

- Whether the purpose and method of handling PI are lawful, legitimate, and necessary
- The impact on personal rights and interests and security risks
- Whether the protection measures taken are lawful, effective, and commensurate with the degree of risks

The PIPIA report must be stored for at least 3 years.

Security Assessments

Q10. Is the security assessment mandatory for all PI exports?
No. For PI exports, the security assessment is only mandatory for PI providers who:

- Provide important data abroad
- Have been identified as CIIOs
- Have processed the PI of over 1 million individuals

- Have provided the PI of more than 100,000 individuals abroad cumulatively since January 1 of the preceding year
- Have provided the SPI of more than 10,000 individuals abroad cumulatively since January 1 of the preceding year

Entities that do not fall into the abovementioned scope are not required to carry out the security assessment and thus can choose other mechanisms.

Q11. What materials are required for a security assessment?
According to Art. 6 of the Measures, the following materials are required:

- Application form
- Cross-border data transfer self-assessment report
- Legal documents to be concluded between the data handler and the overseas recipient
- Other materials required for the security assessment.

Q12. How is the self-assessment different from the PIPIA?
As described in Q9, PIPIA is a mandatory precondition for the cross-border PI transfers regardless of which mechanism is chosen. By contrast, the self-assessment is a mandatory requirement only for the security assessment.

Given their distinct nature, PIPIA is focused on assessing the impact on individual rights, while the self-assessment is focused on potential risks to national security, public interest, etc.

Q13. What is the procedure of a security assessment?
The security assessment must be submitted to the CAC through the local cyberspace administration (CA) at the provincial level. As is illustrated in the following flow chart, it normally takes 57 working days to complete. However, if the data handler has any objection to the assessment result, it can apply to the CAC for a re-assessment within 15 working days upon receipt, in which case the re-assessment result must be the final decision.

GRAPHIC: Security Assessment Application Process

Q14. Which authority reviews security assessment applications?
Although the materials shall be submitted to the provincial cyberspace administration authority for completeness review, it is the national cyberspace administration authority, i.e., the CAC, that organizes the relevant departments of the State Council, the cyberspace administration concerned at the provincial level, and specialized agencies to carry out the substantive review.

Q15. How long does it take for a security assessment?
In general, one complete security assessment should take no more than 57 working days– excluding the time spent on the self-assessment, which usually takes 3-6 months depending on circumstances. However, if the situation is complicated or supplementary or corrected materials are needed, the assessment may be extended.

Q16. What factors can affect the results of a security assessment?
As the security assessment focuses on the assessment of the risks to national security, public interests, or the legitimate rights and interests of individuals or organizations that may be caused by the activity of the outbound data transfer, the following factors will affect the result of the security assessment:

- The legality, legitimacy, and necessity of the purpose, scope, and method of the outbound data transfer
- The impact of the data security protection policies, regulations, and the cybersecurity environment of the country or region where the overseas recipient is located on the security of the data to be provided abroad; and whether the data protection level of the overseas recipient meets the requirements of the laws and administrative regulations of the PRC and mandatory national standards
- The size, scope, types, and sensitivity of data to be provided abroad; and the risks that the data may be tampered with, destroyed, divulged, lost, transferred, illegally obtained, or illegally used during and after the data is provided abroad
- Whether data security and personal information rights and interests can be fully and effectively guaranteed

- Whether the legal documents to be concluded by the data processor and the overseas recipient have fully agreed on the responsibilities and obligations of data security protection
- Compliance with Chinese laws, administrative regulations, and departmental rules
- Other matters that the CAC considers necessary to assess.

Q17. What are the remedies for a failed security assessment?
Data handlers that have any objection to the assessment results can apply to the national cyberspace administration authority, i.e., the CAC, for re-assessment within 15 working days after receiving the assessment results, and the re-assessment result must be the final decision.

Q18. How long is the security assessment valid?
The validity period of the result of the data cross-border transfer security assessment is 2 years, calculated from the date of issuance of the assessment result.

Q19. When is re-application triggered?
The following circumstances will trigger re-application of the security assessment:

- The 2-year validity period has expired
- ctivities of the cross-border transfer have changed. For example, the purpose, method, scope, and type of data provided overseas; the purpose and method of data processing by overseas recipients, affecting the security of data transferred; or the overseas storage period of PI and important data
- The security of the data provided abroad is affected due to changes:
  - In the data security protection policies or regulations or the cybersecurity environment of the country or region where the overseas recipient is located
  - Any other force majeure event
  - Any change in the actual control of the data processor or the overseas recipient
  - Any change in the legal documents between the data processor and the overseas recipient
- Any other circumstance affecting the security of the data provided abroad arises

Q20. What are the legal consequences for failure to apply for the security assessment?
Failure to apply for the security assessment may entail the following legal consequences:

- ***Corporate Liabilities.*** Any entity who transfers important data abroad in breach of Article 31 of the DSL may be:
  - Warned and ordered to make rectifications
  - Imposed a fine ranging from 100,000-1 million yuan—approx. $15,000 to $150,000—or a fine ranging from 1 million-10 million yuan—approx. $150,000-$1.5 million—where the circumstances are serious
  - Subject to suspension of related business, suspension for rectification, or revocation of business license
- ***Individual Liabilities.*** The person directly in charge and other directly liable persons can be imposed a fine ranging from 10,000-100,000 yuan—approx. $1,500-$15,000—or a fine ranging from 100,000-1 million yuan—approx. $15,000-$150,000—where the circumstances are serious
- **Civil Liabilities.** A data transfer agreement that leads to the illegal cross-border transfer of important data may be deemed as void
- ***Criminal Liabilities.*** A fixed-term imprisonment of less than 3 years and/or a fine if the circumstances are serious; or a fixed-term imprisonment of 3-7 years and/or a fine if the circumstances are particularly serious.

Q21. How long is the grace period?
The grace period for the security assessment is 6 months starting from Sept. 1, 2022.

Contract Requirements

Q22. How does the Chinese SCC differ from the EU Standard Contractual Clauses (SCCs)?
Major differences between the Chinese SCC and the EU SCCs include:

- ***Limitation on Data Volume.*** The Chinese SCC is not applicable to many MNCs since it only allows those who process PI of less than 1 million individuals and have not exported the PI of 100,000 individuals or the sensitive PI of 10,000 individuals since January 1 of the previous year to use this mechanism

- ***Limitation on Contracting Parties.*** The Chinese SCC has not specified the rules for the transfer from data processors to outbound data handlers/processors. China-based data processors may not be able to utilize this mechanism
- ***Filing Requirement***. The Chinese SCC contains an archival filing obligation with the local cyberspace administration at the provincial level. The PIPIA report is required as an essential component of the filing materials

Q23. Which standard contracts must be signed for entities that transfer PI between China and the EU?
In the scenario of a two-way transfer, the Chinese SCC shall be signed to regulate the PI transfer from the PRC to the EU, while the EU SCCs shall be signed to regulate PI transfer from the EU to the PRC.

Q24. To what extent can the SCC be modified?
The SCC can only be modified to the extent that it strengthens the PI's level of protection. As long as the contract terms do not prejudice the rights of the data subject and do not directly or indirectly conflict with the content stipulated in the main body of the SCC, the contracting parties can add additional terms to the Chinese SCC.

Q25. What is the relationship between the SCC and the binding legal documents required in the security assessment or certification?
For cross-border PI transfers, the SCC may be deemed as binding legal documents as required in the security assessment and the certification, although other documents such as internal management documents circulated in a group company may also be identified as such binding legal documents. However, the SCC cannot serve as the binding legal document for cross-border transfers of important data.

Q26. What materials are required for the archival filing of the SCC?
The SCC and the PIPIA report.

Q27. Which authority is in charge of the archival filing of the SCC?
The provincial cyberspace administration where the data handler is located.

Q28. What is the procedure for the archival filing of the SCC?
The data handler must, within 10 working days after the effective date of the SCC, file the SCC with the cyberspace administration at the provincial level of the place where it is located for the record.

Q29. Does archival filing affect the validity of the SCC?
No. The archival filing will not affect the validity of the SCC.

Q30. What are the legal consequences for failure of archival filing?
If the data handler fails to perform the archival filing, the provincial cyberspace administration shall order a correction within a prescribed time limit in accordance with the PIPL. If the data handler refuses to make corrections or damages the rights and interests of personal information, it shall be ordered to stop the cross-border PI transfer and be punished in accordance with the law. Criminal liability shall be investigated in accordance with the law if a crime is constituted.

Q31. When must the SCC be re-signed?
The SCC must be re-signed if one of the following circumstances occurs within the validity period of the SCC:

- The purpose, scope, type, sensitivity, quantity, method, storage period, and storage place of the PI transferred overseas have changed; the purpose and method of the overseas recipient to handle PI have changed; or the storage period of PI overseas is extended
- The rights and interests of the PI may be affected by the changes in the policies and regulations in the country or region where the overseas recipient is located
- Other circumstances that may affect the rights and interests of PI

Q32. What rights are data subjects entitled to under the SCC?
Data subjects have the right to exercise the obligations of the contracting parties in the SCC regarding the protection of personal information as a third-party beneficiary.

Certification

Q33. Who may apply for certification?
The following entities may apply for certification:

- The Chinese entity of the MNCs
- Specialized agencies/designated representatives established in the PRC for outbound data handlers that directly collect PI from the PRC pursuant to Art. 3 (2) of the PIPL

Q34. Which institution can grant certification?
Currently, the CAC has not released the list of recognized authorities to grant certification.

Q35. What are the major requirements for certification?
Major requirements for the certification include:

- Legally binding agreements
- Establishment of Data Protection Officer (DPO) and data protection institutions of the parties
- PIPIA
- Data subject rights
- Rules for cross-border transfers
- Acceptance of the supervision of the certification body, including responding to inquiries and routine inspections

Q36. What qualifications are required for the DPO?
The DPO shall have professional knowledge of PI protection and relevant management experience. The hiring for this position shall be undertaken by the organization's decision-making members.

Q37. What are the responsibilities of PI protection agencies?
Responsibilities of PI protection agencies include:

- Development and implementation of plans for cross-border PI transfers in accordance with the law
- Organizing and carrying out PIPIA
- Supervising the organization's handling of PI in accordance with the rules agreed between the data handler and the overseas recipient
- Receiving and handling requests and complaints from data subjects

Q38. How long is the certification valid?
The certification guidelines have not specified the validity period of the certification.

Q39. What is the relationship between the certification and the SCC?
For cross-border PI transfers, both mechanisms are applicable for data that escaped the mandatory threshold for the security assessment. However, an SCC is preferrable for PI export that occurs less frequently, whereas a certification is suitable for PI export among MNCs in daily business operations. Additionally, the current version of the SCC does not apply to scenarios in which data processors provide PI to overseas data handlers/processors. Unless the finalized version includes such scenarios, the only available mechanism might be a certification.

Q40. What rights are data subjects entitled to under the certification?
Data subjects are entitled to the following rights:

- The right to require the data handler and overseas recipient to provide a copy of the legal text involving their rights and interests
- The right to know and decide the processing of their PI
- The right to withdraw consent, restrict, or refuse the cross-border processing of their PI
- The right to access, copy, correct, supplement, or delete the PI transferred to overseas recipients
- The right to require PI handlers and overseas recipients explain their rules for cross-border PI processing
- The right to deny the data handler from making decisions based only on automated processes
- The right to report illegal PI processing activities to PRC authorities that perform personal information protection duties
- The right to bring judicial proceedings in the court of the data subject's usual place of residence against data handlers and overseas recipients conducting cross-border processing activities of PI
- Other rights stipulated by laws and administrative regulations

Important Data

Q41. What is important data?
According to Art. 19 of the Measures, "important data" refers to data that may endanger national security, economic operation, social stability, or public health and safety once it is tampered with, damaged, leaked, or illegally obtained or used.

Q42. What mechanism is available for cross-border transfer of important data?
As described in Q4, only the security assessment is available for cross-border transfer of important data.

Special Scenarios

Q43. Do any rules restrict the cross-border transfer of PI in specific industries?
Sectoral rules also regulate the cross-border PI transfer in different industries.

For example, in the financial sector, the Notice of the People's Bank of China for Banking Financial Institutes to Get the Personal Financial Information Protection Work Well Done (in Chinese) effective as of May 1, 2011, the cross-border transfer of personal financial information is prohibited in principle and is allowed only under exceptional circumstances.

In the health care sector, biometric data may be transferred abroad only under certain circumstances with prior approval by the competent authority under the Regulations on the Management of Human Genetic Resources (in Chinese) effective as of July 1, 2019, released by the State Council.

Q44. What are the rules for data cross-border transfer initiated by foreign judicial or law enforcement authorities?
Under the International Criminal Judicial Assistance Law (in Chinese), institutions, organizations, and individuals within the territory of the PRC are prohibited from providing evidentiary materials or assistance in connection with criminal proceedings to foreign countries without approval from the competent authorities.

With the Chinese government's intensifying awareness of data sovereignty, the DSL extended the restrictive scope from only international criminal judicial assistance to international judicial and enforcement assistance. It provides that no organization or individual within the territory of the PRC may provide foreign judicial or law enforcement authorities with the data stored within the territory of the PRC without the approval of the competent authorities, which undoubtedly includes PI.

Labor & Employment

ANALYSIS

Why Unionization Efforts May Run Out of Steam in 2023

by Francis Boustany
Legal Content Specialist, Bloomberg Law
Nov. 13, 2022

It's been hard to miss the successes that unions have amassed in election after election. Once perceived as a dying force in the private industry, unions have engineered a turnaround to reach their highest level of public approval since 1965.

But as we enter 2023, unions will face new challenges. Burgeoning expectations from newly minted bargaining units, growing employer resistance, and strengthening economic headwinds will be pivotal forces in determining whether recent union achievements represent a long-term shift in the American labor movement or a fleeting string of wins soon to be in the rear-view mirror.

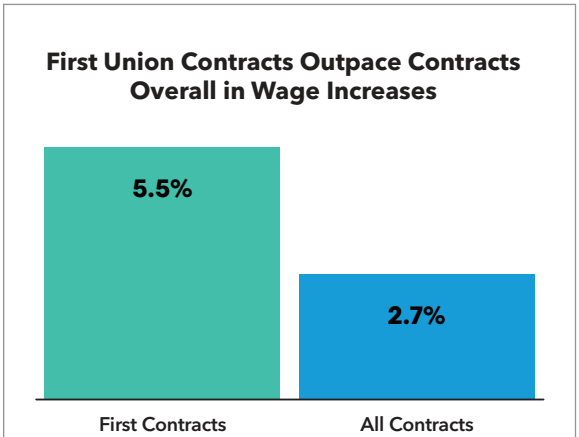
Bargaining: Higher Hopes, but Fewer Resources

Unions won hundreds of elections over the past year alone, and now they're expected to deliver on the promises they made in their organizing campaigns, from higher wages to improved benefits to better working conditions. However, the slow pace of bargaining negotiations and contract ratification may wear on the enthusiasm of even the most ardent supporters, risking the momentum and the media coverage that unions have recently enjoyed.

An analysis of Bloomberg Law's labor data showed that the average number of days it takes for employers and new bargaining units to ratify their first contract is 465 days. This means that a newly formed bargaining unit we hear about today will likely not have a collective bargaining agreement in place until 2024.

That is a long time to wait.

Beyond this, new bargaining units likely have high expectations for their negotiators, as a union's first contract typically includes large wage increases—particularly when compared to raises negotiated during contract renewal sessions.



Source: Bloomberg Law Data. Analysis compares the mean for 623 initial contract settlements ratified 2004-2022 with the annual mean for the 12,888 contracts ratified over the same time period. Wage increases do not include lump sum amounts like signing bonuses.

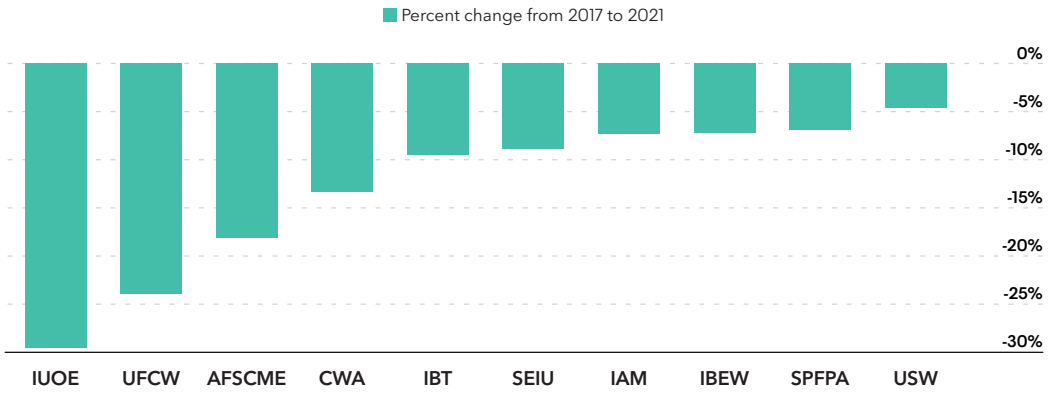
However, workers expecting to hit these kinds of raises will probably be disappointed.

Moving into 2023—when the initial collective bargaining will occur for many newly formed bargaining units— unions and their most effective negotiators will likely be spread thin nationally, essentially having to utilize the same staffing and funding levels they've had in leaner years to negotiate a far greater number of contracts.

This will be particularly concerning to new bargaining units, as the unions that are most active in organizing have had to decrease their spending on representational activities—which includes bargaining negotiations—between 2017 and 2021.

Even if unions secure and utilize the necessary funds, there's no guarantee that they will be able to recruit the seasoned labor-side lawyers and professionals needed to successfully bargain for all newly formed bargaining units. This could equate to fewer improvements in wages, benefits, and working conditions than newly formed bargaining units typically expect.

When the reality sets in that winning a representation election is just the beginning, some workers might become discouraged—and others may peel away from the movement altogether.



Source: US Department of Labor. Percentages show 2017-to-2021 changes in spending on "representational activities" aslisted in annual reports (Form LM-2) filed by the 10 unions with the most NLRB elections during that period. Some unions' reporting years do not align with calendar years.

Employers Are Ready for a Fight

Unions may be winning representation elections in large numbers, but employers have taken note and are better preparing on multiple fronts.

From standard forms of unionization prevention (read: union busting) to challenging election administration to fighting outright with the National Labor Relations Board (NLRB), employers have several options available to them to fight unionization efforts. They will likely use the tools available to fend off union support among employees by discussing the less glamorous realities of unionization, regulating solicitation and distribution, and limiting activities of non-employee union members.

And they may win the long game doing so.

In 2023 we will see broadened employer efforts to stop the spread of labor activities nationwide. It is likely that more employers will expand the labor relations arm of their legal teams to prepare for legal challenges, double down on challenging elections, raise concerns of irregularities in said elections, and allege that unions are using unlawful tactics to gain support (although claims of free cannabis giveaways might not gain widespread usage).

And while it's unclear whether any employer challenges would overcome union wins in elections, it is probable that they will succeed in some critical facets: slowing down unions' momentum (which can lead to lower raises in negotiations), stalling progress toward collective bargaining, and wearing on the patience of union-supporting employees.

The Elephant in the Room: Economic Instability

There are economic headwinds ahead in 2023. The risks of global and US recessions (some putting the US risk at 98%), inflation, and a slowing job market expose the entire global economy to instability—and the US labor movement is no exception.

And if an economic downturn materializes, unions might feel pressure from multiple angles.

To start, employees may be less willing to participate in union organizing activities if the job market tightens and they feel that their jobs are in danger.

While it is true that the jobs of unionized employees, particularly those covered by a CBA, are better protected than non-unionized employees, those who consider starting a union at an organization may think twice before joining an organizing effort.

They may see retaliation as a real possibility, even though employer punishment for concerted action is unlawful under federal labor law. Or they may feel like the threat of unionization would put an employer in a worse economic position, necessitating layoffs before an organizing drive even has the chance to begin.

In addition to the personal risks for employees, union leaders themselves may be hesitant to negotiate boldly during an economic downturn, due to employers having fewer resources to fund expanded benefits or increased wages.

If a recession materializes in 2023, there is a real potential that newly organized bargaining units will be at a disadvantage when it comes to their first time at the table, threatening their ability to win additional wages or benefits.

Unfavorable collective bargaining outcomes, combined with fear of employer retaliation, may ultimately steer employees who would have engaged in organizing efforts in 2020, 2021, or 2022 away from such behavior in 2023.

Amid an economic downturn, increased employer challenges, and looming concerns about the effectiveness of newly formed bargaining units, 2023 looks like it could be a challenging year for the US labor movement. How unions, their bargaining units, and their supporters handle these challenges will make next year a make-or-break year for the momentum that unions hope to maintain.

ANALYSIS

New Laws, Culture Shifts Push Pay Transparency Forward

by Dori Goldstein
Legal Analyst, Bloomberg Law
Nov. 13, 2022

California is the latest state to enact a new type of pay equity law that requires employers to include pay ranges in job descriptions. This follows a larger trend of states and individuals using pay transparency to shrink the ever-present pay gap.

Look for that trend to continue, as state laws and the changing culture around money push conversations about pay into the spotlight in 2023.

Transparency Laws Evolve

California's recent pay transparency law has been grabbing headlines, but laws aimed at giving employees more power in how they talk about and negotiate their pay are nothing new. Since the passage of the National Labor Relations Act in 1937, both unionized and non-unionized employees have successfully argued that Section 7 protects workers' right to discuss their wages, and a slew of states have their own laws protecting workers from discrimination or retaliation if they disclose their pay.

Roughly 20 states have gone further to adjust the power imbalance in wage negotiations by banning or restricting the use of salary history during the hiring process.

Pay transparency laws like those in California and Colorado, which require pay ranges in job postings, and laws like those in Connecticut and Nevada, which require the pay range for a position to be disclosed during the hiring process or upon request, force employers to speak first.

What makes these pay transparency laws such game-changers for employers is that the laws will fundamentally alter the way many employers set salary rates. Currently, some employers set a range for a position and stick to it, while others set a range for each candidate. This candidate-focused approach has a lot of benefits for employers—it can give them more flexibility in what candidates they consider, and it can allow them to meet the market of available candidates where it is (something that's particularly useful right now). But it can also lead to wide variations in pay for a particular job classification, and can result in workers being paid very differently for the same work. Pay transparency laws will force employers to shift to a position-focused approach.

Employers who are already feeling uncomfortable with this type of transparency should brace themselves for more. Not only are more states working on pay transparency laws, but the Securities and Exchange Commission is poised to require specific reporting related to human capital management, potentially including disclosures related to pay.

The Culture Shift

As fast as states are acting to move the needle on pay, the culture around pay is moving even faster. The pandemic, its recovery, and the resulting "worker shortage" have created a new generation of workers who know what they want from a job and aren't afraid to ask for it.

This mindset is most visible when it comes to talking about pay. Younger workers are dramatically more comfortable sharing their income than their older counterparts. And they don't just share it with their coworkers—they share it with strangers on the street. They post about it on social media. They share strategies for negotiating pay and for asking for a raise. They offer tips on breaking into different industries.

If employers are feeling safe because pay transparency laws haven't (yet) come to their state, they shouldn't: Whether or not it's in a job posting, employees are discussing, comparing, and assessing their pay.

Turmoil, Lawsuits, and Equity?

Most employers have already felt the effects of the pay transparency movement. It probably helped fuel the great resignation, and the movement will continue to fuel resignations as long-term workers start to discover their recently hired coworkers are being paid more because they were hired in a more competitive job market.

Increased pay transparency will reveal instances of unlawful pay discrimination and will open employers up to more lawsuits. Gender and race pay gaps exist, and bringing them into the light will almost certainly lead to litigation.

But will it close the pay gap? That's a tougher question. The pay gap is stubborn, but innovative transparency laws and a real culture change are a powerful duo.

Responding to Change

Most employment law issues can be prevented with a clear policy that's consistently enforced. Addressing pay transparency will require more than just a policy from employers, however.

Instead, employers will need to audit worker pay—both to uncover unlawful discrimination and to reveal unfairness. They will need to take steps to ensure that pay practices are fair, consistent, and nondiscriminatory—even if that means a lot of raises. It's better for everyone if employers can uncover these issues and address them proactively than it is to battle through lawsuits and resignations.

But with labor costs soaring, giving "a lot of raises" won't be an option for every employer, especially ahead of what many are predicting will be an economic downturn. There's no easy answer for employers in that position. Pay audits that reveal discrimination can be used against employers in pay discrimination lawsuits if they fail to remedy the discrimination, but waiting for pay transparency laws to reveal inequities isn't a great plan either. Conducting pay audits in segments, and realigning job duties to better match pay are two options that could help ease the burden on employers.

However employers choose to proceed, they should prepare to answer questions about pay. Despite the changing culture around transparency, asking for a raise can be scary and emotional for employees. Employers that are sensitive to that will fare best at building and retaining their workforce.

ANALYSIS

After Midterms, Biden Eyes Employment Changes in 2023

Noah Jennings, Legal Analyst, Bloomberg Law

Democratic legislative priorities like raising the minimum wage or enacting the Protecting the Right to Organize Act will face steep obstacles next year because of a divided Congress. Lacking a viable path to pass new labor and employment legislation, the Biden administration will turn to executive orders and rulemaking to expand worker protections, raise wages, and strengthen organizing rights.

Democratic legislative priorities like raising the minimum wage or enacting the Protecting the Right to Organize Act will face steep obstacles next year because of a divided Congress. Lacking a viable path to pass new labor and employment legislation, the Biden administration will turn to executive orders and rulemaking to expand worker protections, raise wages, and strengthen organizing rights.

Rewriting Worker Classification

Steps to redraw the boundaries between contingent workers and employees are already in motion. On Oct. 11, the Biden administration announced a new regulation that would redefine the legal test for determining who is an independent contractor.

The proposed rule lists six factors to consider that determine whether a worker should be classified as an employee or contractor:

- the worker's opportunity for profit or loss;
- investments by the worker and the employer;
- the degree of permanence of the work relationship;
- the nature and degree of the employer's control over the work;

- the extent to which the work performed is an integral part of the employer's business; and
- the skill and initiative exhibited by the worker.

Weighing these factors would inform whether, under a "totality-of-the-circumstances" analysis, the worker is economically dependent on the employer or is in business for themselves. The new standard revives a version of the "economic realities test" used by courts before the Trump administration implemented a more employer-friendly rule in 2021.

Some legal analysts have compared the new regulations to California's "ABC test," which requires employers to meet three requirements in order to classify a worker as an independent contractor. However, the new regulation is decidedly less strict than the ABC test: Unlike the ABC test, no single factor would be dispositive.

Independent contractors are more flexible, cheaper, and less regulated than employees. Instead of paying full-time employee wages, employers can engage a contractor on an as-needed basis. Contractors aren't covered under the FLSA and are thus not entitled to overtime and minimum-wage protections. Employers can also save costs because they don't have to cover contractors' health benefits.

While the rule will likely result in numerous current contractors being reclassified as employees, it's unlikely to cause a drastic change that would abolish the "gig economy" pioneered by ride-sharing companies like Uber and Lyft. In fact, noted gig employers appear open to the proposal; a statement from Uber described the proposed regulations as a "measured approach."

Still, business groups have voiced concern about the new standard, arguing that it creates undue costs, burdens, and confusion for employers. While litigation is likely, the proposed rule is largely a return to a tried and tested legal standard.

Barring any successful legal challenges, the new rule will tighten the independent contractor definition and make more workers eligible for the benefits of being an employee.

Boosting Pay for Exempt Employees

Employers should also expect the Biden administration to raise the minimum salary threshold for executive, administrative, and professional employees to be considered exempt from earning overtime. President Biden ran on a platform to extend overtime pay to additional workers, and the administration began taking concrete steps toward raising the salary threshold earlier this year. In June testimony before the House, Labor Secretary Marty Walsh described the current salary threshold of $35,586 ($684 per week) as "definitely" too low.

Later that month, the Department of Labor signaled that it would release draft regulations to update overtime exemptions in the fall. Although the administration apparently prioritized updates to the worker classification rule instead, employers should also get ready for the administration to raise the minimum salary threshold.

The height of the threshold remains an open question. The Obama administration previously attempted to raise the threshold to $47,476 ($913 per week), but its efforts were blocked in 2016 by a federal court. The current $35,586 threshold was set in 2019 by the Trump administration. Progressives in Congress have called on Biden to raise the threshold to above $82,000. Unsurprisingly, business groups have protested any new requirements that enforce higher wages.

To qualify under the executive, administrative, or professional exemptions to federal wage laws, employees must perform duties related to their exemption and earn a salary at or above a minimum threshold. If the minimum threshold goes up, employers will have to decide what to do with workers who continue to meet the duties test but not the salary test: Change their status and pay them for overtime, or keep them exempt by increasing their salaries. Either way, raising the salary threshold for exempt employees will raise pay for millions of workers.

Department of Labor officials are likely wary of another legal challenge; the Obama administration's regulation was overturned because a federal judge held that its salary bump was too drastic. While an exact figure hasn't been discussed publicly, the Biden administration will probably seek a modest adjustment in the range of the $47,476 minimum proposed six years ago under Obama.

So, even though Democrats may be unable to push a new minimum wage increase through Congress, many American workers are still in for a pay raise.

Strengthening Organized Labor

Finally, the Biden administration will flex its powers to strengthen union rights for organized labor. After campaigning to be "the most pro-union president" in US history, Biden is now facing pressure from labor groups to make good on his promise.

Executive efforts to strengthen union power began in early 2021, when the White House formed a labor task force dedicated to expanding union rights via executive order.

The task force released a report earlier this year that provided more than 60 recommendations to expand workers' access to unions. Although proposed orders or regulations to implement the task force's recommendations haven't been made public, Biden is likely to announce related measures in the coming year, focusing on these issues:

Reviving the "persuader" rule. Biden will adopt a regulation from the Obama administration's playbook that strengthens disclosure requirements for anti-union activity. Like his Democratic predecessor's 2016 rule, which was ultimately jettisoned by the Trump administration in 2018, Biden's measure will require businesses to disclose spending on anti-union consultants, or "persuaders," engaged to counter employee organizing.

Ensuring workers know their rights. The White House will increase educational resources for employees seeking to organize. The task force has already launched an online resource center on unions and collective bargaining, and will increase employer notice requirements.

Stepping up enforcement. The NLRB will become more aggressive in actions against employers accused of anti-union violations. Just last month, the NLRB announced new efforts to streamline Section 10(j) relief for organizers in enforcement actions. Similar initiatives and heightened enforcement are likely.

More expansive labor proposals like allowing secondary strikes or "closed shop" unions are off the table, since they would require legislative action.

But even without Congress's help, Biden will still be able to push through executive actions to deliver Democratic labor policies and expand workers' rights.

Whether these actions stand up in courts will be determined in the years to come.

ANALYSIS

Mental Health Benefits Become Key to Worker Retention

by Christina Bethune
Legal Content Specialist, Bloomberg Law
Nov. 13, 2022

Employers grappling with the post-pandemic worker shortage have been innovating with new ways to hire and retain workers. But with salaries soaring, many are still struggling to find a path forward, and workers are stressed, burned out, and leaving.

To differentiate themselves from the competition in 2023, employers should consider redefining their employee value proposition to demonstrate their commitment to their workers' well-being from the start of the employee-employer relationship.

Employers should also consider using lessons learned from the pandemic to innovate and expand their mental health-related benefits and to increase awareness of existing offerings to attract and retain employees.

Expand Access to Mental Health Services

During the Covid-19 pandemic, the lines between work and home blended for many employees. Working women and children often bore the brunt of the fallout from the pandemic. School and day-care closures, the demands of remote work and virtual school schedules, and the loss of loved ones all contributed to a prolonged period of isolation.

All of that can take a toll of its own. As highlighted in a 2022 report by US Surgeon General Vivek Murthy, competing work and personal demands can often magnify psychological stress. Also, employees with children may need additional support to help their children adjust to post-Covid life. This was reinforced by the US Preventive Services Task Force's Oct. 11 recommendation that all children and adolescents ages 8 to 18 years old be screened for anxiety.

In addition to coverage for mental health services, employers looking to demonstrate their commitment to employees' well-being should continue to promote parent-friendly policies and practices in the workplace such as:

- parental leave and paid time off;
- flexible scheduling, such as remote or hybrid work, compressed work weeks, flextime, and summer Fridays;
- emergency child care;
- a culture where employees feel safe taking mental health days; and
- training programs aimed at teaching managers to identify and have tough conversations with employees that might be experiencing mental health issues.

Increase Access to Treatment

Telehealth represents a growing segment of the health-care sector. Early in the pandemic, the Medicare program expanded telehealth access for beneficiaries. In addition, many states lifted licensing barriers, allowing doctors to treat patients remotely. With this in mind, employers should look to expand telehealth offerings, especially for mental health services. In addition, employers can offer plans with more in-network behavioral health providers, despite the current shortages of behavioral health providers.

Finally, employers can turn to employer-sponsored EAPs and benefits providers that provide workers with free therapy, coaching, and self-guided care sessions, using various modalities such as live video, live messaging, in-person visits, phone calls, or onsite care.

Renew Focus on Mental Health Parity

In 2023, employers will face more scrutiny in the form of increased litigation over mental health parity, heightened compliance enforcement, and possibly even new legislation. To get ahead of this trend, employers should take a more active role in ensuring that their insurers and third-party administrators are complying with mental health parity requirements.

The Mental Health Parity and Addiction Equity Act requires mental health and substance use disorders to be covered by insurance plans to the same extent that coverage is provided for medical and surgical benefits. The Biden Administration has emphasized

a focus on mental health parity enforcement. Meanwhile, states are still struggling to enforce mental health parity laws.

In September, the House passed the Mental Health Matters Act. This bill, if signed into law, would provide the Department of Labor with strengthened authority to enforce mental health parity violations.

Focus on Equity

Employers can reinforce their commitment to diversity, equity, inclusion, and accessibility by promoting mental health-friendly policies and practices in the workplace.

This can be an especially valuable retention practice for employers of health-care workers, caregivers, members of historically marginalized communities, and other population segments that employees can identify as adversely impacted by the Covid-19 pandemic.

Remove the Stigma

Employers can also find innovative ways to engage employees in activities, such as "lunch and learn" conversations and social media video campaigns, which facilitate shared learning experiences. Employees may be more likely to utilize mental health benefits if they build trust with their peers and feel a sense of belonging.

To retain and recruit top talent in 2023, employers are going to have to meet employees where they are in the workplace. The connection between employee well-being and employee productivity is undeniable. Home demands can negatively affect employees, and employees are more likely to perform better at work when their whole person is supported by their employers.

ANALYSIS

Six Degrees of Classification Could Upend Gig Work

by William Welkowitz
Legal Content Specialist, Bloomberg Law
Nov. 13, 2022

Federal agencies, as well as some state governments, have begun to more broadly define what an "employee" is for official classification purposes.

The issue of whether a worker should be considered an independent contractor or an employee is more important than ever because of new technologies that make the national workforce more mobile and flexible. As a result, important service industries rely more and more on independent contractors (many of whom are gig workers) as a significant portion of their own workforces.

These independent contractors could gain significant benefits in the coming year if a rule proposed by the Biden administration to more broadly define what an "employee" is becomes reality.

Biden Administration's Proposed Rule

The battle to define the term "employee" for purposes of classification under federal and state labor and employment laws isn't new. Currently, the Biden administration's priorities on this issue are being formalized through the rulemaking process. On Oct. 13, the Department of Labor's Wage and Hour Division published a notice of proposed rulemaking that would rescind the Trump administration's rule on the subject.

In addition, the new rule would do the following:

- align the department's approach with courts' FLSA interpretation and the economic realities test;
- restore the multifactor, totality-of-the-circumstances analysis to determine whether a worker is an employee or an independent contractor under the economic realities test;
- revert to the longstanding interpretation of the economic reality factors;
- ensure that all factors are analyzed without assigning a predetermined weight to a particular factor or set of factors; and
- assist with the proper classification of employees and independent contractors under the FLSA.

This new method to determine the meaning of "employee" would generally favor those arguing that gig workers and other independent contractors are being misclassified as such by employers and should be classified as employees instead. The outcome of this shift could mean that these individuals would become eligible for benefits such as overtime, health insurance, and paid leave. In addition, they would gain protections under EEO and other employment rights laws.

In particular, there are six prevalent issues that would affect the legal outlook in labor and employment law, should the proposed rule be implemented.

1. Payroll Issues
Independent contractors aren't legally entitled to the FLSA's minimum wage or overtime pay coverage like employees are, with exceptions in some states. They also don't receive workers' compensation. Under the new rule, more workers are likely to be classified as employees and are therefore entitled to coverage under the FLSA, as well as eligible for workers' compensation.

2. Benefits
In recent years, several states have adopted laws that require employers to provide a certain amount of paid leave to their employees. In addition, the federal Affordable Care Act now requires employers with at least 50 employees to offer health insurance or health coverage to all of their workers. Furthermore, ERISA imposes certain requirements on private employers that provide pension and retirement plans to their employees, and there are certain states that impose requirements on private employers to provide retirement savings plans to their employees.

However, independent contractors aren't generally covered by these laws. Under the new rule, more employers will be required to spend more money as a part of the cost of doing business in order to offer health insurance to their workers and administer retirement benefit plans.

3. EEO Protections
Many of the protections provided to employees under Title VII and other federal nondiscrimination laws don't apply to independent contractors. For

cases involving employment discrimination, courts use the "economic realities" test to determine whether someone is an employee or an independent contractor. This test has a litany of factors a court can consider in its determination, although the most important factor is usually the extent to which an employer can control the means and manner of the worker's performance.

An expanded definition of "employee" issued by the DOL is likely to alter whether some of these factors are deemed present, as well as how these factors are weighed, in individual cases.

4. Union Organizing
Under the NLRA, independent contractors don't fall under the NLRB's jurisdiction. This means that unlike employees, independent contractors can't form a union or collectively bargain with their employers. While the NLRB is generally free to come up with its own rule of what constitutes an "employee" within the NLRA's parameters, a formal rule issued by a DOL division could prompt the NLRB, another DOL division, to adopt the rule's definition for its own legal analyses.

A broader definition of "employee" could open up new worker groups to unionization drives than we're seeing now, which would extend labor protections to an even greater percentage of the workforce.

5. Tax Commitments
For anyone considered an employee under the Internal Revenue Code, the employer must withhold certain taxes from the employee's paycheck—such as Social Security, Medicare, and state and federal income taxes—that they don't have to for an independent contractor's payment. In addition, an employer must pay a certain amount of money to the IRS in payroll taxes for each worker classified as an employee. Independent contractors, on the other hand, aren't subject to the payroll tax requirement.

This change in status will likely lead to higher taxes and more paperwork for employers. The new definition could also affect whether an employer would be required to pay federal and state unemployment insurance taxes.

6. Worker Safety
The DOL's new regulation would also affect whether a worker is considered an employee or an independent contractor for the purposes of being protected by OSHA regulations. Although there's no formal authority on this issue, it's generally accepted that the agency excludes "self-employed workers"—a widely understood term for independent contractors—from OSHA jurisdiction. As a division of the DOL, OSHA would follow the department's rules and guidelines in determining who is an employee and who is a "self-employed worker."

State Action, Legal Challenges

In addition to the federal government, multiple states have also begun to reassess how they define who is an employee and who is an independent contractor. Because there's currently no single national standard for worker classification, each state determines on its own what standard to use for this determination. The two most common standards are the ABC test and the common-law test, with some states opting to use part, but not all, of the ABC test. (Even the various federal agencies differ in which test they use for this determination. For example, the DOL uses the ABC test, while the IRS uses the common law test.)

In all likelihood, barring any serious court challenges, the proposed rule will go into effect in early 2023 with few (if any) amendments to the current proposal, and will remain in place through at least the end of the Biden administration. It's doubtful that any court activity would alter this trajectory based on past precedent. After the Biden administration ends, the rule could be altered or rescinded through a subsequent round of rulemaking, depending on who becomes the next president—as is wont to happen for every new administration, especially if there's a different political party in control.

CHECKLIST

Employer Considerations Post-*Dobbs* (Annotated)

Editor's Note: On June 24, 2022, the U.S. Supreme Court ruled that the U.S. Constitution does not confer a right to abortion, permitting states to allow, regulate, or ban abortion. See Dobbs v. Jackson Women's Health, No. 19–1392.

This checklist outlines the major considerations for employers in light of the *Dobbs* ruling. For information about state abortion laws, see State Chart Builder: Reproductive Health – Provision of Abortion Services.

On December 29, 2022, President Biden signed the Consolidated Appropriations Act, 2023 into law, which included the Pregnant Workers Fairness Act (PWFA). Effective on or around June 27, 2023, the PWFA requires employers with 15 or more workers to provide reasonable accommodations for qualified employees' known limitations related to pregnancy, childbirth, or related medical conditions unless providing the accommodations would impose an undue hardship on the entity's business operations. The PWFA also bars discrimination or retaliation based on pregnancy status, childbirth, or related medical conditions.

While the U.S. Supreme Court did not specifically mention labor and employment laws in the *Dobbs* opinion, the ruling will impact employment practices, terms of employment, benefits, and employee relations. When navigating the labor and employment aspects of *Dobbs* employers must consider:

Discrimination Protections

- **Pregnancy discrimination:** The Pregnancy Discrimination Act, an amendment to Title VII of the Civil Right Act, protects individuals from pregnancy-related discrimination. See 42 U.S.C. § 2000e-2. While the act does not explicitly protect workers from discrimination related to abortion, guidance from the Equal Employment Opportunity Commission (EEOC) interprets the law as prohibiting an employer from discriminating against an employee because they have, have had or have contemplated an abortion. EEOC's stance has not changed in response to the decision in *Dobbs*. See EEOC's Enforcement Guidance on Pregnancy Discrimination and Related Issues. In addition to federal law, some states have implemented laws that prohibit discrimination related to abortion or reproductive choices. For more information, see State Chart Builder: Pregnancy Discrimination.
- **Disability discrimination:** Pregnancy itself is not covered by the Americans with Disabilities Act (ADA), but employees may be protected by the ADA if they have a disability or become disabled during their pregnancy. See Point of Law. Employers should engage in their standard ADA interactive process to make determinations on any disability accommodation request. See Flowchart – ADA Reasonable Accommodation Interactive Process. State disability discrimination statutes may provide more protections than federal law for employees who contemplate or have an abortion. For more information, see State Chart Builder: Disability Discrimination.
- **Political beliefs or affiliation.** While no federal law prohibits private employers from discriminating against employees based on their political beliefs or affiliation, some states have enacted laws that do. When operating in states with these protections, employers should be cautious in how they implement and enforce policies related to political displays or discussions. For more information, see State Chart Builder: All EEO Topics, Lawful Activities.

Comment: Under Section 7 of the NLRA, an employer must not take adverse action against employees who engage in concerted activities regarding their terms of employment – including discussions or actions regarding employer-provided abortion benefits – as this could be a violation of the NLRA and result in an unfair labor practice charge. See *Eastex, Inc. v. NLRB*, 437 U.S. 556, 98 LRRM 2717 (1978); Overview – Concerted Activities Protected Under Section 7 of the NLRA (Annotated), Checklist – NLRA Concerted Activity Compliance Pitfalls (Annotated); NLRB's About NLRB – Employee Rights.

Leave Considerations

- **Family and Medical Leave Act (FMLA) Leave:** Under the federal FMLA, employees can be entitled to leave if they have a qualifying serious health condition. If employees request FMLA leave for an abortion or the subsequent healing process, employers should engage in the same approval process they would with other serious health conditions. For more information, see Checklist – Handling FMLA Requests (Annotated).
- **State Leave Laws:** State leave laws may provide different or additional leave benefits for employees who seek an abortion beyond those provided by the FMLA or the ADA. For more information, see State Chart Builder: Reasons for Leave Chart – Pregnancy, Childbirth, and Related Conditions.

Benefits Considerations

- **Travel, leave, and abortion reimbursements benefits:** Employers may consider providing travel costs, abortion-related paid or unpaid leave, and/or abortion reimbursement benefits for employees who must travel out of state or a certain distance to obtain an abortion. These programs are permitted under federal law but existing benefits and tax laws will still apply to any additional benefits employees are offered. Additionally, employers must consider state criminal law on abortion when determining whether to provide these benefits, as financially assisting an employee in obtaining an abortion may be criminalized in certain jurisdictions. See State Chart Builder: Reproductive Health – Provision of Abortion Services.
- **Insurance coverage (federal law):** Under Title VII as amended by the Pregnancy Discrimination Act, employer-provided health insurance plans must cover abortion when the life of the individual would be endangered if the fetus were carried to term as well as cover medical complications that have arisen from an abortion (regardless of whether the underlying abortion was covered by an employer's health insurance plan). See 42 U.S.C. § 2000e(k).

Comment: While *Dobbs* has not directly struck down this law, employers will have to consider state law on abortion when determining whether a plan should cover abortion. See State Chart Builder: Reproductive Health – Provision of Abortion Services. It is currently unclear and remains to be litigated whether the PDA would preempt state law on this matter.

- **Insurance coverage (state law):** If an organization has a self-insured health plan, ERISA may preempt state law on abortion coverage in a health insurance plan. Employers must consider ERISA implications when determining what, if any, abortion-related services to cover in a health insurance plan.

Comment: While ERISA will usually preempt state insurance law on self-insured health plans, there will likely be future litigation regarding whether ERISA preempts specific state insurance and criminal laws related to abortion. If an employer has a fully insured health plan, it will have to follow state law regarding abortion benefits, as ERISA preemptions only apply to self-insured plans. See 29 U.S.C. § 1144.

- Collective bargaining agreements. If a unionized employer plans on adding or removing abortion-related benefits, they must consider whether these are covered by a collective bargaining agreement and the steps to change these benefits, if so. For more information, see Document Description – Collective Bargaining Agreements and Checklist – Collective Bargaining Agreement Negotiations (Annotated).

PRACTICAL GUIDANCE

Overview – Pay Transparency Laws

Pay transparency laws, which require employers to disclose wage information to job applicants and employees in certain situations, are becoming more common and expansive. These laws come in many different forms and require employers to disclose different kinds of wage information at different points in the recruitment process or the employment relationship. For more information, see State Chart Builder: Wage Disclosure.

The laws often have similar goals including a focus on promoting pay equity among genders, races, and other classifications by providing applicants and employees with an idea of where the hourly wages or salary they are offered fall in comparison to the overall pay range for their positions.

Pay Transparency in Job Postings

Some of the most expansive pay transparency laws are those that require employers to include wage information in job postings. In addition to including salary or hourly wage ranges, some laws also require employers to disclose information about other forms of compensation and benefits in their job postings. See C.R.S. § 8-5-201. When recruiting in a jurisdiction that requires wage information in job postings, employers must review the law to determine exactly how to comply and must also gather wage information to be furnished in the job posting.

Remote positions present other considerations on this front as well. Employers must follow the laws of the jurisdictions where they recruit when they post remote jobs. If employers are not located in a jurisdiction that has these requirements and wish to post a remote job, they have to consider whether they want to accept applicants from jurisdictions that require wage information in job postings or if they want to exclude applicants from those jurisdictions. If they choose the former, they will have to include the required wage information in job postings. If they choose the latter, they will not.

Required Pay Transparency in the Recruitment Process

Many jurisdictions have laws that require employers to automatically disclose wage information, such as salary and hourly rate ranges, to applicants at some point in the recruitment process. Some of the most common points in the recruitment process when an employer must disclose wage information include:

- After an initial interview;
- When current employees switch positions;
- When current employees are promoted;
- At the time of an offer; or
- At the time of hire.

These laws present compliance considerations for employers both when they are hiring in a specific jurisdiction as well as when they are hiring remote positions. When hiring in a specific jurisdiction, employers should research whether any of these laws apply in the jurisdiction and, if so, should be prepared to disclose wage information at the required point in time. Alternatively, when hiring for remote positions, employers must consider the jurisdictions of their applicants and ensure wage information is provided to applicants at the required time in the recruitment process.

As with applicants in jurisdictions that require wage information in job postings, employers can decide to not recruit in areas with pay transparency requirements in the recruitment process.

Pay Transparency Information by Request

The least stringent of pay transparency laws are those that allow applicants to request wage information at certain points in the recruitment process. These laws alleviate employers from being required to disclose wage information at a certain point in the recruitment process. And while these laws do require employers to provide wage information if requested at the appropriate time, they put the onus on the applicants or employees to know when to request it.

Some of the most common points in the recruitment process when this classification of law allows employees to request wage information include:

- At any point in the recruitment process;
- After an initial interview;

- When current employees switch positions;
- When current employees request said information for their current role;
- At the time of an offer; or
- At the time of hire.

When employers recruit new employees, they must determine whether laws that require pay transparency by employee request apply. If they do, employers must comply with the law and provide wage information when requested at the appropriate time. As with applicants in jurisdictions that require wage information in job postings or at certain points in the recruitment process, employers can decide to not recruit in areas with pay transparency requirements in the recruitment process.

CHECKLIST

NLRA Concerted Activity Compliance Pitfalls (Annotated)

Editor's Note: The National Labor Relations Act (NLRA) applies to more than just unionized employers and employers with unionization efforts in motion. Under Section 7 of the NLRA (Section 7), employees of both unionized and nonunionized employers are provided the right to engage in concerted activities for the purposes of mutual aid and protection. This has broadly been interpreted to allow employees certain rights when it comes to activities and speech related to working conditions. Employers must be wary when disciplining or establishing policies that may impact their employees' Section 7 rights, as a violation of these rights may result in an unfair labor practice (ULP) and entitle employees to remedies such reinstatement or back pay. See NLRB Remedies: Reinstatement and Back Pay.

For more information on complying with these provisions, see Overview – Concerted Activities Protected Under Title 7 of the NLRA (Annotated).

This checklist provides employers with a tool to audit current practices and policies to ensure that they do not inadvertently violate employees' Section 7 rights as they relate to concerted activity for mutual aid or protection.

Wage Discussion Bans

Policies that ban wage discussions among employees are barred under Section 7, as these discussions are protected concerted activity. Additionally, disciplinary action taken against employees that discuss their wages are a violation of Section 7, even if an employer does not have an official policy banning such discussions. If an employer implements such a policy or takes such a disciplinary action, the NLRB considers this an ULP. See *NLRB v. Brookshire Grocery Co.*, 919 F.2d 359, 136 LRRM 2136 (5th Cir. 1990).

Social Media Activities

The proliferation of social media provided a new avenue for employees to discuss working conditions, wages, and their employers. In response, employers understandably wish to limit some of the things that employees post on social media platforms. NLRB rulings create employer restrictions on limiting employee speech on social media but also provide employers with leeway to regulate some employee speech online.

Employers may not implement policies banning employees from discussing or sharing about pay, benefits, working conditions, and other related issues on social media, nor may they discipline them for these activities as long as the activity is concerted in nature. However, the NLRB stated that employers that discipline employees for individually "griping" about these topics on social media may not face an ULP if the employee's post did not:

- Have a relationship to group action;
- Seek to initiate, induce, or prepare for group action; nor
- Bring a group complaint to the attention of management.

Therefore, while employees may post about the aforementioned topics on social media, they do not have blanket protections when they do.

Comment: Concerted activities are not limited to those that occur in-person, and social media present opportunities for employees to engage in them online. For more information, see the NLRB's About NLRB: Social Media and About NLRB: The NLRB and Social Media.

Confidentiality Policies

Confidentiality policies are important to employers, as they help to ensure that their important business information (e.g., trade secrets and client information) is kept confidential. While confidentiality policies are not barred by Section 7, there can be elements in confidentiality policies that violate Section 7 rights.

Employers should carefully define "confidential information" and word policies to ensure that they do not interfere with Section 7 rights. For example, employers should not mandate that employees keep wages, working conditions, or other Section 7-protected information and activities confidential. However, confidentiality policies can bar employees from disseminating a wide range of business-related information such as intellectual property, business strategies, security methods, and customer lists.

Comment: Section 7 makes it an ULP for employers to implement confidentiality policies that bar employees from discussing topics outlined above. Generally, facially neutral confidentiality policies will be analyzed under an "objectively reasonable employee" standard, which evaluates whether an "objectively reasonable employee would understand that the

Confidentiality Agreement applies only to the Respondent's proprietary business information and would not interfere with employees' Section 7 rights." See *Argos USA d/b/a Argos Ready Mix, LLC*, 369 N.L.R.B. No. 26, 2020 BL 40726.

However, confidentiality policies that bar discussions of ongoing workplace investigations are considered presumptively lawful, but confidentiality policies that bar discussions about closed investigations do not receive this presumption. See *Apogee Retail LLC d/b/a Unique Thrift Store*, 368 N.L.R.B. No. 144, 2019 LRRM 481637, 2019 BL 481637 (2019).

Confidentiality policies (or other employer policies) that define employee handbooks as confidential and bar their discussions or disclosures violate Section 7, but policies can bar employees communicating information about the business proprietary information, such as intellectual property and customer lists. See *Motor City Pawn Brokers, Inc., Aubrey Brothers, LLC (d/b/a Motor City Pawn Brokers II), The Aubrey G.*, 369 NLRB No. 132, 2020 BL 277298.

Mandatory Arbitration Agreements

Employers that implement mandatory arbitration agreements must be careful to not infringe upon employees' protected Section 7 rights. Specifically, mandatory arbitration agreements that require employees to arbitrate all disputes that arise under the NLRA and procedural limitations on such claims can violate Section 7. See *Motor City Pawn Brokers, Inc., Aubrey Brothers, LLC (d/b/a Motor City Pawn Brokers II), The Aubrey G.*, 369 NLRB No. 132, 2020 BL 277298. However, mandatory arbitration policies that contain class action and collective action waivers related to wage and hour disputes are not a violation of Section 7. See *Epic Sys. Corp. v. Lewis*, 138 S. Ct. 1612, 211 LRRM 3061 (2018). Moreover, employers are not prohibited from informing employees that failure to sign a mandatory arbitration agreement will result in discharge.

Non-Disparagement Agreements

Non-disparagement agreements allow employers to protect themselves from employees' public criticisms of their organizations, but non-disparagement agreements can violate Section 7. When crafting non-disparagement policies, employers should be careful to ensure that the policies do not limit protected Section 7 rights, such as employees' rights to engage in concerted activities regarding wages, working conditions, or safety conditions at the workplace. In many instances, however, employer non-disparagement agreements can bar employees from criticizing aspects of the business, such as products and services – particularly if there is no relation to a labor controversy.

Comment: Non-disparagement agreements that bar employees from engaging in Section 7-protected activities are often a violation of the NLRA, particularly when they are as broad as banning employees from criticizing, ridiculing, or disparaging an employer in any fashion. See NLRB's Advice Memorandum. The memorandum further explains that facially neutral non-disparagement agreements' lawfulness should be analyzed under the second prong of the Boeing Analysis, which requires that an employee reasonably interpreting the rule would believe it prohibits or interferes with the exercise of NLRA rights and, if so, whether any adverse impact on NLRA-protected conduct is outweighed by legitimate business justification. See *The Boeing Company*, 365 N.L.R.B. No. 154, 210 LRRM 1433, 2017 BL 447608.

Transactions

ANALYSIS

Private Equity Can Slow Down, But It Can't Stop

by Grace Maral Burnett
Legal Analyst, Bloomberg Law
Nov. 13, 2022

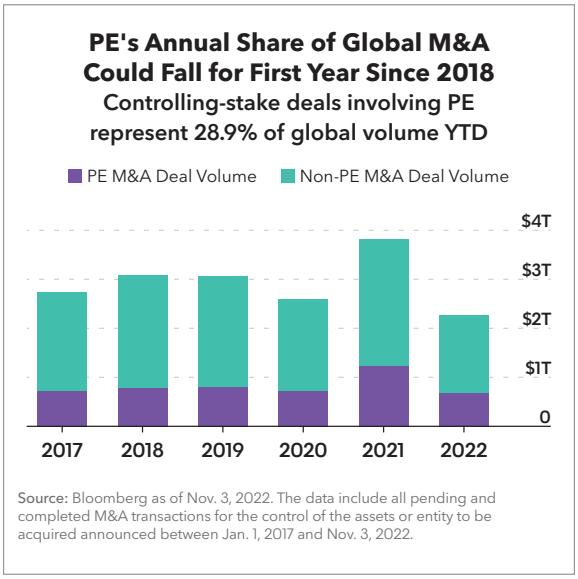
Even in the face of economic difficulties and market challenges this year, private equity cycles forward. Buyouts have slowed to a trickle, exits have been harder, and, for many in the industry, fundraising has been more challenging. But the PE wheel keeps spinning, and will continue to do so in 2023—in part with the help of the over $1 trillion in unspent capital the industry has available to invest.

A Much Slower Year

Along with the broader M&A market, private equity deal activity, including on the venture capital side, has slowed considerably during 2022. Private equity controlling-stake M&A deal volume has fallen by 46% compared to last year.

A slowdown was almost inevitable. Even before the challenges posed by rising interest rates, inflation, and a looming recession, market players predicted less activity this year following last year's break-neck PE deal pace, simply due to sheer exhaustion. But the current drop is clearly of a more serious nature.

One hit to deal volume has come via LBOs. Facing a difficulty or outright inability to secure financing for leveraged buyouts this year, these debt-financed deals—which were a key driver of overall PE M&A volume in 2021—fell sharply in the third quarter. As a result, despite an impressive roster of mega and very large PE buyouts announced earlier this year (e.g., the Citrix Systems, Inc., Nielsen Holdings PLC, and Atlantia SpA buyouts), the volume of all PE buyouts that have signed or closed this year is over 25% behind last year's record total—regardless of financing type. And the number of these deals is over 30% behind last year's count, which was the highest on record, according to Bloomberg data.



Source: Bloomberg as of Nov. 3, 2022. The data include all pending and completed M&A transactions for the control of the assets or entity to be acquired announced between Jan. 1, 2017 and Nov. 3, 2022.

Another likely explanation for the hit to deal volume is that the typical exit routes for PE—the avenues for funds to cash out on their investments—have become more challenging or have closed off entirely.

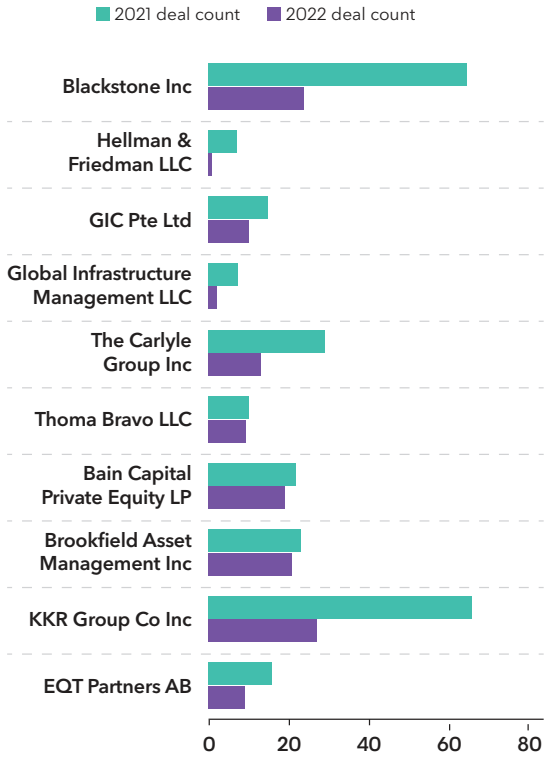
For example, M&A exits (acquisitions of PE portfolio companies by non-PE entities) are more challenging under the current market conditions. And with lower valuations, higher interest rates, and higher volatility, the IPO exit option hasn't been as attractive this year. As a result, there's been a noticeable shift in exit strategies from traditional M&A and IPO exits to more secondary transaction exits, in which a PE firm buys out the portfolio company of another PE firm.

This year could be the first since 2018 that sees PE's annual share of global M&A volume drop. Year to date, over 5,000 controlling-stake M&A deals with an aggregate value of $655.8 billion involving at least one private equity deal party have been signed. This volume represents 28.9% of all global controlling-stake M&A volume. Despite fluctuations in the overall M&A market, PE's share of this market has risen steadily each year since 2018, and reached a high of 32.1% in last year's record market.

The number of controlling-stake acquisitions signed this year by some of last year's top PE acquirers illustrates this year's slower activity. For example, major PE players Blackstone Inc. and KKR Group Co. Inc. have thus far engaged in fewer than half the acquisitions they made last year.

Last Year's Top PE M&A Buyers: 2021 vs. 2022 YTD Deal Counts

Pending and completed controlling-stake M&A transactions



Source: Bloomberg as of Oct. 28, 2022. The data include all pending and completed mergers and acquisitions announced between Jan. 1, 2017 and Sept. 30, 2022 by target industry. The industries included are the top five target industries based on aggregate deal volume from 2017 to 2022.

That being said, another takeaway from looking at the year-to-date activity among last year's top buyers is that, overall, they haven't stopped buying. A handful of the top buyers, such as Thoma Bravo LLC and Bain Capital Private Equity LP, are even already nearing their 2021 full-year total acquisition counts.

An Adaptable Playbook

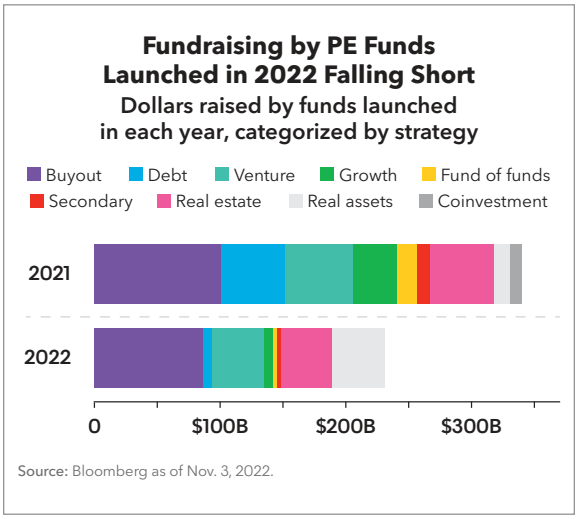
As put succinctly by my colleague Jan-Henrik Foerster at Bloomberg News: "That dry powder is still there and it will be deployed. No financing? Use cash. No financing for big buyouts? Do smaller transactions or minority deals." The PE deal playbook is adaptable and we've already seen bold fixes, however temporary (like all-equity buyouts) applied to push deals through since the start of the fourth quarter.

Since the start of Q4, 427 controlling-stake M&A deals involving at least one PE party with an aggregate value of $43.2 billion have been announced and are either pending in the period between signing and closing or have closed. Of these deals, 103 have been PE buyouts, valued at a total of $11.5 billion. And to the point about doing smaller deals: data for controlling-stake deals do indicate that the average deal size has been dropping quarter-to-quarter since the second quarter this year. In fact, fourth quarter deals thus far have the lowest average deal size since Q2 2020.

Bankers and PE advisers reportedly expect the pace of deals to increase in the new year, with take-privates and secondary transactions being an important source of flow. And PE has already begun to invest in industries, such as health and software, seen as better able to weather economic storms, a trend that will continue into 2023.

'Insatiable Fund Raisers'

Though fundraising has been more difficult this year, PE fundraising has persisted. Year to date, funds launched this year pursuing a variety of strategies have raised roughly $230 billion, with the largest portion—nearly $90 billion—raised by buyout funds.



Source: Bloomberg as of Nov. 3, 2022.

While this amount falls well short of 2021's total of dollars raised by funds launched last year (which surpassed $340 billion), it's a testament to the private equity cycle propelling itself forward. There's a reason PE managers have gained a reputation for being "insatiable fund raisers."

Commitments to investors, unspent capital, new funds launched, and exits that can't be delayed will all propel private equity deal activity well into the new year.

ANALYSIS

From War to Weather – 2023's Top Supply-Chain Disruptors

by Denis Demblowski
Legal Analyst, Bloomberg Law
Nov. 13, 2022

Supply chains, which have been tested to their limits in the last few years, will need to continue to increase their flexibility in 2023.

Covid-19 took us by surprise in 2020. Overnight, offices and businesses were shuttered, and supply lines collapsed. We adapted by working from home, limiting socialization, and lowering expectations on the resiliency and flexibility of "just-in-time" supply chains.

But the pandemic is slowly fading in the rearview mirror as a cause of supply-chain disruptions, and other factors that surfaced this year are likely to take its place in 2023. These include war, extreme weather, the threat of a global recession, and politics.

Also—different from the Covid era—inflation, rising interest rates, and the strong US dollar will play a leading role in supply-chain dynamics for the coming year. Because of developments this year, next year will likely be worse for worldwide supply chains than either 2020 or 2021.

Russia-Ukraine War

Russia and Ukraine account for major portions of the world's production of wheat, barley, and sunflower oil. But Russia's invasion of Ukraine has made Russia a trading partner pariah, and, due to the conflict, Ukraine exports of grain were initially curtailed or shut down as ports were blocked and grain production fell. While some relief came from the lifting of grain embargoes by Russia in July, Russia's withdrawal from the Black Sea safe passage compact in late October is again jeopardizing global food resources, particularly in developing countries.

The effects of these wartime disturbances mainly fall on Ukraine's major trading partners. But rising food and energy prices and shortages know no borders, and are occurring globally.

The Ukrainian economy is projected to contract by 35% in 2022 because of the destruction caused by the war and the displacement of millions of Ukrainians, according to the World Bank. The enormous economic cost of the war on both sides (including their allies) will fuel inflation and be a drag on the global economy.

Perhaps the most damaging economic effects of the invasion are the surging energy prices in Europe. Russia has been accused of "weaponizing" its hydrocarbon resources in retaliation for European economic sanctions and Ukrainian aid. Energy shortages and rising costs in Europe this winter due to the curtailment of natural gas supplies from the Nord Stream pipeline, alleged pipeline sabotage, and oil embargoes will test the strength of Ukraine's European allies' resolve.

Weather Disasters

Extreme global weather has fueled wildfires, historic droughts, and unprecedented flooding in 2022. These climate-change phenomena will undoubtedly continue into 2023. In addition to human suffering and economic and ecological damage, their effects on world food and water resources are likely to be of the greatest consequence. As the impact of weather-related incidents intensifies, supply-chain participants must begin to develop adaptation strategies, such as moving critical logistics centers away from storm-prone locations, to diversify sourcing and distribution channels and to alleviate supply-chain stress.

2022 Extreme Weather	
Heat Records Summer 2022 (June - August)	
Europe & China	vHottest on record
North America & Asia	2nd hottest on record
World	5th hottest on record

Source: NOAA's National Centers for Environmental Information.

Natural disasters caused by severe weather are traditionally considered "force majeure" events to the extent that they prevent or impede supply-chain participants' contractual obligations. That's small comfort for populations caught in the middle, however, since they suffer both the physical effects of the natural disaster and the resulting shortages.

Recession Fears

Some experts question whether we're already in a recession; others only disagree as to the timing and whether the landing will be "soft" or "hard." In any event, we will need to deal with recession scenarios in 2023.

If the economy contracts significantly, declines in spending and employment could signal an increase in extended payment terms, payment defaults, and supplier bankruptcies. Higher interest rates may dampen US demand even as the strong dollar makes imports more affordable. Coupled with inflationary price pressures, a recession may jeopardize demand/supply equilibrium leading to a longer-term recovery with fewer market players. Buyers with cash will hold an advantage. In this novel environment, transactional lawyers' creativity, ingenuity, and expertise will be in high client demand.

Political Ploys

International politics will continue to play an oversized role in supply-chain supply and demand as national interests take precedence over international needs. India, for example—in an effort to increase the price of a leading commodity—imposed a duty on certain rice exports in September 2022, leading neighboring Asian countries to search for alternate sources of supply and adding to food shortages. OPEC's production cutbacks are maintaining high fuel prices worldwide.

The full effect of the US Uyghur Forced Labor Prevention Act (UFLPA) on worldwide supply chains will become clearer in the new year. This law, which became effective in June 2022, creates a rebuttable presumption that any goods that have been produced, manufactured, or mined in the Xinjiang Uyghur Autonomous Region of China or by certain named entities have been made using forced labor. Unless the importer can show by clear and convincing evidence that no forced labor was used in the goods' production, the goods may not enter the US. This high bar effectively bans Xinjiang-based products, including cotton and polysilicon products principally used in the production of solar panels, from US import. Europe is developing similar legislation so that goods made with forced labor may soon find themselves without a welcoming Western port.

Ongoing national security tensions between the US and China may continue to restrict semiconductor trade and trade in other advanced components, as China accuses the US of "politicizing" science, technology, and trade issues. If China experiences another Covid-19 outbreak in 2023, a resulting shutdown of manufacturing or shipping facilities could again reverberate negatively throughout the global supply infrastructure.

Stay the Course

Next year will continue to see supply-chain disruptions, albeit from different causes than in 2020 and 2021. The 2023 disruptions may be more subtle and geographically dispersed than the collapse occasioned by Covid-19, but the key again will be to build flexibility into supply-chain structures. Buyers will want the flexibility to modulate quantity in response to demand changes, and sellers will require price protection in the face of rising costs. Challenges will abound.

ANALYSIS

How the US Is Using Trade Rules for Non-Trade Reasons

Louann Troutman, Legal Content Specialist, Bloomberg Law

The US government is developing new rules and enforcing existing ones that further its environmental protection, human rights, and national security objectives by regulating the trade in goods.

While using trade rules to address non-trade issues isn't new, the US government increased its use of these measures in 2022. Both import and export requirements are being used to pressure Russia and Belarus to end the war in Ukraine, and to address human rights violations in China.

2023 will see enhanced use of such measures to target not only Russia and China, but also countries that boycott Israel. The Biden administration has indicated that it will also use trade rules to address deforestation. These measures will impact both the importation and exportation of a wide range of goods.

Import Restrictions

In response to alleged Chinese government human rights violations, Congress passed the Uyghur Forced Labor Prevention Act in 2021 nearly unanimously. President Biden signed the bill into law Dec. 23, 2021, and it took effect June 21, 2022.

The law expands on Section 307 of the Tariff Act of 1930 to cover goods made in the Xinjiang Uyghur Autonomous Region of China and those made by entities on the UFLPA Entities List. It requires Customs and Border Protection personnel to determine that UFLPA deems, as a rebuttable presumption, that covered imported goods are made with forced labor and, as such, are denied entry into the US.

In June, Customs and Border Protection issued guidance placing the onus on the importer to show compliance with UFLPA and requiring the importer to demonstrate by "clear and convincing evidence" that the goods were not made with forced labor. This is a very high standard and one that will be nearly impossible for Xinjiang-origin goods to meet.

In FY 2022, approximately $500 million in shipments were detained by the CBP under UFLPA. This total accounts for almost half of the year's

3,000 detained shipments, even though the law was only in effect for the last quarter of the fiscal year. The CBP estimates that 11.5 million shipments per year may be subject to UFLPA, with an increase of petitions to over 20,000 a year. The CBP FY 2023 budget adds $70 million and 300 positions for UFLPA enforcement to the current base of $10.6 million and 29 positions, which indicates that the issue is a priority for the agency.

The CBP is also updating its Automated Commercial Environment (ACE) to enhance UFLPA enforcement. ACE is the online system importers use to provide the information that the CBP relies upon to determine whether a shipment is permitted to enter the US. In November, the CBP established a working group to discuss adding an UFLPA Region Alert to ACE entries. The ACE updates would require importers to enter a postal code for all imports from China when making an Entry or Manufacturer Identification Code. Importers who enter a postal code from within the XUAR will receive a warning message indicating that the shipment may be subject to UFLPA.

Imports can be used as leverage in pursuits outside of geopolitics as well. For example, President Biden's April 22 executive order targets international deforestation as a priority issue. The State Department, working with numerous government departments and agencies, is required to issue a report in 2023 with "options, including recommendations for proposed legislation, for a whole-of-government approach to combating international deforestation." This approach may include restricting or prohibiting the importation of commodities produced on deforested land and requiring traceability of those commodities. The EO also calls for including deforestation and land conversion in both new and existing trade agreements.

Export Restrictions

The Biden administration envisions a larger role for export compliance to advance US policies on military actions and human rights abuses.

A report released in October by the Commerce Department's Bureau of Industry and Security stated that "export controls have never been a better fit for addressing [national security] challenges than they are today." The report emphasized changes to strengthen enforcement and compliance with export controls and anti-boycott requirements. These changes include a greater focus on public disclosure, an increase in fines, and a requirement that companies publicly admit to facts as part of pre-trial settlements. The report also encouraged companies to comply with export controls and anti-boycott requirements rather than treat fines as a cost of business.

Commerce Under Secretary Alan Estevez testified before a House committee in July that existing US export controls on Russia provide a "great framework" to combat Chinese human rights abuses.

On Oct. 13, the BIS announced an interim final rule that amends the Export Administration Regulations to impose significant export controls on certain IT products, including integrated circuits and items used to manufacture semiconductors. This rule is intended to limit China's ability to develop advanced computing technology. According to an Oct. 20 Bloomberg News report, the Biden administration is considering expanding these new controls to cover quantum computing and artificial intelligence as well.

Anti-boycott laws are a particular type of export restriction that discourages or prohibits American businesses from participating in unsanctioned boycotts. First adopted in the 1970s, primarily in response to the Arab League's boycott of Israel, anti-boycott actions are traditionally limited in scope. Historically, fines have been relatively small, with most fines coming in under $1 million and many under $100,000. Businesses have not had to make any admissions of wrongdoing to obtain a settlement.

The BIS issued a regulation in October announcing "enhanced enforcement" of anti-boycott laws in 2023 to target serious violators. Much like the new enforcement policies for export controls, the new policy will increase fines and require companies found to be violating the anti-boycott rules to admit misconduct. The new policy also focuses on more serious anti-boycott violations and on foreign subsidiaries of US companies.

Bloomberg Law

2022 In-House Counsel Customer ROI Survey

In 2022, we surveyed in-house counsel customers to examine the potential return on investment (ROI) legal departments may realize by utilizing Bloomberg Law.

94% of GCs and CLOs surveyed agree that Bloomberg Law has all the legal research tools, resources, and content in-house counsel need on a single, integrated platform.

Click here to download the Executive Summary
and see how Bloomberg Law can help your department

Expand Your Expertise

Bloomberg Law helps them get up to speed on new or existing matters, allowing them to do more work in less time.

Bring More Work In-House

Bloomberg Law allows their legal department to bring more work in-house and reduce reliance on outside counsel.

Work Efficiently and With Confidence

Bloomberg Law helps them complete work with efficiency, accuracy and confidence.

Accelerate the Drafting Process

Bloomberg Law gives them a better starting point to work on contracts, agreements and clauses.

PRACTICAL GUIDANCE

Sample Clause – Responsible Supply Chain Representation, Warranty and Covenant (Annotated)

Editor's Note: The following clause may be adapted for use in a commercial manufacturing or supply agreement to formalize expectations and commitments regarding the Supplier's supply chain performance.

Sample Language:

Section X. Responsible Supply Chain

(a) Labor. Supplier represents, warrants, and covenants that it does not, as of the Effective Date, and shall not, during the Term (i) use involuntary, bonded, or underage labor at the facility(ies) where its performance under this Agreement will occur; (ii) engage in human trafficking; or (iii) maintain unsafe or unhealthy conditions in any dormitories or lodging that it provides for its employees. Supplier agrees that during the Term it shall promptly disclose to Customer any use, whether intentional or unintentional, of involuntary, bonded, or underage labor or instances of human trafficking, and shall correct unsafe or unhealthy conditions in any lodging that it provides for its employees. Supplier shall use reasonable efforts to include similar prohibition and disclosure requirements in agreements with its own suppliers. Supplier shall cooperate and provide such information and/or certifications regarding its compliance with this sub-section (a) as may be reasonably requested by Customer.

(b) Environment, Health, and Safety. Supplier represents and warrants to Customer that Supplier has and Supplier covenants that it will continue to have a documented, comprehensive environment, health, and safety (EHS) policy that addresses, among other things, its ongoing commitment to environmental stewardship and elimination of workplace injuries and illnesses. Upon Customer's request, Supplier shall provide Customer with evidence of implementation of such policy and agrees to provide information related to the environmental impact of any Product (or any materials used therein) including but not limited to greenhouse gas emissions, waste generation, recycled content, amounts of regulated chemicals in a Product, and disposal information.

(c) EHS Improvements. As and when they become available, Supplier shall identify and bring to Customer's attention Product options that have a reduced environment, health, and/or safety impact. In the event Supplier receives an Order for Product for which Supplier has an option with a reduced environmental footprint or a more favorable health and safety profile, Supplier shall promptly notify Customer of such option(s). Supplier shall discuss with Customer the feasibility, efficacy, and regulatory and cost implications of any of the foregoing alternate Product options and shall provide such options if and as directed by Customer.

(d) Anti-Corruption. Supplier shall conduct its activities hereunder in accordance with all Applicable Law related to anti-bribery or anti-corruption legislation, including the U.S. Foreign Corrupt Practices Act of 1977 and all national, state, provincial or territorial anti-bribery and anti-corruption statutes. Accordingly, in connection with its performance under this Agreement, Supplier shall make no offer, payment or gift, will not promise to pay or give, and will not authorize the promise or payment of, directly or indirectly, any money or anything of value to any Customer employee or agent, any government official, any political party or its officials, or any person while knowing or having reason to know that all or a portion of such money or item of value will be offered, given or promised for the purpose of influencing any decision or act to assist Supplier or Customer or otherwise obtaining any improper advantage or benefit. Supplier will take appropriate actions to ensure that any person representing or acting under its instruction or control will also comply with the provisions of this sub-section (d).

(e) Import/Export Control. Supplier, any officer, director of Supplier, and any agent, consultant, or other third-party representative of Supplier, acting in its capacity as such, shall conduct their activities in accordance with all Applicable Law relating to the exportation of the Products from [Country] and importation of the Product by Customer into the United States. Supplier shall promptly notify Customer in the event Supplier receives written

notice from any Governmental Authority alleging Supplier's failure to comply with any export or import requirements with respect to the Products.

Comment: This clause combines supplier's agreement to comply with law in the performance of its contractual obligations with a commitment to exceed that minimum standard in the labor and environmental, health, and safety areas. Companies are increasingly called to task on these topics by investors, customers, employees, and other constituencies, and public disclosure or certification of performance is often necessary or desired. Note that the corruption prohibitions in paragraph (d) above apply to payments, gifts, etc. to customer employees or agents as well as to governmental officials.

Example Clause Search: Access our Transactional Precedent Database of Responsible Supply Chain clauses found in publicly filed commercial agreements.

Value/Risk Analysis: Having a clause such as this one in a manufacturing or supply agreement confirms the importance that the parties assign to lawful and ethical conduct in the operation of the supply chain. It also provides a contractual basis for the customer to request compliance information or certification periodically from the supplier and for the customer to consider EHS process or product improvements discovered by the supplier. The absence of such a clause does not necessarily negate the significance of the subject areas in the parties' relationship, but it does risk the perception that the parties do not consider the areas to be of importance.

Affected Clauses: Adding a responsible supply chain clause to a commercial agreement may impact the meaning or affect other provisions or the operation of other provisions in the agreement, including:

- Definitions
- Confidentiality
- Breach; Remedies
- Compliance with Laws
- Term and Termination

CHECKLIST

Cyber Insurance Application & Purchase Considerations

Editor's Note: This checklist details best practices for implementing information security measures and third-party risk management procedures, which are needed for a company to obtain comprehensive cyber insurance coverage. It also lists several key policy considerations that a company should review prior to committing to the purchase of a cyber insurance policy.

Contributed by David Derigiotis, Burns & Wilcox

Best Information Security Practices for Obtaining Optimal Coverage & Pricing

The following information security best practices are reflective of underwriting guidelines throughout the cyber insurance marketplace. Implementing these procedural and technical controls can help an organization to qualify for the best available coverage and pricing. Verification of security posture is typically self-attested via an insurance application.

❑ Broad application of multi-factor authentication, including for:

- Employee and third-party access
- Key applications
- Privileged accounts

Comment: Based on insurance claims data, lack of multi-factor authentication has commonly led to unauthorized access and ransomware incidents.

❑ Restrict or disable remote connections/Remote Desktop Protocol (RDP).

Comment: Microsoft RDP is utilized to connect virtually from one machine to another. This is used frequently in remote work environments. Organizations that leave RDP accessible to the internet, specifically port 3389, are more susceptible to unauthorized access. Claims data support that this often leads to an attacker accessing sensitive information, disabling antivirus protections, and installing ransomware or other malware following a compromise.

❑ 3-2-1 Backup Strategy:

- Create three copies of your data (one primary and two backups);
- Store your copies in at least two types of storage media; and
- Store one of these copies offsite.

Comment: Implementing a sound backup strategy can allow an organization to better recover following a ransomware incident. This method combined with a documented and properly rehearsed disaster recovery plan can significantly reduce the likelihood of paying a ransom.

❑ Timely patching of Common Vulnerabilities and Exposures (CVEs) through a documented program to identify, assess, track, and remediate vulnerabilities on all enterprise assets within infrastructure.

Comment: Unpatched systems and software have led to substantial security compromises. One notable incident is the 2017 Equifax data breach where software used on the credit giant's website went unpatched, leading to the compromise of nearly 150 million consumers.

❑ Endpoint detection and threat response through a security solution that uses behavioral and signature-based analysis to identify and stop cyber threats such as ransomware and suspicious activity.

Comment: This is a security solution used to detect unauthorized access and other threats across an organization's environment.

❑ Employee security awareness training program.

❑ Affirmative compliance with local and internationally recognized standards for information governance and privacy regulation.

Cyber Supply Chain Risk Management (C-SCRM)

Organizations should document and evaluate the written policies and procedures of their third-party service providers and other vendors through an established C-SCRM plan that incorporates the following:

❑ Due diligence processes used to evaluate the adequacy of cybersecurity practices of third-party service providers.

❑ Periodic assessment of third-party service providers based on the risk they present and the continued adequacy of their cybersecurity practices.

❑ Protocols for third-party vulnerability disclosure and incident notification to company.

Comment: Security vulnerabilities and other points of compromise can be introduced via third-party access. Notable technology supply chain compromises include Accellion, SolarWinds, and Microsoft Exchange Server.

Key Cyber Insurance Coverage Considerations

Not all cyber insurance policies are the same. Policy wording, insuring agreements, and definitions will vary widely from one carrier to another. To receive the most favorable wording available, items of interest should include the following:

❑ Definition of a privacy/security incident should be broadened to include information stored outside of the organization's network.

- Example wording: Any actual or alleged failure by the Insured; a third party for whom the Insured is legally responsible; or a service provider under written contract with the Insured to process, store, or maintain Protected Information on behalf of the Insured to prevent Unauthorized Access, Unauthorized Use, acquisition, manipulation, loss, theft, or misappropriation of Protected Information.

❑ Definition of computer system needs to include systems operated by a third-party service provider.

- Examples of applicable systems include hosted computer application services and other cloud services that process, maintain, host, or store the insured's electronic data.

❑ The policy should provide affirmative coverage for state-sponsored, or government affiliated cyber-attacks (e.g., cyber war/terrorism).

Comment: Considering the current geopolitical climate across the world, attacks from government-affiliated or state-sponsored actors have increased. A policy with affirmative coverage will reduce the risk of having a claim denied should an attack be attributed to a foreign government. Notable incidents include the 2017 Russia-attributed NotPetya attack and the 2014 Sony Pictures Entertainment hack attributed to the North Korean government.

❑ The policy should have no exclusion for failure to maintain information security standards.

❑ The policy should contain "duty to pay" (on behalf of) versus "duty to reimburse" wording that describes the obligations of the insurer, where possible, in order to help preserve the insured's cashflow in the event of a security incident.

Comment: In a duty to reimburse agreement, the insured will be responsible for bearing all the costs upfront following a security incident, which can include forensics, legal, notification, and ransomware payments. The insurer will then reimburse the policyholder for those expenses. These unexpected expenses can be burdensome for a small to midsized enterprise. In a "duty to pay" agreement, the insurer will pay expenses on behalf of the insured following an incident, helping to preserve cashflow for the organization.

PRACTICAL GUIDANCE

Overview – ESG Risk Factors in SEC Filings

On March 21, 2022, the Securities and Exchange Commission proposed rule changes that would require registrants to include certain climate-related disclosures in their registration statements and periodic reports, including information about climate-related risks that are reasonably likely to have a material impact on their business, results of operations, or financial condition, and certain climate-related financial statement metrics in a note to their audited financial statements. The required information about climate-related risks also would include disclosure of a registrant's greenhouse gas emissions, which have become a metric to assess a registrant's exposure to such risks.

The Proposed Rule Changes

This proposal has generated significant interest from registered public companies and other interested parties, leading the Commission to initially extend the public comment period on this proposed rulemaking until June 17, 2022. Per the SEC's Spring 2022 Regulatory Agenda, the agency had expected the Commission would begin formal consideration regarding whether to adopt final climate-related disclosure rules in or around October 2022. However, the SEC issued a press release on October 7 stating that it had reopened the proposal's comment period with the implication that the Commission's adoption of new rules, if any, would be necessarily delayed. Once adopted, any new rules would likely go into effect 60 days after their publication in the Federal Register.

There are numerous standards and frameworks for ESG disclosures around the world, but no comprehensive ESG disclosure regime has become law in the United States. The proposed rule changes, if adopted, would represent a significant expansion of the mandatory disclosure regime for registered public companies. Climate-related disclosures fall under a larger, emerging umbrella of environmental, social, and governance (ESG) matters that are increasingly being considered for new regulation. The focus of the SEC's proposal concerns risk. The rules would require companies to identify climate-related risks to the company's business, disclose their impact on the company and the larger world, and provide information about the company's efforts to manage those risks.

These new disclosures would require companies answer the following risk-related questions:

- What are the company's risk management processes and how does it govern its climate-related risks?
- What have been or are likely to be (short-, medium-, or long-term) the company's climate-related risks that are likely to materially impact the company's business and consolidated financial statements?
- How have identified climate-related risks affected or are likely to affect the company's strategy, business model, and outlook?
- What is the company's assessment of the impact of climate-related events (severe weather events and other natural conditions) and transition activities on the line items of its consolidated financial statements, as well as on the financial estimates and assumptions used in those financial statements?

Risk Factors in SEC Filings

Public companies are required to identify and discuss the material risks affecting their business in both their initial registration statement and in certain mandatory periodic reports filed with the SEC. The inclusion of risk factors in SEC filings is intended not only to inform potential investors of the hazards facing the business so they may better assess whether the company's securities represent a suitable investment, but also to insulate the reporting company from claims of securities fraud since investors were alerted to those risks. (For more, see Drafting Effective SEC-Compliant Risk Factors)

Risk Factors are not required in every SEC filing. A risk factors section is typically required in initial registration of securities (on Form S-1/F-1) under the Securities Act of 1933 and periodic reports filed pursuant to the Securities Exchange Act of 1934. Periodic reports with risk factors are usually filed on Form 10-K (annual report) and Form 10-Q (quarterly report), but risks, particularly emerging material risks that fall under the form's Item 8.01 (other events that the registrant believes are important), may also be disclosed on Form 8-K (current report).

Instructions to Form 10-K provide that smaller reporting companies, as defined in Regulation S-K, Item 10(f), 17 C.F.R. § 229.10(f), are not required to include risk factor disclosure under Item 105 in their Exchange Act filings, though many do. A smaller reporting company is an issuer that is not an investment company or asset-backed issuer and (1) has a non-affiliate public float of less than $250 million; or (2) has annual revenues of less than $100 million and either (a) no public float or (b) a public float of less than $700 million.

The SEC's Form 10-Q requires any "material changes from risk factors" disclosed in the Form 10-K be updated as necessary.

ESG Disclosures in SEC Filings

The SEC's long-standing disclosure regime is predicated on registrants providing disclosures that are material to the company's business. ESG disclosures are not currently required unless the ESG matter is material to the company and its prospects.

In 2010, the SEC issued Commission Guidance Regarding Disclosure Related to Climate Change, guidance rooted in the materiality standard that remains the agency's most direct expression of how companies should approach climate change disclosures in their SEC filings. The materiality standard relies on the U.S. Supreme Court decisions in *TSC Industries, Inc. v. Northway, Inc.* (1976) and *Basic Inc. v. Levinson* (1988) which effectively give registrants significant discretion in determining which climate-related disclosures are sufficiently material to potential investors to necessitate their disclosure.

ESG Risk Factors in SEC Filings

Until the Commission adopts prescriptive ESG disclosure rules, inclusion of ESG risk factors by a registrant in its SEC filings will remain voluntary for most. Still, many companies elect to make voluntary disclosures and the SEC has encouraged companies to do so.

Many of these voluntary ESG-related disclosures focus upon the public's increasing scrutiny of corporate ESG activities, the risk of damage to the company's brand and reputation if it fails to act appropriately in areas such as corporate governance, environmental stewardship, diversity, equity, and inclusion, transparency in how the company considers ESG factors in running the business, and the additional costs and adverse impact to its business and results of operations associated with ESG activities and adverse incidents. Companies operating in an industry sector particularly vulnerable or contributing to climate-related risks, such as agriculture or energy, may have risks that already would be considered material by potential investors and therefore must be disclosed.

There are three ESG areas that the SEC has previously announced its intention to focus on for new ESG-related disclosure requirements: (1) diversity, equity, and inclusion; (2) climate change; and (3) human capital management. See, Examples of ESG-related risk factor disclosures in SEC filings.

ESG

ANALYSIS

From Acronym to Concept, Investors Connect ESG Pillars

Abigail Gampher, Legal Analyst, Bloomberg Law

Investors have begun to shift away from approaching the term "ESG" as distinct environmental, social, and governance issues affecting a company's financial performance. Instead, investors are increasingly conscious of whether the companies they're investing in embody their overall values—and those values can often cut across ESG pillars.

Companies that have implemented environmental policies to address climate change, for example, may have once satisfied the value appraisals of investors seeking to make climate-conscious investments. But now investors are looking for companies to address the human displacement resulting from extreme weather as part of that same risk equation.

This development is likely to render the current political debate and regulatory action surrounding the term ESG less relevant in the coming years. Public officials and regulators alike have claimed that the term ESG is charged with underlying meanings related to political agendas or promises of certain sustainability commitments. But the current understanding of ESG as distinct environmental, social, and governance issues that may affect a company's financial performance isn't a view that all investors share.

And in the coming months and years, investors are going to push companies to implement more cross-pillar policies—likely bringing companies and regulators to their side of the table.

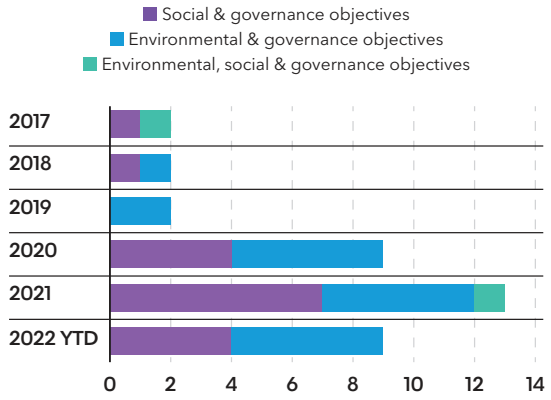
Activists Are Connecting the ESG Pillars

When investors are dissatisfied with the actions a company is taking, the company runs the risk of an activist taking a stake in the company in order to enact change. Investor activism campaigns often focus on achieving governance objectives—such as board representation or control—that would allow the activist to install a representative who can advocate for initiatives that align with the activists values.

In 2020, investor activism campaigns with objectives from at least two ESG pillars saw an uptick from 2019 counts, according to Bloomberg data. These campaigns saw another increase in numbers last year and, while 2022 data is still preliminary, this year's totals are likely to at least meet 2021 levels by year-end.

Investor Activists Look to Integrate More Aspects of ESG

Investor activism campaigns including objectives from at least two ESG pillars



Source: Bloomberg as of Oct. 28, 2022. Data was sorted by campaign start date. No campaigns included environmental and social objectives without a governance objective in this period.

All investor activism campaigns that cut across ESG issues since 2017 have included a governance objective, meaning that investors are consistently looking to make governance changes at companies in which they have a financial interest.

But when investor activists couple a governance objective with a social or environmental objective, they're attempting to enact company policies that align with their values and that ensure that the company has a governance structure to support this agenda.

Companies seem to have picked up on this investor interest and have begun including potential board members bios with relevant environmental and social positions in their definitive proxy statements—which is likely to continue in the coming years.

Litigation Risks Cut Across Pillars

It's not surprising that investors have employed a cross-pillar approach to activist campaigns because legal risk already cuts across the ESG pillars. Many ESG-related complaints include terminology belonging to at least two of the environmental, social, and governance categories. And shareholders have filed almost 70 complaints that touch on ESG issues from multiple pillars since 2020.

In an effort to reduce legal risk, companies may start implementing crossover ESG policies and programs. For example, litigation related to an oil spill may include terminology relating to the breach of environmental laws and human health implications in the area. Companies in industries that have heavy environmental risks—like energy—are likely to start building community support into their risk management policies and programs as a means of addressing investor interest.

Integrating an Interconnected ESG

As the US begins its regulatory journey into the ESG space, investors are likely to use mandated climate-related disclosure information to push for changes that traditionally have fallen within the social and governance categories.

If investors determine that a company's management isn't prioritizing the disclosures of accurate climate-related information in its 10-K, for example, investors may vote for a board candidate who will prioritize investor access to climate information.

And as ESG regulation continues, investors are likely to continue treating ESG as a whole, rather than its parts—regardless of the political and regulatory discourse surrounding the use of the name.

ANALYSIS

A New SEC Human Capital Rule Is Coming – So Is Pushback

by Abigail Gampher and Dori Goldstein
Legal Analysts, Bloomberg Law
Nov. 13, 2022

The rise of ESG over the past several years has cemented investor interest in incorporating environmental and social impacts into the financial investment equation. Next year, human capital management will be at the forefront of the conversation, and we'll see investors looking for more disclosures to ensure that they are investing in companies that align with their values.

The current rumblings of a new, clarified version of the 2020 rule on human capital management are likely to transform into a final rule that provides investors with more clarity into human capital management. The new rule, however, may be just as ill-received as its 2020 predecessor.

Principle-Based Approach

In 2020, the SEC sought to improve investor access to human capital information by adopting a rule requiring companies to disclose the human capital management measures and objectives they focus on in managing their businesses—provided those measures or policies are material to the company's business as a whole.

The SEC noted in the final rule that human capital management disclosures were industry-specific, necessitating its principle-based approach to the topic.

Before and after the SEC adopted the rule in 2020, the agency received pushback on the principle-based methodology from investors and stakeholders who claimed that it didn't effectively provide investors with the information they were seeking. Comments on the proposed rule and, more recently, the Working Group for Human Capital Accounting Disclosure's petition for rulemaking filed in June, have argued that human capital disclosures should deviate from the primarily principle-based approach to provide investors with a clearer picture of human capital management.

The SEC's principle-based approach may not offer investors a complete picture of a company's workforce because it leaves disclosures to the company's discretion, allowing companies to miss or obscure workforce issues.

What's Next for Disclosures: A Prescriptive Shift

But any future SEC movement on human capital management is going to be more, not less prescriptive, in the coming year, and may thus address these workforce-issue omissions.

The SEC's expected proposed rule on human capital management is likely to require that companies make 10-K disclosures on key elements of human capital—such as workforce composition—to provide that clearer picture to investors. Currently, the list of human capital measures that may surmount to materiality outlined in Item 101(c) is not exhaustive or binding and therefore investors are not guaranteed that set of information.

And a proposed rule on climate-related disclosures may provide stakeholders with insights as to how the human capital management rule will unfold.

Though this shift would be disruptive, it would not require the SEC to reimagine disclosures. Just this year, the SEC proposed prescriptive climate-related disclosures in a rule that seeks to standardize climate-related disclosures and to allow investors a deeper look into environmental information. For example, the SEC set forth a universal definition for Scope 3 emissions that would require certain publicly traded companies to disclose information that falls within that definition in its 10-K. While the amount of Scope 3 emissions produced may vary widely based on industry, the same disclosure framework applies regardless of the industry, but investors can account for industry differences.

The prescriptive shift is likely to happen in the human capital space as well—a modification that some commenters requested for the 2020 rule. The commenters asked for the SEC to approach human capital disclosures by requiring a key set of disclosures (such as full-time and part-time employees, and seasonal workers) regardless of the industry. The comments acknowledged that

there may be some variation based on industry, but argued that the same baseline of disclosures should be required. Such an elaboration in the new rule is likely to give investors more insight into what is arguably a company's most important resource—human capital management.

Assessing the Value of a Workforce

A prescriptive approach would provide more transparency into the health of a company's workforce. It gives investors hard numbers to analyze, and it forces companies to track and disclose metrics that they might not otherwise track or disclose.

Such an approach also shifts the focus from general assessments about a company's workforce to quantifiable metrics, allowing investors to adjust for industry-specific differences. Turnover metrics are an excellent example: There's a clear, industry-specific nuance in assessing the value of worker turnover metrics. Certain industries, like the hospitality industry, tend to see higher employee turnover rates than industries like finance and insurance. Higher-than-normal turnover rates in any industry likely a signal human capital management issue. Investors can use their discretion to assess the relevance of the rate for a particular business.

Similarly, many of the most pressing labor issues facing companies today—like staffing shortages, soaring labor costs, an increasingly remote workforce, and diversity, equity, and inclusion—are both easily quantified and directly linked to the success and the stability of a company.

But not every workforce issue is so clear cut. Consider company culture—it represents a major workforce challenge and opportunity that influences a company's success and can be hard to quantify. Metrics like worker turnover and DEI assessments can offer some clues about company culture, but without its own dedicated metric, will investors leave it out of the equation?

Even though both companies and investors have asked for more clarity from the SEC on human capital management disclosures, don't expect everyone to celebrate a prescriptive approach. Companies will almost certainly bristle at the added reporting burdens, and investors will call for more expansive reporting requirements.

ANALYSIS

SEC's Climate Rules Face Skeptical Courts, APA Hurdle

Preston Brewer, Legal Analyst, Bloomberg Law

Climate-related disclosures forecast: The Securities and Exchange Commission will adopt climate disclosure rules in 2023; opposition will be fierce; and, unless the proposed rules are retooled prior to their adoption, a court will likely either remand and order that the rules be reworked or vacate them.

Legal challenges should be expected on many fronts—including a major questions doctrine or Chevron deference analysis, and under the First Amendment—and from diverse opponents, such as affected industries, state attorneys general, think tanks, and trade associations. This analysis focuses on whether the SEC complied with the strictures of the Administrative Procedure Act.

Proposal Would Remake Disclosure Regime

The rules, as proposed in March, represent more than simply new rules that will require additional disclosures about a public company's environmental impact. They are no less than a highly controversial remaking of the US securities disclosure regime. Disclosures required by securities laws have long been predicated on the information being material to investors making an investment decision.

The proposed climate-related rules depart abruptly from that materiality standard. The proposed rules are frequently prescriptive, requiring public companies to gather certain information and disclose it even when the burdens of compliance are significant, and even if the data provided will not be consequential to investment decisions.

After recently reopening the proposed rules' public comment period, a Commission vote on final rules looks to take place in 2023, perhaps sometime in the second quarter.

How Might the APA Restrict Climate Rules?

Many doubt the SEC's authority to impose climate-related disclosure mandates on the public companies it regulates.

However, broadly speaking, when any public company information is material to investors, the SEC may require its disclosure. If climate-related disclosures would be material to investors, then those disclosures are already legally mandated under the SEC's court-tested rules, subject to an economic analysis of the benefits and burdens under the APA.

Under the proposed rules, some climate disclosures will continue to be based on their materiality (e.g., Scope 3, which addresses indirect supply chain emissions, though the burden for compliance would be extremely high), while others are prescriptive (e.g., Scopes 1 and 2, which address direct emissions from operations), such as requiring companies to disclose climate-related risks that total as little as 1% of a total line item in their financial statements.

The proposed prescriptive rules go beyond discussing a material risk or disclosing matters that have a material impact on the business and its finances. The SEC may enjoy some latitude with courts in defining what is material beyond financial concerns, and that could provide some degree of support to courts inclined to defer to the agency's prescriptive rules approach.

The APA Is an Old Nemesis

The SEC has suffered important defeats to its rulemaking in the US Court of Appeals for the DC Circuit for violations of the APA.

That act mandates that all federal agencies take certain steps when adopting new rules that break with

The DC Circuit Has Dealt the SEC Many APA Setbacks
Selected Administrative Procedure Act decisions since 2000

Decision Year	Key Holding Regarding SEC Compliance with APA (case citation)
2005	The SEC violated the APA by failing to adequately consider the burden of compliance and by failing to adequately consider independent chair alternatives. (Chamber of Commerce of the U.S. v. SEC, 412 F.3d 133, 366 U.S. App. D.C. 351)
2010	"[T]he SEC failed to properly consider the effect of [a new rule treating fixed indexed annuities as not annuity contracts] upon efficiency, competition, and capital formation." (Am. Equity Inv. Life Ins. Co. v. SEC, 613 F.3d 166, 392 U.S. App. D.C. 1)
2010	The court was unable to affirm the SEC's determination that NYSE fees were "fair and reasonable," found that the agency had failed to "disclose a reasoned basis" for concluding there are significant competitive forces in pricing, and vacated the SEC's order approving an NYSE proposed rule change. (NetCoalition v. SEC, 615 F.3d 525, 392 U.S. App. D.C. 272)
2011	The SEC failed to consider Rule 14a-11's effect upon efficiency, competition, and capital formation, and the court consequently vacated the rule. (Bus. Roundtable v. SEC, 647 F.3d 1144, 396 U.S. App. D.C. 259)
2017	The SEC lacked "reasoned decisionmaking" and its "Order was arbitrary and capricious, unsupported by substantial evidence, and otherwise not in accordance with law." (Susquehanna Int'l Grp., LLP v. SEC, 866 F.3d 442, 432 U.S. App. D.C. 46)
2022	The SEC's approval of a FINRA proposal creating a data service was arbitrary and capricious under the APA because the Commission neglected to give a reasoned explanation in response to Bloomberg's significant concerns about the costs that FINRA and market participants will incur. (Bloomberg L.P. v. SEC, 45 F.4th 462)

Source: NOAA's National Centers for Environmental Information.

established agency policy, such as the SEC's departure from the materiality standard (if the agency adopts the climate disclosure rules as proposed).

The SEC will need to show courts that it performed a rigorous economic analysis assessing the benefits and costs imposed on companies required to comply with those new rules, including demonstrating that it studied how the proposed climate rules would affect efficiency, competition, and capital formation.

To meet APA requirements, the agency can't have acted in an arbitrary or capricious way, and must have addressed significant comments from the public about the proposed rules. Comments considered significant are those that challenge a fundamental premise underlying the rule change, raise significant issues, or make claims that—if true—would necessitate that the proposed rule be altered.

Overcoming the Arbitrary-or-Capricious Hurdle

For informal agency rulemaking, such as here, federal courts will set aside the commission's climate rules if the SEC is found to have acted in a manner that the APA defines as "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law."

Key court considerations include:

- the expected compliance burden and less-costly alternatives;
- the effect on efficiency, competition, and capital formation; and
- whether the rules were made through reasoned decision-making supported by substantial evidence.

There's widespread concern over the cost that rules requiring such detailed disclosure will impose on the roughly 6,000 affected public companies. Many companies would need to build substantial climate reporting infrastructure to comply, in addition to the cost of collecting, analyzing, and reporting data. The proposal would create a much more expansive, complex, and expensive reporting regime with financial risks sharing the stage with climate concerns. The SEC has admitted that its economic analysis is unable to reliably quantify costs and benefits.

The burden of the proposed rules could dissuade companies from going public and could incentivize existing public companies to go private to avoid these mandates, arguably impeding capital formation and limiting the investment opportunities of retail investors.

Given the history of setbacks the SEC has suffered in the DC Circuit, adopting climate rules that impose inflexible, prescriptive disclosure mandates that require data that are difficult and very costly to gather and are potentially confusing and even unhelpful to investors, would seem to well satisfy the APA's test for arbitrary or capricious.

In their submitted comments to the SEC, many companies have pushed back on the prescriptive rules, suggesting a higher threshold than the proposed 1% in line items, which would bring the triggers for disclosure closer to material.

To comply with the APA, the SEC should consider the submitted comments, should thoughtfully evaluate proffered alternatives, and should provide a reasoned explanation in response. Adhering to the APA process will give the SEC its best chance to avoid any adopted rules being vacated by the DC Circuit.

(Bloomberg LP, parent company of Bloomberg Law, submitted a letter to the SEC supporting the proposed rules.)

PRACTICAL GUIDANCE

Comparison Table – ESG Frameworks

For companies endeavoring to report on ESG issues, many implement one or several voluntary reporting frameworks to help do so. Employing the guidance of a voluntary ESG framework can help with the determination of which particular issues to disclose, the form that the disclosure takes, and may facilitate the verification of information contained in your company or client's report. For most, the determination of an appropriate framework stems from a company's individual ESG objectives and the desired audience for their disclosure.

See Overview – Global Reporting Initiative; Overview – Sustainability Accounting Standards Board; Overview – United Nations Global Compact; and Overview – Task Force on Climate Related Financial Disclosures.

	Global Reporting Initiative (GRI)	Sustainability Accounting Standards Board (SASB*)	United Nations Global Compact (UNGC)	Task Force on Climate-related Financial Disclosures (TCFD)*
Summary	An international independent standards organization that helps businesses, governments and other organizations understand and communicate their impacts on issues such as climate change, human rights, and corruption. GRI is the most widely used reporting framework, with 82% of the world's largest 250 corporations reporting in accordance with GRI Standards.	A sector-based, industry specific guidance framework used primarily to help publicly traded companies determine the financial materiality of sustainability related information for disclosure to the SEC and the public.	A voluntary initiative based on CEO commitments to implement universal sustainability principles; A way for companies to support and advance the UN's Sustainable Development Goals, which have been adopted by all UN member states.	A voluntary framework of recommendations on climate-related financial disclosures that are applicable to organizations across sectors and jurisdictions. Organizations can use the Recommendations to help them prepare more consistent and comparable disclosures of their material, climate related risks and opportunities, and how they manage them.
What is the framework's structure?	There are two primary groups: Universal Standards and Topic-specific Standards. The Universal Standards, also called the "100 Series of the GRI Standards" includes three standards to use in preparing a sustainability report: • GRI 101: Foundation 2016 • GRI 102: General Disclosures 2016 • GRI 103: Management Approach 2016. The Topic-specific Standards include: • GRI 200: Economic Standards • GRI 300: Environmental Standards • GRI 400: Social Standards.	The SASB standards are broken down by industry, making SASB metrics comparable from company to company within an identified peer group. There are 77 identified industries in the SASB Standards, in 11 different Sectors.	The Global Compact consists of 10 Principles intended for incorporation into companies' value systems and business operations. The SDG program provides 17 lofty goals with a 2030 target date for attainment. They aim to end poverty and environmental degradation, reduce inequality, expand access to healthcare and education, and engender sustainable economic growth	The TCFD Recommendations are designed to help organizations comply with existing mainstream reporting requirements, rather than impose additional reporting standards.

	Global Reporting Initiative (GRI)	Sustainability Accounting Standards Board (SASB*)	United Nations Global Compact (UNGC)	Task Force on Climate-related Financial Disclosures (TCFD)*
Is there a prescribed reporting format?	Reports will be company/ organization specific, but will include an "in accordance" designation, meaning the report was written in accordance with GRI Standards. To claim that a report has been prepared in accordance with the GRI Standards, look to GRI 101: Foundation for guidance.	Sustainability information and performance metrics that are "financially material" should be incorporated into a reporting company's scheduled SEC disclosures and in that company's sustainability, impact, CSR, or ESG report.	Communication on Progress (CoP): The CoP is an annual reporting requirement wherein companies set out key information regarding their Global Compact-driven activities.	Organizations are encouraged to disclose material climate-related issues in their mainstream financial filings, whether with the SEC, other regulatory agencies, or ESG/ sustainability reports.
Can the framework be employed in conjunction with other frameworks?	**YES –** GRI is intended as a guide for developing a company specific sustainability report and including metrics and reporting information from other frameworks within the report is encouraged and facilitated.	**YES –** Because SASB is intended to identify financially material sustainability information, the subsequent data, metrics, and narrative are wholly intended to be integrated into both regulatory filings and published sustainability reports.	**YES –** The UNGC and SDGs are both intended as aspirational frameworks used by companies to reach sustainability goals and increase equity across all sectors of society. The principles of the UNGC and the SDGs can be incorporated into sustainability communications, reports, and regulatory filings.	**YES –** The Recommendations were also developed in alignment with other existing reporting frameworks (e.g., CDP, SASB, CDSB, GRI, and IIRC). Therefore, organizations reporting under those frameworks may already have tools that would be useful for the collection and reporting of climate-related information under the TCFD framework.
Does the framework require a materiality assessment?	**YES –** GRI requires an organization to identify material topics in order to establish the scope and included issues covered by a company's report. GRI's framework contemplates that materiality may meaning for different stakeholders. Therefore, material topics are those that may reasonably beconsidered mportant for reflecting the organization's economic, environmental, and social impacts, or influencing the decisions of stakeholders.v	**YES –** SASB is intended to identify financially material sustainability information. Materiality under the SASB framework is determined exclusively through the lens of the "reasonable definition of which has been established by the courts. See Point of Law (POL).	**NO –** The UNGC and SDGs are not intended to be used to narrowly identify specific material information, but rather as goal oriented guideposts for companies seeking to themselves.	**YES –** The Task Force recommends that organizations assess materiality for climate-related in the same way they determine the materiality of other information included in their financial filings.

CHECKLIST

ESG Risk Management for Financial Institutions (Annotated)

Editor's Note: Financial institutions (FIs) may be exposed to ESG and climate risks directly through their own operations and indirectly through services provided to their clients (e.g., financing clients in controversial industries). If not managed well, these risks can negatively affect FIs' financial performance and credit as well as their reputation. Increasingly, FIs are pressured by legislators, regulators, and society, to better manage and disclose these risks, in both the EU and the U.S. For general information about reputational risk, see Overview – Reputational Risk. FIs are often categorized as banks, insurance companies, asset managers, and asset owners. This document focuses mainly on banks, with some examples of climate-risk management for insurance companies. Throughout the document, ESG risks also include climate risk.

Common ESG Risks for Financial Institutions

❑ **Environmental risks**

Climate risks are often categorized into physical risks and transition risks. See Overview – Climate-Related Risks & Opportunities.

Banks can be exposed to the physical risks of climate change when severe weather events like floods, fires, and hurricanes result in borrowers' damaged assets being devalued. This could lead to increased loan default rates, resulting in increased credit risk. In addition, banks that hold collateral assets of fossil-fuel or other carbon-intensive industries may face transition risks of climate change and stranded asset risks. For example, the introduction of a new climate regulation could reduce the demand of fossil fuels, thus devaluing coal reserves.

Insurance companies may also be negatively affected by both physical and transition risks through their underwriting and investment activities. For instance, the value of their real estate portfolios located in areas facing increased physical risk of climate change could be decreased. The NYDFS issued an Insurance Circular Letter asking NY domestic and foreign insurance companies to integrate climate risks in their risk management and governance frameworks, as well as business strategies.

Practice Tip: Best practices include identifying climate risks across all asset classes, sectors, and geographies of a portfolio. Assets in certain jurisdictions could be more vulnerable to the impact of physical risks of climate change such as droughts and sea-levels rise than others.

Nature-related risks (e.g., biodiversity loss) may expose FIs to increased risks such as credit and reputational risks through their operations or services. For example, a company that causes damage to natural resources or biodiversity could be exposed to litigation. As a result, the company's assets could be tied up, resulting in loss of revenue, production, and eventually slowing or stopping overall operations. This would expose FIs to credit risk, as it affects the company's ability to repay its loans. Additionally, FIs that lend to or invest in companies or projects that cause biodiversity loss may suffer reputational damage and risk losing new business opportunities as customers may opt for FIs with a better reputation for sustainability.

The Taskforce for Nature-related Financial Disclosures (TNFD) has been formed by a group of FIs and private firms to develop guidelines for the financial sector to better understand and disclose how they manage risks related to biodiversity loss.

❑ **Social & Governance Risks**

FIs may be exposed to social & governance risks through their own operations or their services. Poor corporate governance practices (e.g., lack of effective board oversight or procedures to monitor and control risks) could adversely affect their financial stability and reputation. FIs that fail to manage and control a workplace safety risk, which is considered a social risk, could be exposed to liability and reputational damage. Additionally, FIs that lend to or invest in companies engaged in human rights violation or companies with poor corporate governance practices may suffer reputational damage and lose new business opportunities if customers opt for FIs with a better reputation for sustainability.

Managing ESG Risks

❑ **Check** that a board member or someone in senior management oversees the assessment and management of ESG risks.

❑ **Integrate** ESG risks into your existing risk management framework. Banks can refer to the OECD Guidelines to carry out ESG due diligence systemically to ensure responsible corporate lending. See Overview – ESG Compliance & Enterprise Risk Management.

- ❑ **Integrate** ESG risks into your credit risks analysis as part of the lending or investment decisions, at customer and transaction level, and at portfolio level.
- ❑ **Disclose** ESG risks to appropriate stakeholders. For climate risk disclosure, refer to the Task Force on Climate-related Financial Disclosures (TCFD)'s supplemental guidance for the financial sector. The Sustainability Accounting Standards Board (SASB) also provides disclosure recommendations for seven industries within the financial sector. For example, it recommends commercial banks disclose how they incorporate ESG into their credit risk analysis in their sustainability report.

PRACTICAL GUIDANCE

Climate-Related Risks & Opportunities

Companies should integrate their climate-related considerations into their strategic planning. In order to do that effectively, companies should ensure that they have identified short, medium, and long-term climate-related risks and opportunities. They should also understand how these risks and opportunities could impact their operations, supply chains, strategy, and finances, among other factors.

Each company may be exposed to different climate-related risks and opportunities depending on the region, market, industry, and the environment in which it is operating. This document provides examples of common climate-related risks and opportunities in alignment with the explanation provided by the Task Force on Climate-Related Financial Disclosures (TCFD). The list is, however, not exhaustive. See Overview – Task Force on Climate-Related Financial Disclosures (TCFD).

Climate-Related Risks

These risks refer to the potential negative impacts of climate change on an organization. They fall under two broad categories: transition and physical risks.

Transition risks	**Legal risks** – risks posed by increasing policies and regulations designed to address climate challenge by: (1) Constraining activities that contribute to the adverse effect of climate change. Examples are greenhouse gas (GHG) emissions regulations such as emissions reduction targets, cap-and-trade regulation, and carbon taxes. These changes could significantly impact companies' financial performance, their assets, and non-compliance may result in fines or penalties; or (2) Promoting adaptation. Examples include regulations imposing mandatory renewable energy targets and energy efficiency standards for buildings or products. Non-compliance could result in fines, penalties, or refusal for occupancy or construction permit (in the case of mandatory energy efficiency standards for buildings). **Litigations risks** – risks posed by claims brought against companies for contributing to climate change. Cases have been brought by private companies, government entities, and state attorneys to hold companies responsible regarding their business's impact on climate change and the financial risks associated with it. Directors and officers of companies who fail to disclose material climate-related risks could also face increased exposure to litigation risks. **Reputation risks** – risks posed by consumers' or the public's attitude toward a company's actions. Climate-related litigation as mentioned above, whether successful or not, could also affect corporate reputation. Emerging technology and market risks – risks posed by uncertainties in the development and use of emerging technologies with lower emissions options (e.g., carbon capture storage, energy efficiency, and renewable energy). For instance, by adopting new energy-efficiency technologies, companies could reduce their electricity bill and enhance their competitiveness in the market. However, the pace of the development and deployment of new technologies are often unknown. Potential financial impacts include research and development (R&D) expenditures for adopting alternative technologies and capital investments in new technology developments.
Physical risks	Physical risks refer to risks posed by increased severity of extreme weather events such as floods and cyclones. They also include long-term shifts in climate patterns that may cause rising mean temperatures and rising sea levels. Physical risks can affect the continuity of companies' operations and their supply chains. This may lead to the reduction of revenue as a result of decreased production capacity and lower sales, as well as increased capital and insurance costs as a result of damages to their facilities.

Climate-Related Opportunities

These opportunities refer to the potential positive impacts on an organization that result from companies' efforts to mitigate and adapt to climate change.

Resource efficiency	Increasing recycling rates and energy efficiency of both buildings and processes could help companies reduce their operating costs.
Energy Source	Increasing the usage of alternative energy sources and technologies could help companies lower carbon emissions from their operations.
Products and Services	Developing new low-emission products and services could improve the companies' competitiveness in the market.
Markets	Seeking new markets can help companies' better position themselves in shifting to a lower-carbon economy.
Resilience	Improving operational efficiencies, developing new products, or designing new operational processes could enable companies to be more resilient to climate impacts. By taking actions to mitigate and adapt to climate change, companies are likely to build reputational resilience as well.

Risk Management

According to the Institute of Risk Management, risk management refers to a process of understanding, analyzing, and addressing risk in order to make sure that organizations achieve their objectives. Risk management must be proportionate to the complexity and type of organization involved.

When adopting a plan for managing climate-related risks, companies may choose to:

- integrate the management of climate-related risks into its company-wide risk management processes such as their centralized enterprise risk management (ERM) program which cover all potential risks and opportunities; or
- establish a specific climate-related risk management process for identifying, assessing, and responding to climate-related risks and opportunities.

See Comparison Table – Leading Strategic Frameworks for Managing Enterprise Risk.

About Bloomberg Law

Bloomberg Law helps legal professionals provide counsel with access to action-oriented legal intelligence in a business context. Bloomberg Law delivers a unique combination of Practical Guidance, comprehensive primary and secondary source material, trusted content from Bloomberg Industry Group, news, timesaving practice tools, market data, and business intelligence. For more information, visit pro.bloomberglaw.com.

For more information, visit **pro.bloomberglaw.com**.

Bloomberg Law