Baker McKenzie.

The Data Protection Imperative:

Litigation and Enforcement Trends in the New Normal | March 25, 2021

Welcome!

Jessica Nall
Partner, Litigation

Jessica is a partner in our San Francisco and Palo Alto offices. She has extensive experience in conducting internal corporate investigations for companies in the technology, financial services, energy, and health care industries, with a focus on technology companies headquartered in Silicon Valley. Jessica has helped a number of well-known public and private companies navigate high-profile crisis situations involving cutting-edge government enforcement and compliance issues. Jessica brings to the table a wide range of experience in both traditional and emerging white collar issues, including in international antitrust enforcement, trade secrets theft, false claims act violations, cyber-crime, information security and privacy, crypto-currencies and tokens, ICOs, and block-chain technology. In addition to her broad internal investigations practice, Jessica has significant expertise in defending individual executives and employees and groups of executives and employees as "pool counsel" in internal investigations and in follow-on government and regulatory inquiries by the SEC, DOJ, and California Attorney General's Office.

Brad Newman
Partner, Litigation

Brad is a litigation partner resident in Baker McKenzie's Palo Alto Office and Chair of the North America Trade Secrets Practice. According to Chambers USA, Brad is a "recognized authority on trade secrets cases" who "is valued for his tenacious, intelligent and thoughtful approach to trade secrets matters." Brad regularly serves as lead trial counsel in cases with potential eight and nine-figure liability, and has successfully litigated (both prosecuting and defending) a broad spectrum of trade secrets cases in state and federal courts throughout the country. He routinely advises and represents the world's leading technology, banking, professional service, manufacturing and commerce companies in connection with their most significant data protection and trade secret matters. Brad is the author of Protecting Intellectual Property in the Age of Employee Mobility: Forms and Analysis, a comprehensive treatise published by ALM that offers authoritative guidance on legal risks and practical steps companies can take to protect their IP and remedy IP theft. Brad specializes in matters related to trade secrets and Artificial Intelligence. He is the Chair of the AI Subcommittee of the ABA. Recognized by the Daily Journal in 2019 as one of the Top 20 AI attorneys in California, Brad has been instrumental in proposing federal AI workplace and IP legislation that in 2018 was turned into a United States House of Representatives Discussion Draft bill. He has also developed AI oversight and corporate governance best practices designed to ensure algorithmic fairness.

Ashley Good,
Chief Legal Officer
& Secretary

acorns

Introduction

Module

1. Post Pandemic + New Administration:
   Regulatory and criminal enforcement trends imposing heightened standards on companies to protect trade secrets and other sensitive data
2. Increased regulatory scrutiny of Artificial Intelligence hiring tools
3. Recent + important California court challenge to employee confidential information and invention assignment agreements
4. Practical Steps

Introduction

Pandemic resulted in unprecedented shifts in how we do business.

- Remote work is here to stay.

Breakneck pace of evolution in US privacy, intellectual property, and cybersecurity law and policy.

- long-standing risks.
- once-in-a-generation challenges.

Changes will reverberate throughout 2021 and beyond, shaping how companies, governments, and the general public use, protect, and regulate data.

Polling question

What are your company's plans for remote work post-pandemic?

A. employees will be permitted to work 100% remotely

B. hybrid model: some days remote, some days in office

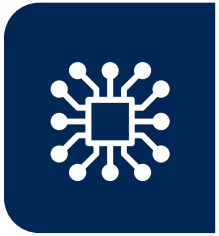
C. some employees, e.g., management level, will be restricted as to level of remote work

D. undecided

Background

Baker McKenzie Connected Compliance Survey and Emerging Trends

Baker McKenzie Connected Compliance Survey Results: New Risks From Digital Acceleration in Pandemic



Rapid digitalization of business drives new compliance risks

- 47% of compliance leaders say that COVID-19 has accelerated a focus towards digital products, approaches and tools in their organizations
- 41% state that ill-considered and poorly implemented technology has already resulted in enforcement investigations
- Up to 64% predict that scrutiny of tech-enabled business models has and will result

Compliance leaders leverage tech to address risk areas

- 56% report that compliance budgets have been cut as a result of COVID-19
- But they continue to make new technology investments to the tune of USD 4.4 million on average per organization
- 71% agree that smart application of technology has already enabled the compliance team to reduce their administrative burden

Evidence on the ground from global investigations

We have seen first-hand that as companies quickly transitioned to remote offices and video conferencing this past year, they did not adequately take into account security, data privacy, and compliance considerations

Polling question

What is your company's policy for use of personal devices and implementation of same?

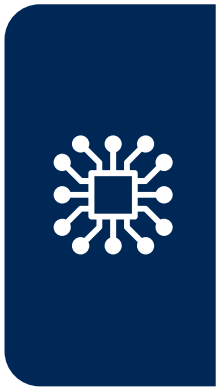
A. personal devices and/or ephemeral apps not allowed to be used at all for work communications

B. personal devices such as employee-owned iPhones commonly used for work

C. company can and does access/retrieve work communications on personal devices

(regardless of policy) personal devices are used as a practical matter when necessary for business

Control of Key Data More Important Than Ever in Enforcement Context



DOJ's Evaluation of Corporate Compliance Programs (June 2020)

- "Data Resources and Access – Do compliance and control personnel have sufficient direct or indirect access to relevant sources of data to allow for timely and effective monitoring and/or testing of policies, controls, and transactions? Do any impediments exist that limit access to relevant sources of data and, if so, what is the company doing to address the impediments?"
- "Updates and Revisions – Is the risk assessment current and subject to periodic review? Is the periodic review limited to a "snapshot" in time or based upon continuous access to operational data and information across functions? Has the periodic review led to updates in policies, procedures, and controls? Do these updates account for risks discovered through misconduct or other problems with the compliance program?"
- "Control Testing – Has the company reviewed and audited its compliance program in the area relating to the misconduct? More generally, what testing of controls, collection and analysis of compliance data, and interviews of employees and third parties does the company undertake? How are the results reported and action items tracked?"

DOJ guidance requires that companies ensure

"Appropriate retention of business records, and prohibiting the improper destruction or deletion of business records, including implementing appropriate guidance and controls on the use of personal communications and ephemeral messaging platforms that undermine the company's ability to appropriately retain business records or communications or otherwise comply with the company's document retention policies or legal obligations."

Dep't of Justice, U.S. Attorney's Manual § 9-47.120(3)(c) (Mar. 2019)

Trade secret litigation at a glance

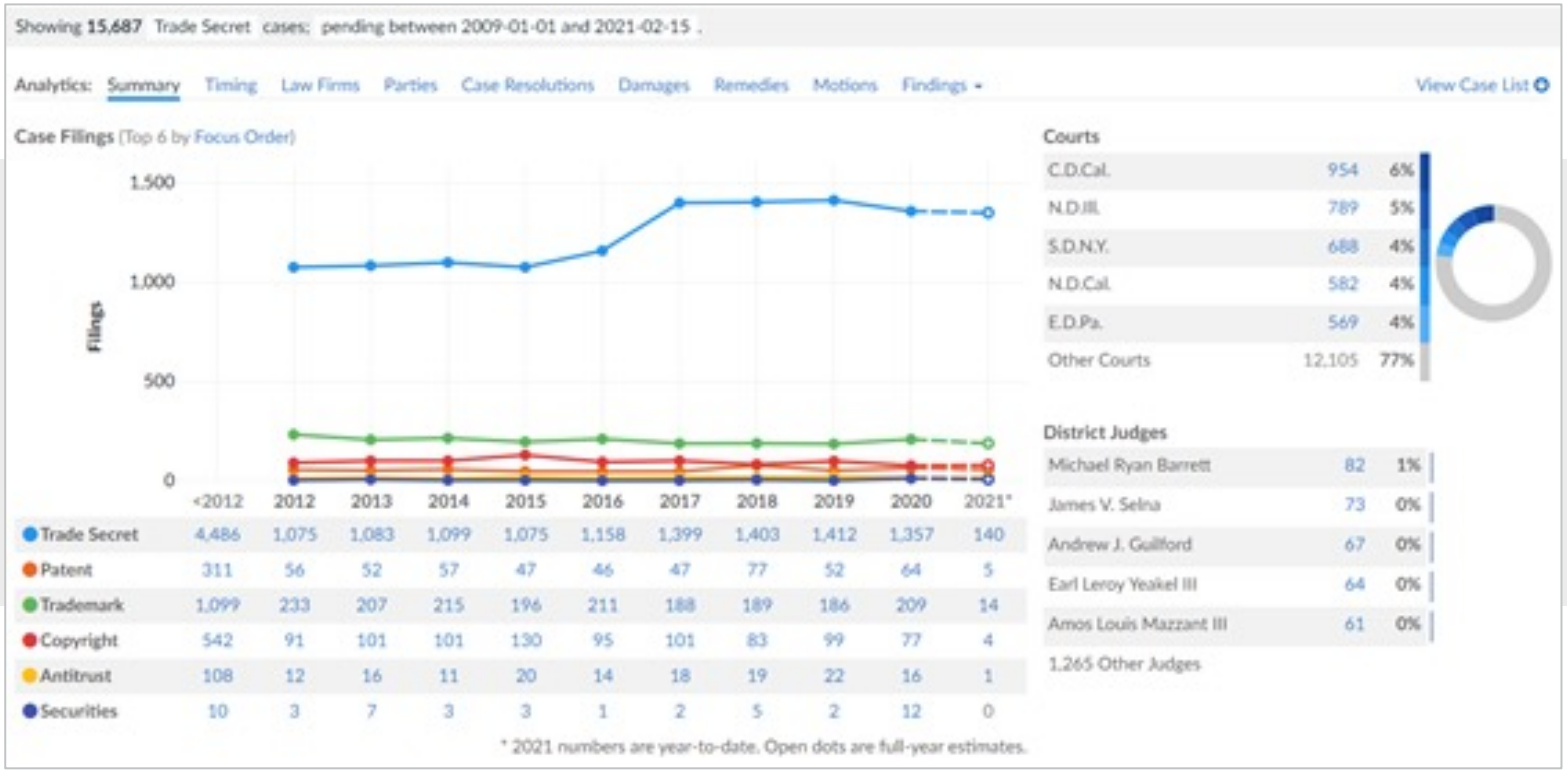
Approximately 1,400 civil trade secret cases filed in federal courts each year in 2018, 2019 and 2020

Central District of California leads by the number of cases filed

The time to trial increased from 2 years to 2.5 years over a three year period

The most amount of damages awarded in trade secret cases was in 2020

Trade secret cases: summary



Top Damages Awards – Trade Secrets Litigation

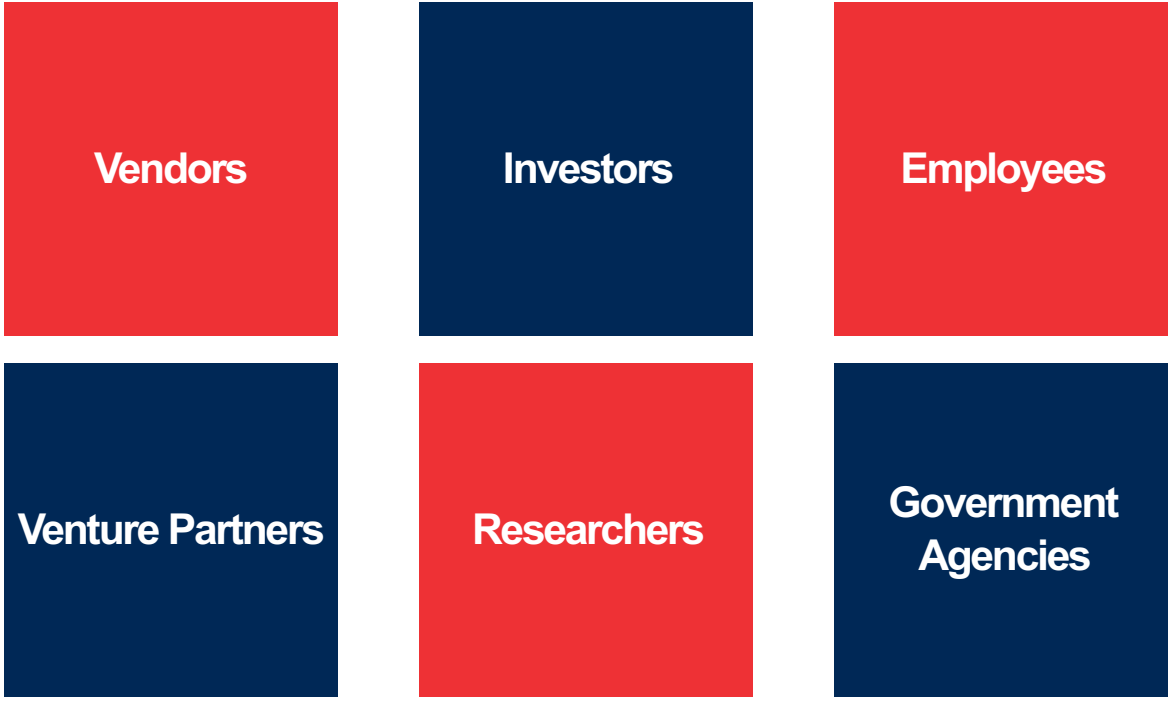
E. I. duPont de Nemours and Co. v. Kolon Industries, Inc. and Kolon USA, Inc.	$919,990,000	Virginia (Eastern)	2011
Epic Systems Corporation v. Tata Consultancy Services Limited and Tata American International Corp.	$420,000,000	Wisconsin (Western)	2017
Cadence Design Systems, Inc. v. Avanti Corp., et al.	$265,000,000	California (Northern)	2002
Bancorp Services, LLC v. Hartford Life Insurance, et al.	$118,338,000	Missouri (Eastern)	2002
X-IT Products, LLC v. Walter Kidde Portable Equipment, Inc.	$116,000,000	Virginia (Eastern)	2002
Brocade Communications Systems, Inc. v. A10 Networks, Inc.	$112,373,822	California (Northern)	2013
Texas Advanced Optoelectronic Solutions, Inc. v. Intersil Corp.	$88,856,662	Texas (Eastern)	2015
Mattel, Inc. v. MGA Entertainment, Inc.	$88,500,000	California (Central)	2011
Alphamed Pharmaceuticals Corp. v. John, Jarrett, Noreen, and Darren Lezdey	$78,000,001	Florida (Southern)	2006
XpertUniverse, Inc. v. Cisco Systems, Inc.	$70,034,383	Delaware	2014
Farm Bureau Life Insurance Co. v. American National Insurance	$69,934,214	Utah	2009

Trade Secret Actions Frequently Joined with:

- Contract Claims
- Tortious Interference
- Whistle-blower
- Breach of Fiduciary Duty
- Patent Infringement
- Unjust Enrichment

Addressing Risk of Litigation

Business relationships that may trigger heightened scrutiny



Module 1: Regulatory and Criminal Enforcement Trends Impacting Data Protection

2020 Securonix Insider Threat Report

- Over 80% of "flight risk" employees tend to take data with them, anywhere from 2 weeks to 2 months prior to their termination date.
- The exfiltration of sensitive data over email (forwarding to personal account) continues to be the #1 egress vector, followed by web uploads to cloud storage sites.
- Other insider risks from:
  - Expansion of cloud collaboration;
  - Circumvention of IT controls or lack of controls;
  - Privileged access misuse.

Symantec Cyber Security Survey 2019

- 62% of employees believe it's appropriate to transfer work documents to personal computers, smartphones, or file-sharing applications, and most never delete the data.
- 44% of employees believe a software developer who creates source code for a company has some ownership in the work, and 42% don't think it's a crime to reuse the source code, without permission, in projects for other companies.
- 65% of employees don't believe it's a crime to use a competitor's trade secrets.

Rapid Changes and Related Risks

Rush to adopt new technologies during pandemic has led to a major shift in the risk of exposure to organizations.

- Security, data privacy, compliance suffered. Companies quickly transitioned to remote offices and video conferencing but did not factor into account security, data privacy, and compliance considerations.
- Whistleblower activity on the rise. Calls to compliance hotlines increased; and uptick in tip-offs to enforcement agencies -- leads that regulators use for new investigations and criminal proceedings.

Spur of the moment decisions in putting technology in place to allow for business continuity in the global emergency led to:

- work on platforms rolled out quickly and with inadequate access controls.
- expanded use of personal devices for business continuity: sensitive data stored on personal devices with inadequate security or controls.
- no or reduced physical supervision.

Greater adoption of virtual payments including anonymized digital currency: new avenues for paying bribes.

Employees who want to do the right thing have found it more difficult due to pandemic restrictions.

Rapid Changes and Enforcement Risks

Trade secrets civil litigation and criminal enforcement is on the rise in the US and globally.

- US DOJ has shown willingness to reach beyond borders to enforce its laws against foreign companies and individuals where the alleged data theft impacts US companies and priorities (e.g. the "China Initiative").

Data security enforcement increasing: when sensitive data is accessed/stolen, "victim" company in the cross-hairs.

- e.g., October 1, 2020, ransomware Advisory by the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC").

Criminal Trade Secrets Enforcement

Criminal Trade Secrets Enforcement

- Criminal trade secret enforcement in the Trump administration was robust.
  - E.g. DOJ's "China Initiative" announced in 2018
- Unprecedented FBI resources assigned nationally to investigating and prosecuting trade secrets violations.
- U.S. Attorneys' Offices (USAO) for the Northern, Central, and Southern Districts of California among most active in prosecuting trade secrets misappropriation cases.
- Incoming administration's Justice Department expected to continue aggressive pursuit of trade secrets misappropriation cases.

Criminal Trade Secrets Enforcement

Key elements of a criminal trade secrets misappropriation case:

- The degree to which the misappropriated information is vital to company's business model or operations;
- The value of the trade secret within the industry;
- The degree to which the misconduct forms a pattern (i.e., hiring more than one employee from the same competitor, etc.);
- The degree to which the misappropriation can be linked to a foreign actor (economic espionage).

Mid-sized and emerging growth tech companies with key technology and a high degree of employee mobility often become a victim or a target in a trade secrets misappropriation criminal investigation.

Civil Enforcement by Securities and Exchange Commission

Biden nominates Gary Gensler to lead the SEC

Gary Gensler,
SEC lead nominee

- Former chairman of US Commodity Futures Trading Commission; led reform of $400 trillion swaps market
- Professor at MIT Sloan School of Management
- Former Goldman Sachs executive
- Former advisor to US Senator Paul Sarbanes in writing the Sarbanes-Oxley Act (2002)
- Former Undersecretary of the Treasury for Domestic Finance; former Assistant Secretary of the Treasury during the Clinton Administration

Under Gensler, the SEC will take a more active role as a market "watchdog" and pursue greater protections for investors.

SEC Enforcement and Priorities

SEC Examination Priorities

- On March 3, 2021, the SEC announced its examination priorities for 2021.
- A glimpse into the Biden administration's overall priorities for white collar criminal enforcement.

Operational Risk From Remote Work

- Prior to COVID-19 pandemic, firms did not generally focus on the risks of remote work.
- Now the SEC indicated that it will be looking for special policies and procedures that ensure remote work does not compromise data security, including the electronic storage of books and records, and investor records and information.

Information Security Policies

- Companies should re-evaluate and strengthen policies for protection of key information in a remote working environment.

Alternative Data/Disruptive Technology

- Firms using alternative data or "data gleaned from non-traditional sources" can expect scrutiny.
- Focus on regulatory compliance – ensuring that firms properly address concerns related to, among other things, due diligence and material nonpublic information.

2

Module 2: Increased Regulatory Scrutiny of Artificial Intelligence Hiring Tools

Polling question

Is your company:

A using AI hiring tools

B considering AI hiring tools

C wants to learn more about AI hiring tools

not interested in AI hiring tools

"Using AI to Make Hiring Decisions? Prepare for EEOC Scrutiny"

Brad Newman, Bloomberg Law, January 2021

https://news.bloomberglaw.com/us-law-week/using-ai-to-make-hiring-decisions-prepare-for-eeoc-scrutiny

"Ten Senators have written to the EEOC asking it to use its power to investigate and take enforcement action against vendors who create—and companies that utilize—discriminatory hiring algorithms. Baker McKenzie attorney Bradford Newman explains what steps companies should take to prepare."

3

Module 3: Your Employee Confidential Information Agreements Need Review

Polling question

Has your company:

A. reviewed the confidential information and invention assignment agreement in last year?

B. been informed of the difference between "Proprietary" information and "trade secrets"?

C. sued a former employee for employee or customer solicitation?

been sued by a former employee over a post-employment restriction?

New Risk With Confidential Information Agreements

Brown v. TGS Management Company, LLC, 57 Cal. App. 5th 303 (4th Distr. 2020)

- confidentiality provisions prohibited Brown from disclosing or using "Confidential Information" for his own benefit or the benefit of any party other than TGS or a TGS client during and after his employment with TGS.
- Contended provision was overbroad, vague and ambiguous, and in violation of Bus. & Prof. Code 16600.
- Argue the agreement defined "Confidential Information" so broadly as to prevent him from ever working not only in statistical arbitrage, but from securities trading, in general.
- "Confidential Information" included "information, in whatever form, used or useable in, or originated, developed, or acquired for use in, or about or relating to, the Business[.]"
  - Confidential Information" did not involve "information which is or becomes generally known in the securities industry through legal means without fault by" Brown. Brown contended this exception was worthless because the essence of successful statistical arbitrage comprises information and variables that are not generally known.
  - Court noted securities-related information that was not confidential before Brown's employment with TGS would somehow transform into "Confidential Information" of TGS, unless Brown evidenced his prior knowledge with written record
- "Business" was further defined to include "without limitation analyzing, executing, trading, and/or hedging in securities and financial instruments and derivatives thereon, securities-related research, and trade processing and related administration…"
- Court held definition was "strikingly broad"
- TGS Management essentially reserved for itself, without restriction, all information that is "useable in" or that "relates to" the securities industry.
- "Business" would encompass not only the actual business of TGS, statistical arbitrage, but anything related to the entire securities field and perpetually bar Brown from trading securities again, both for commercial and personal purposes.

4

Module 4: Practical Steps

Practical Steps

- Risk-based analysis of new hires.
- High risk hires: obtain consent to search personal devices.
- Attention to levels of access.
- Off-boarding employees sign certifications again: no plausible deniability.
- Make sure everyone understands trade secrets theft is a crime.
- Ensure relevant teams continue vigilance on these issues in times of increased financial pressure and unusual working practices.

Newly Hired Employees Coming Direct from Competitors

Interview phase:

- Homework assignments
- Inform them not to divulge any third party confidential information

Onboarding phase:

- Certification that includes
  - Searched for and returned all third party data
  - None stored in personal accounts, cell phone, etc.
  - No soliciting former colleagues or clients without approval
  - Non-use

First 45 days

- Forensic check of company systems ensuring no third party data
- HR interview
- More important with dispersed employees

Institute High Risk Departure Programs

Prepare well before a remote employee says goodbye

- Critical for when remote employees exit
- Data Loss Team: HR + IT + Legal
- Critical elements include:
  - Immediate accounting for data
  - Return and forensic remediation
  - Exit certification
  - Preservation of hard drives
  - Forensic review for evidence of data theft
  - Be prepared to seek a TRO or seizure order

Polling question

Does your company:

A have a trade secret committee?

B use Data Loss Prevention tools?

C simply rely on HR policies for data protection?

The Trade Secret Audit:

- Forming IP Committee (IPC) + Trade Secret Plan (TSP)
- Site Security, IT, HR, R & D, Product + Legal
- Initial TSP
  - Identify
    - Find the source (drawings, pictures, source code, etc.), creator(s) + custodian(s)
  - Protect
    - Review and strengthen protections; identify and remedy deficiencies
  - Develop scalable processes
    - Proper classification + handling
    - Assigning owners
    - Oversight and accounting

Additional Resources

Additional Information

- Our thought leadership
  - Connected Compliance 3.0: The Currency of Connection
  - Taking Center Stage: The Rise and Rise of M&A Compliance Due Diligence

- Understand the context: increased regulatory and law enforcement scrutiny is real. The stakes are high, and having an effective compliance program is a critical line of defence. Part and parcel of that program is the use of data to identify potential risk areas and control weaknesses. This is both a risk and an opportunity for many tech companies.

- Involve us as advisers. Our time spent will be a drop in the ocean and we can add enormous value:
  - Mitigate risk
  - Implement proper controls
  - Develop policies

How We Can Help?

Our expertise falls into three main buckets:

Client Programs & Risk Management Advice

We conduct risk assessments to assess the efficacy of compliance processes and procedures and internal controls. We design and implement compliance programs, as well as delivering compliance training.

We provide legal advice on trade secret protection, bribery and corruption, fraud, money laundering, trade sanctions, tax evasion, antitrust, ESG compliance.

Transactions

We conduct compliance due diligence as part of transactions to ensure clients are aware of and protected from any potential risks from proposed targets. We support the deals teams to assess the impact on price/value, as well to communicate with the counterparty on sensitive compliance issues. We support on post-acquisition integration

Investigations and 1st Chair Trials: Prosecuting and Defending

We conduct complex internal investigations into trade secret misappropriation, data breaches, anti-bribery and anti-corruption, trade compliance, and sanctions. Our clients rely on us to serve as their first chair trial counsel to both prosecute and defend high stakes trade secrets and data breach cases. We also routinely represent our clients who are subject to law enforcement and regulatory investigations and prosecution.

Baker McKenzie.

Thank you!

bakermckenzie.com