

FOCUS

President's Message

K. Vesna Mijic-Barisic



Dear North-east Ohio Chapter Mem-bers:

As the new Chapter President, I look forward to working with you, our Board of Directors and

our sponsors in 2022.

I cannot thank my predecessor Ray Stefanski enough for his leadership and engagement as our outgoing Chapter President. He left me with big shoes to fill;

luckily, he will remain an active mem-ber of our Executive Committee as the Chapter Treasurer. He is taking over for Kelly Albin, who served in this role for three years. A sincere thank you to her for managing our finances during that time.

The below sponsors delivered so much value to our members in terms of practical and timely legal advice. New issues seemed to arise at every corner for in-house coun-sel since the pandemic started, and our members were grateful they could turn to our network of sponsors to advise, enable and protect their organizations.

We had hoped to transition to more in-person events in late 2021; unfortu-nately, while we were able to hold a few,

we quickly realized that we still needed to rely heavily on virtual platforms. None-theless, our Chapter still had a busy and event-filled year, ending on a positive note with a fantastic virtual social and trivia contest, hosted by Littler.

Thank you all for a wonderful 2021. Here's to a new year of learning, engaging and networking with our corporate coun-sel colleagues and friends.

Sincerely,

Vesna

K. Vesna Mijic-Barisic

2021 - 2022 Chapter President

**I also wish to thank our 2021 sponsors for all their efforts and support.
Once again, they were:**

LAW FIRMS

PLATINUM

Frantz Ward
Jackson Lewis
Littler Mendelson

GOLD

Fisher Phillips

SILVER

Blake, Cassels & Graydon
Dinsmore & Shohl
McGlinchey Stafford
Squire Patton Boggs

VENDOR SPONSORS

DIAMOND

FTI Consulting



Data Privacy and Security in the Remote Work Era

By Bruce F. Martino, CIPP/G, CIPM, 2020 ACC NEO Chapter President

Employees have been working remotely since the mid-2000s.¹ Some employers adopted policies and practices to permit and manage work from a location other than an office facility. Employees (such as the author) at other organizations worked remotely on an informal basis.

The pandemic, starting in March 2020, forced employers to permit employees with certain types of jobs, usually white collar, to work remotely on at least a part-time basis. It is an understatement to say corporate IT departments had to move quickly to enable employees to work remotely. The need for speed was greater than following established processes and procedures around data security. One speaker said IT departments created 'shadow IT' rolling out solutions that were not tested and on which employees were not trained.²

Concerns about security turned out to be real. A study conducted five months after the pandemic began found that 20% of respondents suffered a data breach caused by a remote worker.³ A survey conducted in May 2021 found that 58% of the respondents said they would experience a data breach caused by a remote worker. 26% of the respondents attributed this to lack of employee concern.⁴

A recent survey of chief legal officers found that data privacy and cybersecurity is first on their list of most important issues. Data privacy and cybersecurity has occupied that position since 2020. 55% of the respondents said data protection is their biggest legal challenge. That is a significant increase from 2017 when 27% of respondents said data privacy and data security are extremely important.⁵ IBM published its most recent study on the cost of a data breach in late 2021. The study is based on research done by the Ponemon Institute. The research found the average cost of a data breach was \$4.24 million, a 10% increase over the prior year. The survey also found that the average cost was \$1.07 million higher when remote work was a factor in causing the breach.⁶

We are in Q2 2022. Covid-19 vaccinations have been available since January 2021. Many states and cities have lifted mask requirements and other safety protocols because the danger posed by the original Omicron variant decreased in terms of average daily infection rates and hospitalizations. While the BA.2 variant is now with us, senior executives and human resources professionals are studying their organizations as they plan for the post-Covid-19 workplace.

Global Workplace Analytics estimates that 56% of the U.S. workforce has a job compatible with a remote work arrangement. The same organization predicts that 25 – 30% of the eligible workforce will be working remotely multiple days a week. The reasons include increased demand by employees, competition for talent, greater trust that employees will be productive in a non-office setting and the positive impact on environmental sustainability resulting from less home-to-office travel.⁷ PwC found in its January 2021 survey that while remote work proved successful, many executives were hesitant to move to permanent remote work making the hybrid workplace, i.e., days in and out of the office, the norm.⁸ An October 2021 Gallup poll concluded employers largely foresee making remote work permanent or at least hybrid.⁹

The general trend favors a full-time or part-time remote workplace. This will not be implemented on a universal basis. Some companies prefer workers in the office to enhance collaboration. Certain employees, such as those with lesser experience, benefit from in person interaction.

Employers have presumably improved upon their remote work data security processes and procedures since the early days of the pandemic. They moved from a position of 'just get everyone access so they can do their job' to implementing a thoughtful, risk-based approach to data security in the remote environment. Still, employers are dealing with the need to enable a remote workplace and the need to collect, use, store and transmit data in a

secure way. Employers may still have questions about the extent of their legal obligation to secure data and best practices used to meet that obligation. The remainder of this article will focus on those areas.

Security Standards - Employers' Obligations.

There is no universally inclusive data security standard mandated by federal law.¹⁰ If an employer is not the type of organization covered by a federal standard, that employer must be guided by the applicable state standard.

Ohio enacted the Data Protection Act ("DPA") in 2018.¹¹ The DPA requires organizations to implement a written cybersecurity program designed to, among other things, protect the security and confidentiality of personal information. Further, the program must be of a scale "... consummate with the following factors: (1) the company's size and complexity; (2) the nature and scope of its activities; (3) the sensitivity of the personal information maintained by the company; (4) the cost and availability of tools to improve information security; and (5) the resources available to the company."¹² This is a reasonable measures standard. The DPA requires companies to implement a security program that reasonably conforms with a recognized industry framework such as that published by the National Institute of Standards and Technology. Employers meeting these requirements may be eligible for a safe harbor against tort claims arising out of a data breach. The DPA is intended to be an incentive to organizations to build a cybersecurity program that measures risk in relation to the organization's profile and the sensitivity of the data it handles.

There are a number of other jurisdictions which require organizations to take reasonable measures to protect against the unauthorized access to, and acquisition, use and disclosure of personal information. See, for example, Maryland, MD Code, Comm'l Law § 14-3503(a), California, Cal Civil Code § 1798.81.5 (b), Delaware, Code tit. 6, § 12B-100, the District of Columbia, D.C. Code §

continued on page 3

28-3852a, New York, N.Y. Gen'l Bus Law § 899-BB 2.(a)¹³ and Virginia, Code of Virginia § 59.1-578 A.3 (effective January 1, 2023).

Massachusetts took the groundbreaking step of passing a data security law in 2007. The law required the state's Department of Consumer Affairs to "... adopt regulations relative to any person that owns or licenses personal information about a resident of the commonwealth. . . designed to safeguard the personal information. . . ." of Massachusetts residents. Mass. Gen. Laws. ch. 93H § 2.

201 Mass. Code Regs. 17.03 (1) requires each organization to which the regulation applies to maintain a written information security plan detailing the physical, administrative and technical safeguards it uses to protect personal information. The safeguards must be appropriate to the size, scope and type of business, the organization's available resources, the amount of data stored and the need for security and confidentiality, i.e., the sensitivity of the stored data. §17.03 (2) then lists the types of activities that must be part of the security plan. They include, but are not limited to, appointing an employee(s) who is responsible for administering the plan, conducting risk assessments and reviewing the safeguards annually. Further, §17.04 lists 8 items that should be part of a security program where digital data is present.

Employers not covered by a specific federal or state standard may be left in a quandary as to what constitutes reasonable measures. Legislators and regulators use the reasonable measures standard because one size does not fit, nor it is appropriate for all situations. The data security program implemented by, for example, a global financial institution does not need to be the same as that implemented by a small, local grocery store. The reasonable measures standard gives an employer the

flexibility to implement a program that is risk-based and otherwise appropriate for its unique circumstances.

For an employer still trying to determine what is reasonable, the author suggests that it review the Massachusetts regulation¹⁴. Regulators would likely look favorably on the argument that an organization modeled its security plan on an actual state law even if the employer is not subject to the law. Adverse parties would have a hurdle to overcome in arguing the employer did not act reasonably.

Controls an Employer Can Implement.

As employers evaluate and re-evaluate their data security programs to account for larger numbers of full-time or hybrid remote workers, the following are some of the physical, administrative and technical safeguards which can be used as part of an employer's reasonable security measures¹⁵:

1. Require employees to use complex passwords of at least 8 characters with a combination of upper and lower case letters, numbers and symbols. Establish a standard to change passwords at least every 90 days.
2. Make multi-factor authentication mandatory. A second log in credential greatly decreases the ability of threat actors to infiltrate an employee's account.
3. Keep all software updated with the latest patches and security configurations.
4. Raise employee awareness of threats such as phishing, spear phishing and deep fakes via periodic messaging and mandatory training.
5. Issue corporate-owned devices to employees. The devices should be secure using methods such as encryption.

6. Establish a written incident response plan. Assemble an incident response team, including an IT forensics resource, which is available at the ready to carry out the plan in the event of a data incident. Test the plan periodically via a table top exercise.
7. Remind employees to not share a company-owned device with a family member. Children, in particular, are susceptible to downloading malware.
8. Procure and renew cyber insurance. Be certain it covers incidents caused by remote workers.
9. Devices used by employees working in public spaces using public WiFi and hot spots should be secured by a virtual private network, also known as a VPN.
10. Remind employees to observe the 'clean desk' concept even if at home. Persons other than family can be present in a home.
11. Documents containing sensitive information that are printed away from the office should be returned to the office for shredding.

Conclusion.

Remote work, whether full-time or part of the time, is likely to continue as we seem to be emerging from the worst of the Covid-19 pandemic. It is likely that a larger number of employees will be working remotely than those who worked remotely pre-pandemic. Employers need to use reasonable measures to secure the data they handle.

About the Author

Bruce Martino is a former ACC NEO Board Member and past-President. In 2021, he moved back home to Dayton and has transitioned from in-house counsel to working for a law firm where he specializes in data privacy and security. Bruce can be reached at bmartino@wtplaw.com.

¹³Remote includes work at home. Home can be geographically close to the employee's office location or many miles away. Home can be a second home or a vacation destination. It can be anywhere with an internet connection.

¹⁴International Association of Privacy Professionals, Webconference: "The New Normal: Navigating Work-from-Home Privacy and Cybersecurity Risks" May 8, 2020.

¹⁵Malwarebytes Labs, "20% of Organizations Experienced a Data Breach Due to Remote Workers", <https://blog.malwarebytes.com/reports/2020/08/20-percent-of-organizations-experienced-breach-due-to-remote-workers-labs-report-reveals/#:~:text=Since%20the%20start%20of%20the,shelter%2Din%2Dplace%2Dorders>, August 20, 2020.

¹⁶Help Net Risk, "58% of Orgs Predict Remote Workers Will Expose Them to Data Breach Risk", <https://www.helpnetsecurity.com/2021/05/03/remoteworkers-data-breach/>, May 3, 2021. See also, Osbourne, ZD Net, "Working From Home Causes Surge in Security Breaches", <https://www.zdnet.com/article/working-from-home-trend-causes-surge-in-cybersecurity-costs-security-breaches/>, August 20, 2021.

¹⁷Blake, ACC Docket, "Privacy Professionals Are on the Rise", <https://www.accdocket.com/privacy-professionals-are-rise> [accdocket.com], February 9, 2022.

¹⁸IBM, "Cost of a Data Breach", 2021.

¹⁹Global Workplace Analytics, "Work-at-Home After Covid-19 - Our Forecast", <https://globalworkplaceanalytics.com/work-at-home-after-covid-19-our-forecast>.

²⁰PwC, "It's Time to Reimagine Where and How Work Will Get Done, PwC's US Remote Work Survey, 1-12-21", <https://www.pwc.com/us/en/library/covid-19/us-remote-work-survey.html>.

²¹Saad and Wiget, "Remote Work Persisting and Trending Permanent", <https://news.gallup.com/poll/355907/remote-work-persisting-trending-permanent.aspx>, October 13, 2021.

²²Federal law sets out standards in a sector-like way. As an example, the Security Rule, 45 CFR 164.302, et seq. ("Rule"), adopted under the Health Insurance Portability and Accountability Act, as amended ("HIPAA"), sets

out security standards for safeguarding electronic protected health information. HIPAA and the Rule apply only to 'covered entities', which is defined to include healthcare providers, clearing houses and insurers. The Federal Trade Commission adopted a rule in 2002, amended in 2021, the so-called 'Safeguards Rule', 16 CFR 314, that sets forth standards to protect consumer information. The rule applies only to certain financial institutions.

²³Ohio Rev. Code Ann. § 1354.01, et seq.

²⁴Oberly, "Ohio's Data Protection Act", The Ohio Lawyer, July 1, 2019.

²⁵Subsection (b)(ii) goes on to list the elements of reasonable security program grouping those elements under physical, administrative and technical safeguards. In addition, the New York State Department of Financial Services implemented regulations, 23 NYCRR 500, et seq., to establish cybersecurity requirements for covered financial institutions.

²⁶201 MA ADC §17.01 - 17.05.

²⁷These are not listed in order of importance. All are effective.

Operational GC: Journeying Beyond the Law

By Neil Peretz, Sawa Credit Inc.

As a lawyer, whenever we encounter a new potential legal problem, we are rarely provided answers on the spot. Instead, our most common refrain is, “Let me go look that up and study it.” We answer this way because law is inherently retrospective. We are studying the past to give guidance to our clients for the future.

But what we do when there is not a sufficiently similar “past” to examine?

Recent technologies and new business models are often unaddressed by laws, regulations, and prior cases. In common law jurisdictions, we are particularly challenged because it is this case law that fills the gaps when statutes and regulations are not sufficiently on point.

In civil law jurisdictions, the court may at least have a guiding principle espoused in law that can be applied to a de novo scenario by the court. By contrast, common law courts have less flexibility in their decision-making due to stare decisis.

It’s true some fields are governed by umbrella laws that provide more general principles to follow, such as laws against unfair, deceptive, and abusive Acts and practices (UDAAP). These umbrella laws were created because Congress and regulators could not predict every possible future violation of the law.

Thus, regulators, and possibly private litigants, may develop new causes of action based on broad concepts embodied in these laws. In practice, however, these umbrella laws provide scant prospective guidance because most market participants and litigants wait for regulators to identify which types of fact patterns fall under these umbrella laws.

Given the retrospective nature of law, how should we counsel our clients as in-house attorneys when they are contemplating a new business model or the application of new technologies that are distinct from those covered by existing laws?



In common law jurisdictions, we are particularly challenged because it is this case law that fills the gaps when statutes and regulations are not sufficiently on point.

Rules from the road

Almost a decade ago, I was asked to help a new ridesharing company find a path to legally provide ridesharing services while avoiding becoming saddled by regulations that were inappropriate for their business model. Providing them legal guidance in a truly emerging field taught me many lessons.

1. Set expectations about conflict

In any market where there are incumbent players, someone will be unhappy with a new entrant and even the most airtight legal positioning will not ward off potential litigation and regulatory inquiries.

For example, in ridesharing, the taxi and limousine companies, many of whom held oligopolistic licenses for certain territories, were sure to raise a fuss. Accordingly, my first step in advising my clients was to advise them to set aside a budget for litigation and potential regulatory investigations. Even on the sturdiest legal footing,

my clients would be challenged by those seeking to create a public spectacle or perhaps bankrupt my client.

Make sure your client is ready to invest in a fight!

2. Cover stories matter

Even in a strict liability setting, one’s state of mind and intentions matter to human factfinders. In a regulatory inquiry or tribunal, one will be treated more sympathetically when one has demonstrated a concerted effort to comply with the law before taking any actions.

For the ridesharing company, I advised my client that we should develop a detailed examination of all potentially applicable legal classifications, regardless of how ill-fitting to their business, and either how my client might be able to comply with each or why the classification was inapplicable.

continued on page 5

This study enabled my client to say that its intentions were law-abiding because it did not take a single operating step until it uncovered all the applicable laws and determined how it would comply.

3. Find the best basket

A key goal for the in-house attorney is to examine all possible categorizations that could apply to your business and influence the business model or application of technology itself to fit into the most preferred basket.

You should not just be reactive and feel obliged to find a legal home for any technology or business model thrust at you.

You should not just be reactive and feel obliged to find a legal home for any technology or business model thrust at you. You need to learn the levers in the business model and technology that can be twisted without breaking the economics and market impact that your company is seeking.

Think about how manipulating these levers can potentially shoehorn your business into your most favored categorization or escape from the ambit of the most oppressive regulatory schemes.

In the ridesharing world, for example, we looked at a variety of business categorizations: were we a new kind of common carrier? Could we form a private club of company customers, and would it exempt us from certain rules? If we limited ridesharing to friends, how might one define that term “friend” and would it encompass social media friends or friends-of-friends?

A common theme across many regulatory categorizations that were ill-fitting for the business was that they were all on receiving fares. To escape those categorizations, I suggested changing the business model to eliminate charges for transportation and find other ways to recoup costs.

The result was we launched a free ridesharing service, where riders were given an opportunity at the end of the ride to provide a gratuity to the driver. In order to help everyone assess what might be an appropriate tip, we shared

information about how much others tipped for a ride of a similar length.

4. Train your people’s people

As an attorney, it’s likely you will deal with only the most senior executives in the company or your division. Remember that scores of other team members (perhaps thousands) in your organization are describing your business and business model to the public daily.

In the case of ridesharing, each one of our drivers could be asked by a reporter, regulator, or a spy for a competitor about our business terms and business model. If a single driver were to erroneously report that she received a “fare” instead of an “optional tip,” this would be duly recorded and used as a weapon to undermine our carefully developed regulatory positioning. To address this, we created talking points for all drivers that explained the business model and requested that they pass inquiries about it to a particular senior executive in the company.

Once you develop the appropriate positioning for the company, make sure that even part-time workers can understand it and communicate it clearly and uniformly.

5. Remember the fragility of the commerce clause

My ridesharing client heard about federal laws and license frameworks that sounded on paper, like a regulatory shortcut for the business that could preempt a complicated patchwork of state laws. In reality, the federal government had not occupied the local transportation field, so it was unlikely that a magic federal silver bullet could solve all our regulatory challenges across the country.

But how could I, the in-house attorney, counteract the enthusiasm of the allegedly expert outside counsel?

The answer: Caselaw.

Not surprisingly, we had outside counsel eager to generate fees by studying these federal options and seek vaguely structured meetings with federal officials on our behalf. My client had a very limited legal budget, and I was worried

that the time waiting for the completion of such a study could lead to incorrect representations to investors about our corporate legal positioning.

But how could I, the in-house attorney, counteract the enthusiasm of the allegedly expert outside counsel? The answer: Caselaw.

My law clerk and I looked across the country for cases where a local transportation law violation was preempted by federal law. Not surprisingly, we found extensive caselaw to the contrary. Summarizing the facts and holdings of these cases proved decisive in convincing the business’ senior executives to not rely on a non-existent federal solution to inherently local issues.

6. Remember your audience when trying to change laws

As soon as we launched our service, we actively engaged legislators across the state about how current laws were not well-suited to our new business model. While the legislators were polite, they did not want to hear about new opportunities for societal efficiency that our business offered. Nor were they persuaded that the advent of new technologies necessitates the creation of new laws.

Instead, what the regulators cared about was their voting base. We needed to couch our regulatory requests in terms of jobs we could create and pollution we could reduce, because those messages would resonate with the legislators’ voting base.

Focus legislative advocacy efforts on how you can help the legislator look effective instead of droning on about your new technology.

Conclusion

The core requirement for implementing each of the lessons discussed herein is that you develop a deeper understanding of your business’ economics and building blocks. This represents a great opportunity for you to join the advance party for the next business expedition, rather than being left to pick up the pieces afterward.

NEO CHAPTER NEWS

We ♥ OUR VIRTUAL PROGRAMS!

Keeping Things from Going Bad: The Business Edition

On August 19, Frantz Ward hosted a half-day, in-person CLE, *Keeping Things from Going Bad: The Business Edition*. Held at Stillwater Place at the Cleveland Metroparks Zoo, this half-day program comprised four sections that addressed the following topics:

- Unexpected business acquisition issues
- Withdrawal liability
- Real estate tax implications
- The aftermath of government lending programs created during the pandemic
- When closely held businesses are held too closely
- Attorney-client privilege
- Data privacy

After the program ended, attendees were invited to enjoy happy hour with the speakers and Frantz Ward attorneys on the patio outside the meeting space. There, a few zoo animals made special appearances with their handlers.



The ABCs of ESG

On September 2, Dinsmore & Shohl presented a virtual 2.0 CLE, *The ABCs of ESG*. During the program, the speakers examined and explained how ESG factors concentrate on three areas:

- Environmental: A company's performance on environmental and sustainability issues
- Social: How the company handles relationships with employees, suppliers, customers, and the wider community, including diversity, equity, and fair trade practices
- Governance: How the company is led and handles, among other things, internal controls, cybersecurity, internal investigations, audits, diversity, and shareholder rights.

Chapter Annual Meeting + RoundTable

Vorys, Sater, Seymour and Pease graciously hosted our Chapter Annual Meeting + RoundTable in-person on September 14. After a half-hour of networking, ACC NEO members approved the 2021-2022 Board of Directors slate. Once the meeting was adjourned, all attendees enjoyed an interesting discussion on wage and hour employment classifications.



Virtual RoundTable

On October 7, Jackson Lewis hosted a virtual RoundTable where attendees discussed President Biden's COVID-19 vaccine mandate.

An Ethics Refresher: Considerations for In House Counsel

Fisher Phillips presented a virtual 1.5 CLE, *An Ethics Refresher: Considerations for In House Counsel*, on Tuesday, November 9. Firm attorneys Lauren Tompkins, Associate, and Jazmyn Stover, partner, provided an overview of the Ohio Ethics Laws applicable to in-house counsel and included relevant and timely examples to help attendees polish their skillset and refresh their knowledge on ethical dilemmas and issues that may arise in day-to-day practice. Chris Klasa, Assistant Bar Counsel, Cleveland Metropolitan Bar Association, provided corporate counsel's perspective.

Managing Your International Subsidiary: What U.S. In-House Counsel Need to Know About Operating in Canada

On Tuesday, November 16, 2021, Canada-based firm Blakes, Cassels & Graydon hosted a 1.0 virtual CLE, *Managing Your International Subsidiary: What U.S. In-House Counsel Need to Know About Operating in Canada*. The panelists—two firm-side attorneys and two from in-house—discussed the important differences in privacy law, employment law, and other nuances that make operating a Canadian subsidiary different from solely operating in the U.S. The panel also addressed the issues that arise with allowing a wholly owned subsidiary to operate independently compared to fully folding it into the operations of the parent company.

Second virtual Winter Social

On Friday, December 3, Littler our second virtual Winter Social. The fun started when packages of wonderfully curated snacks and grown-up beverages were delivered to each registrant to enjoy during the social's headlining feature, a trivia contest. The attendees—ACC NEO members and Littler attorneys—were then separated into several teams of 4-5 people, all of which were gunning for the top prize of \$25 Amazon gift cards for each member of the winning team.

Navigating a Robust M&A Market and Other Year-End Considerations

Finishing up the 2021 calendar, Squire Patton Boggs presented a 1.0 CLE on Thursday, December 9, *Navigating a Robust M&A Market and Other Year-End Considerations*. With 2021 seeing another thriving M&A market, the two speakers provided an overview of trends in M&A transactions, post-acquisition integration issues, and other items to consider as the year-end approaches.



EXPERTS WITH IMPACT™

FTI Technology solves data-related business challenges, with expertise in legal and regulatory matters including:

- Protecting data from internal and external threats
- Discovering data for legal and regulatory matters
- Assessing risks and ensuring compliance
- Maximizing IT investments for better productivity

For more information,
please contact:

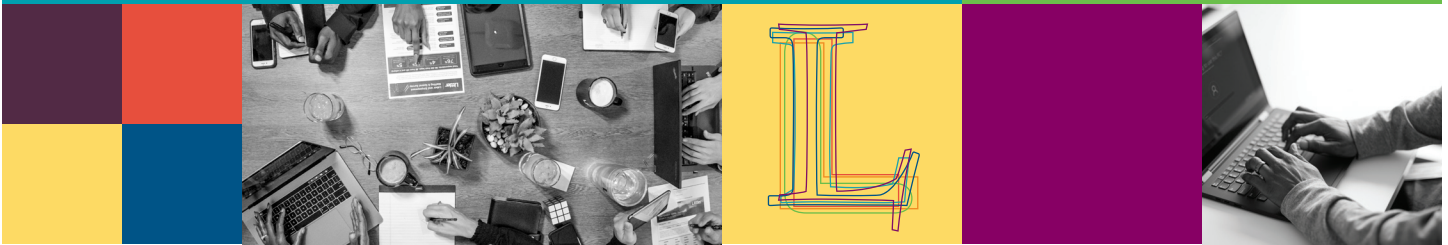
JOHN WINKLER
+1 (216) 543-9087
john.winkler@fticonsulting.com



www.fticonsulting.com

© 2020 FTI Consulting, Inc. All rights reserved.

Littler is a proud supporter
of ACC Northeast Ohio



Unconventional approaches. Ingenious results.

At Littler, we're lawyers. We're also innovators and strategists, passionate problem solvers and creative disruptors. And we're committed to helping our clients navigate the complex world of labor and employment law by building better solutions for their toughest challenges.

Bonnie Kristan
Office Managing Shareholder
216.623.6093
Key Tower
127 Public Square | Suite 1600
Cleveland, OH 44114

Littler[®]

Attorney Advertising

We help you face legal complexities by not being one.

Hiring a lawyer should mean exactly that. You're gaining a partner, a risk manager, and a confidant so that you can finally take a well-deserved deep breath.

Yes, we know exactly the kind of lawyers you'd love to hire, because we've hired them.

FrantzWard.com

Frantz Ward | Love Your Law Firm

Welcome New (and Recently Renewed) Members!

Martina Anders	Lindsie Everett	Craig Moore
Steve Beiting	Robert Fischer	Mark Peasley
Neil Bohan	Traci Forrester	Eric Schreiber
Gina Brickley Beredo	David Gauntner	Nathan Scott
Kevin Burwell	Joshua Goldberg	Aileen Sexton
Timothy Clancy	Alok Gupta	Matt Shady
Maribeth Cooper	David Hirshberg	Ronald Snyder
Erin Creahan	Anne Hurst	Ignacio Walker
Nancy Donnelly	Jennifer Jebber	J. Adam Zangerle
Jeff Dunifon	Jeff League	
Elizabeth Emanuel	Meggan Loudon	

YOUR LEGAL TEAM
of trusted advisors
TO ASSIST WITH ALL
YOUR LEGAL SERVICES.



WALTER | HAVERFIELD

Attorneys At Law

RELATIONSHIPS. COMMITMENT. RESULTS.

Business Services | Intellectual Property | Labor and Employment | Real Estate
Tax and Wealth Management | Litigation | Education Law | Hospitality and Liquor Control | Public Law

CLEVELAND 216.781.1212 | COLUMBUS 614.246.2150 | walterhav.com |   

ACC News

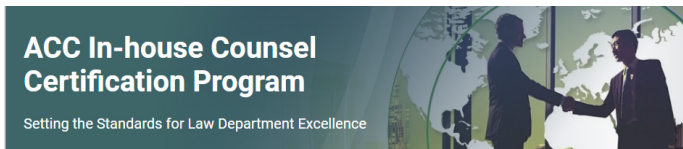
2022 Virtual Cybersecurity Summit: March 8-10, 2022

Registration is now open for the [2022 Virtual Cybersecurity Summit](#). This program offers three days of live educational sessions and networking opportunities, designed to engage and educate professionals about today's most pressing cybersecurity concerns.



ACC In-house Counsel Certification Program: March, 21-31, 2022 Virtual

The [In-house Counsel Certification Program](#) covers the core competencies identified as critical to an in-house career. This virtual training is a combination of self-paced online modules and live virtual workshops. The workshops will be conducted over a two-week period, four days a week for three hours each day.



ACC Europe Annual Conference: May 22-24, 2022 Madrid, Spain

Join your in-house colleagues from across Europe in creating, collaborating, and connecting on topics including ESG, outstanding leadership challenges, DEI, risk management, counsel in a crisis, variance in global anti-trust regimes, legal operations, and much, much more. [Early bird rates end 1 April!](#)



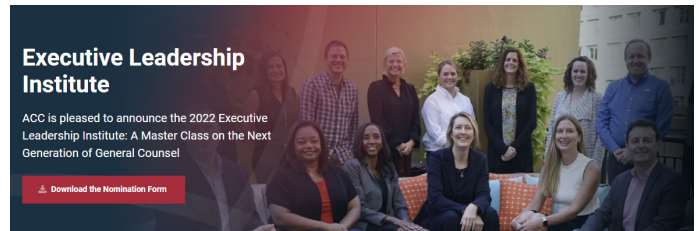
2022 ACC Global General Counsel Summit: June 8-10, 2022 Zurich Switzerland

Save the date for the [2022 Global General Counsel Summit](#), 8-10 June 2022, in Zürich, Switzerland, to collaborate and share ideas on critical trends and challenges facing general counsel with your global chief legal officers in a small, highly interactive setting. Seats are limited. Questions? Want to reserve your seat? Contact Ramsey Saleeby.



ACC Executive Leadership Institute: July 26-29, 2022 Chicago, IL

Invest in your high-performers and put your succession plan in place. Nominate your rising stars to gain the professional development they need to one day lead your department at the [2022 Executive Leadership Institute](#). Seats are limited.



DEI Maturity Model

The DEI Maturity Model is designed for legal departments to benchmark their diversity, equity, and inclusion efforts across a wide range of functional areas. [Download the model.](#)

Renew Your ACC Membership

Don't forget to [renew your ACC membership!](#)



ACC Chief Legal Officers Survey Report Now Available

Uncover CLO's priorities, role, and value to their businesses from ACC's annual in-depth survey of global chief legal officers and general counsel. [Download your free report today!](#) Be sure to join us on Wednesday, March 2 to discuss the findings in this year's report.

**SAVE THE DATE FOR THE
2022 ANNUAL MEETING IN LAS VEGAS!
OCTOBER 23RD TO 26TH.**

Board Members and Contacts

President

K. Vesna Mijic-Barisic

Sr. Associate General Counsel
Cleveland State University

Vice President/President-Elect

Ed Blakemore

Assistant General Counsel
Rockwell Automation

Secretary

Joe Muha

Corporate Counsel/Director of Pharmacy
Compliance
Discount Drug Mart

Treasurer

Ray Stefanski

Corporate Counsel
MetLife Legal Plans

Board of Directors

Kelly Albin

Donald W. Herbe

Jason Hollander

D. Russell Hood

Todd Jackson

Dena M. Kobasic

Jeffrey Lauderdale

David G. Slezak

Dale Smith

Ellen R. Stein

David M. Stringer

Executive Director

Betsy Keck

216.333.3008
neoh@accglobal.com



Betsy Keck
Executive Director
2195 Cranston Road
University Heights, Ohio 44118